On selfish and malicious behaviors in wireless networks - a non-cooperative game theoretic approach

Lin Chen

École Doctorale
d'Informatique,
Télécommunications
et Électronique de Paris

Thèse

présentée pour obtenir le grade de docteur

de l'Ecole Nationale Supérieure des Télécommunications

Spécialité : Informatique et Réseaux

Lin Chen

Sur les Comportements Egoïstes et Malveillants dans les Réseaux sans Fil – une Approche base sur la Théorie des Jeux Non-coopératifs

soutenue le 3 Novembre 2008 devant le jury composé de

Khaldoun Al Agha	**Président**
Tamer Başar	**Rapporteurs**
Ken Chen	
Jean-Pierre Hubaux	
François Bacelli	**Examinateurs**
Philippe Godlewski	
Jean Leneutre	**Directeur de thèse**

Ecole Nationale Supérieure des Télécommunications

École Doctorale
d'Informatique,
Télécommunications
et Électronique de Paris

On Selfish and Malicious Behaviors in Wireless Networks – a Non-cooperative Game Theoretic Approach

Dissertation

submitted in fulfillment of the requirements
for the Ph.D. degree in Computer Science
of Ecole Nationale Supérieure des Télécommunications

Department of Computer Science and Networking

By

Lin Chen

Defended on November 3, 2008

Dissertation committee:

Khaldoun Al Agha	Chair
Tamer Başar	Reviewer
Ken Chen	
Jean-Pierre Hubaux	
François Bacelli	Examiner
Philippe Godlewski	
Jean Leneutre	Thesis Advisor

Acknowledgements

I want to deeply thank my advisor, Dr. Jean Leneutre for his invaluable guidance and support throughout my Ph.D. study. I feel extremely lucky to have Jean as my advisor, whose encouragement and patience is always dedicated to his students, especially in time of doubt and frustration.

My special gratefulness goes to Dr. Lavy Libman for hosting me for a research visit at NICTA in the summer of 2008 (Sydney season), during which Chapter 4 of this thesis was developed. During our fruitful cooperation, Lavy is cordially persistent in steering me and instructing me to explore more deeply in research.

I would like to thank sincerely my committee members: Prof. Tamer Başar, Prof. Ken Chen, Prof. Jean-Pierre Hubaux, Prof. Khaldoun Al Agha, Prof. Philippe Godlewski, Prof. Philippe Godlewski for agreeing to serve in my committee. I would also like to thank Dr. Claude Chaudet, Dr. Marceau Coupechoux, Prof. Olivier Hudry, Prof. Michel Riguidel, Dr. Ahmed Serhouchni whose comments and discussions directly help the development of this thesis.

My gratitude also extends to all my friends and colleagues from whom I have benefited enormously. Particularly, I thank Mohamad Aljnidi for sharing many wonderful moments with me in our conference trips in the last three years; I thank Dr. Xiaoyun Xue for our fruitful discussion and collaboration; I thank Dr. Lixiang Xiong and Dr. Nawaz Safraz at NICTA for making my stay in Sydney a pleasant experience; I thank my present and past officemates, Dr. Jean-Jacques Puig, Dr. Philippe Laurier, Dr. Emmanuel Lavinal, Phuoc Nguyen Tran, Bin Liu and Jing Chi for sharing many wonderful moments with me along the way.

I am indebted to my family. I want to thank my parents and grandparents for their unconditional love and support since my childhood. I want to thank my parents-in-law and many other relatives for their trust and encouragements. Finally, I devote the most special gratitude to my wife Fanfan Zou, to whom this thesis is dedicated. It is their love that throws sunlight into my life.

Abstract

In this thesis, we present an axis of research where non-cooperative game theory is applied as a framework to model and analyze selfish and malicious behaviors in wireless networks. More specifically, the following selfish and malicious behaviors are systematically studied:

- Selfish behaviors
  - MAC layer selfish behaviors in IEEE 802.11 wireless networks
  - Non-cooperative power and rate control in IEEE 802.11 wireless networks
  - Cooperative relaying in wireless networks with selfish users
- Malicious behaviors and defense strategies
  - Intrusion detection in heterogenous networks
  - Jamming attacks in wireless networks and defense strategy
  - Multihop routing amid malicious attackers in wireless networks

By employing non-cooperative game theory as a line of research, for each selfish/malicious behavior, we formulate the corresponding non-cooperative game in the specific context of that problem. The resulting Nash equilibrium (NE) is then derived, followed by an analysis on the key properties of the game solution, i.e., the existence, uniqueness of the NE, the convergence to the NE and the efficiency of the system at the NE. Concerning selfish behaviors, this analysis serves as foundations for the further design of incentive-compatible protocols and pricing mechanisms to fill the gap between the inefficient NE and the global optimal or quasi-optimal point. In the study of malicious behaviors, this analysis leads to the development and validation of new defense mechanisms seeking to eliminate the unfavorable NE from the defender's perspective if multiple NEs exist and limit the damage caused by malicious attackers at the remaining NE.

The first part of the thesis is dedicated to selfish behaviors and defense strategies. We start by addressing the selfish MAC layer behavior in IEEE 802.11 networks where each node can configure its contention window value to maximize its payoff. By establishing a non-cooperative game theoretic model and analyzing the derived solution of the game, we show that selfishness does not always lead to network collapse. On the contrary, selfishness can help the network operate at an equilibrium which is glomal optimal or quasi-optimal under the condition that players are long sighted and follow the TIT-FOR-TAT (TFT) strategy. We then present a game theoretic study on the power and rate control problem in IEEE 802.11 WLANs where network participants choose appropriate transmission power and data rate in a selfish and non-cooperative way to achieve maximum throughput with minimum energy consumption. Three specific games are analyzed: the fixed-rate power control game, the fixed-power rate control game and the joint power rate control

game. Motivated by the fact that only the last game achieves the social optima at the NE, we propose a joint power and rate control procedure whose convergence to the NE is demonstrated both analytically and numerically. Finally, we end this part by addressing the cooperation incentive in cooperative relaying. A pricing framework is proposed based on the idea of "pay for cooperation" to encourage the relay nodes to cooperate. By formulating the cooperative relaying under the proposed pricing framework as a Stackelberg game and deriving the resulting equilibrium of the game, we demonstrate that in general, a Stackelberg Nash equilibrium is guaranteed to exist. By numerical experiments, we further show via several typical scenarios that the equilibria are reasonably efficient.

In the second part of the thesis, we extend our efforts to malicious behaviors. We set out by providing a game-theoretic framework on the network intrusion detection problem in heterogenous environments where network nodes possess different security assets. Under the framework, we derive the expected behaviors of malicious attackers and the optimal strategy of the defenders. We also provide two case studies to illustrate how our game theoretic framework can be applied to configure the intrusion detection strategies in wireless networks. We then focus on jamming, a easily mountable attack with detrimental effects on the victim wireless network. Motivated by the high energy-consuming nature of jamming, we propose our defense strategy to defeat the jammer by draining its energy as fast as possible. To gain an in-depth insight on the jamming and to evaluate the proposed defense strategy, we model the interaction between the jammer and the victim network as a non-cooperative game which is proven to admit two equilibria. We demonstrated mathematically that the propose defense strategy can eliminate the undesirable equilibrium from the network's point of view and increase the energy dispense of the jammer at the other equilibrium without degrading the network performance. To incorporate the specific constraints of wireless networks, we develop a distributed update mechanism for players to adjust their strategies to converge to the equilibrium based on only observable channel information. Finally, we address the challenging task of routing amid malicious attackers in multihop wireless networks with unreliable links. We formulate the multipath routing problem as specific optimization problems. Game theoretic tools are employed to solve the problem and derive heuristic algorithms to compute the optimal path set with polynomial time complexity. As another contribution, we establish the relationship between the security risk and worst-case route availability, which gives the theoretic limit of node-disjoint multipath routing in multihop wireless networks.

Résumé

1 Introduction

1.1 Contexte et motivation

Les réseaux sans fil ont connu un succès sans précédent ces deux dernières décennies grâce à la prolifération des dispositifs sans fil peu coûteux et largement disponibles. Avec une telle croissance explosive, le paradigme traditionnel de réseaux fixes centralisés ne peut plus satisfaire les exigences accrues dans le contexte des réseaux sans fil. Ces exigences posent de nouveaux défis sur le contrôle et la gestion de réseaux. Par conséquent, de nombreuse nouvelles architectures et techniques ont été proposées ou raffinées au cours des dernières années pour rendre l'accès de réseaux plus ouvert et flexible, l'usage de spectre plus efficace. Parmi eux, les réseaux locaux sans fil (IEEE 802.11 WLANs) fournissent une façon efficace d'accéder à Internet à faible coût via les hotspots dans des zones publiques comme les bibliothèques, les aéroports, les hôtels, etc. Les réseaux ad hoc mobiles (MANETs) étendent la connexion sans fil aux scénarios multi-sauts par un ensemble de noeuds mobiles sans infrastructure. La transmission coopérative au niveau des physique (PHY) et/ou MAC (Medium Access Control) offre une opportunité aux utilisateurs de coopérer l'un avec l'autre pour améliorer la performance du réseau

en terme de capacité du canal, de consommation d'énergie et de délai de livraison de paquet.

Dans de tels environnements ouverts, dynamiques et distribués, comme les réseaux sans fil, la sécurité est d'importance cruciale.

D'une part, les réseaux sans fil d'aujourd'hui deviennent de plus en plus ouverts, avec des participants appartenant à différentes autorités. Par conséquent, les noeuds du réseau ont tendance à se comporter égoïstement en maximisant leur propre utilité. Dans ce contexte, les questions centrales sont : comment les comportements égoïstes des noeuds influencent-ils la performance du réseau ? Paralysent-ils le réseau ? Si oui, comment éviter un tel effondrement et encourager les noeuds égoïstes à coopérer ? Malgré les nombreux travaux existants, les réponses aux questions posées sont loin d'être résolues et certaines restent ouvertes, surtout pour les couches PHY et MAC, sur lesquelles nos travaux se focalisent. Nous pensons qu'une étude profonde sur ces problèmes fondamentaux peut avoir un impact important sur la conception des réseaux sans fil modernes.

D'autre part, les caractéristiques uniques des réseaux sans fil d'aujourd'hui (architecture distribuée et dynamique, nature "broadcast" du médium, contraintes de ressource strictes des dispositifs sans fil) les rendent extrêmement attrayants et vulnérables aux attaques malveillantes, e.g., l'attaque par brouillage ("jamming"), la manipulation des informations de routage, l'attaque "wormhole", etc. Dans cette optique, nous arguons que des efforts significatifs devraient être dirigés sur les points suivants

– la caractérisation et l'analyse des comportements malicieux avec un modèle quantitatif bien établi incorporant les caractéristiques spécifiques des réseaux

sans fil ;

– la conception de mécanismes de défense basés sur les résultats analytiques.

1.2 Méthodologie de la thèse

L'objectif de cette thèse est, d'une part, de caractériser et analyser les comportements égoïstes et malveillants dans les réseaux sans fil, et, d'autre part, de concevoir et développer les protocoles efficaces en se basant sur les résultats obtenus pour lutter contre ces comportements. A cet égard, nous introduisons dans cette thèse un axe de recherche où la théorie des jeux non-coopératifs est appliquée de manière systématique pour modéliser les comportements égoïstes et malveillants. Notre motivation de s'attaquer aux problèmes de sécurité des réseaux sans fil en employant une approche basée sur la théorie des jeux (non-coopératifs) est triple :

– la théorie des jeux est un puissant instrument pour étudier les interactions des agents ayant des objectifs mutuellement conflictuels, par exemple, les interactions entre des noeuds égoïstes et les interactions entre des attaquants malveillants à un côté, et des défenseurs ou le réseau victime à l'autre côté ;

– la théorie des jeux non-coopératifs peut modéliser les caractéristiques et les contraintes des réseaux sans fil comme le manque de "feed-back" du réseau et/ou le manque de coordination ; en fait, dans de tels environnements, les comportements non-coopératifs sont beaucoup plus robustes et plus adaptés que le contrôle coopératif centralisé, qui est souvent très coûteux voire impossible à implementer dans certains cas ;

– la théorie des jeux peut servir d'un outil de validation pour évaluer les solutions proposées.

De manière naturelle, la thèse est divisée en deux parties, respectivement dédiées aux comportements égoïstes d'une part, et aux comportements malveillants d'autre part. Dans la suite de cette sous section, sans entrer dans les détails, nous donnons un aperçu de la méthodologie employée dans les deux parties.

Dans la première partie, on considère des scénarios non-coopératifs où chaque noeud égoïste choisit sa stratégie pour maximiser sa propre utilité de manière égoïste. Dans un tel jeu, notre tâche centrale est de déduire et caractériser l'*équilibre de Nash* (NE) où aucun joueur n'a intérêt à modifier son comportement de façon unilatérale. Les études sur l'existence, l'unicité et l'efficacité du NE nous permettent de préciser la structure intrinsèque des comportements égoïstes. Si le NE ne coïncide pas aux optimums sociaux où l'utilité globale du réseau est maximisée, des mécanismes d'incitation comme la tarification et la stratégie TIT-FOR-TAT (TFT) sont alors proposés pour développer des algorithmes distribués orientant les noeuds égoïstes vers les optimums globaux, tout en incorporant les contraintes spécifiques imposées par les réseaux sans fil.

Dans la deuxième partie, les jeux non-coopératifs de deux personnes ("two-person non-cooperative game") sont formulés entre les attaquants malveillant d'un côté, cherchant à maximiser les dommages provoqués dans le réseau victime, et les défenseurs ou le réseau victime de l'autre côté, cherchant à minimiser les dommages. Les travaux avec ces modèles de théorie des jeux nous fournissent un cadre quantitatif pour prédire des stratégies d'attaquants au NE et guider la conception et la validation des mécanismes de défense qui a pour l'objectif d'éliminer les NEs défavorables pour les défenseur s'il en existe plusieurs et de limiter les dommages provoqués par les attaquants à l'équilibre restant.

En résumé, cette thèse aborde un thème pluridisciplinaire en reliant le domaine des réseaux sans fil aux systèmes distribués, à la sécurité, à la modélisation mathématique et à l'économie. Des techniques d'optimisation concave et non-concave sont appliquées pour résoudre les problèmes formulés et analyser les propriétés structurelles des solutions et les compromis correspondants. L'analyse de systèmes dynamiques et les méthodes de calcul distribuées sont employées pour examiner la convergence et la stabilité des mécanismes et algorithmes proposés. Les outils économiques comme la tarification jouent un rôle essentiel pour développer des mécanismes qui ont pour objectif d'inciter les noeuds égoïstes à coopérer et orienter l'équilibre du jeu dans la direction voulue. En effet, nos travaux dans cette thèse peuvent être considérés comme une application de différents outils et méthodes spécifiques dans de différentes disciplines sous le parapluie de la théorie des jeux non-coopératifs pour traiter un problème pluridisciplinaire.

1.3 Contributions et plan de la thèse

Nos contributions dans cette thèse portent sur :

- la modélisation et l'analyse théorique des comportements égoïstes et malicieux en utilisant la théorie des jeux non-coopératifs ;
- la conception et la validation des protocoles et mécanismes basés sur les résultats théoriques et les techniques des simulations afin de répondre aux exigences posées dans Section 1.1.

Plus spécifiquement, nous prenons en compte les comportements égoïstes et malveillent suivants dans le cadre de la théorie des jeux non-coopératifs :

- les comportements égoïstes

- les comportements égoïstes au niveau de MAC dans les réseaux sans fil IEEE 802.11,
- le contrôle de puissance et débit non-coopératif dans les réseaux IEEE 802.11,
- les relais coopératif dans les réseaux sans fil avec des noeuds égoïstes ;

– les comportements malveillant
- la détection d'intrusion dans les réseaux hétérogènes,
- l'attaque par jamming dans les réseaux sans fil et la stratégie de défense,
- le routage multi-chemins parmi les attaquants malveillant pour les réseaux sans fil.

La figure suivante illustre la structure de cette thèse.

Les résultats principaux de cette thèse sont présentés dans les chapitres 2-7. Nous adoptons une structure modulaire pour présenter les résultats : les chapitres sont arrangés comme des modules indépendants, chacun dédié à un thème spécifique mentionné ci-dessus. Plus précisément, chaque chapitre a sa propre introduction et conclusion, décrit le travail lié et l'importance des résultats dans le contexte spécifique du chapitre. Enfin, une conclusion (Chapitre 8) retrace les points essentiels de cette thèse, et présente plusieurs pistes de recherche prospectives dans le prolongement de nos travaux.

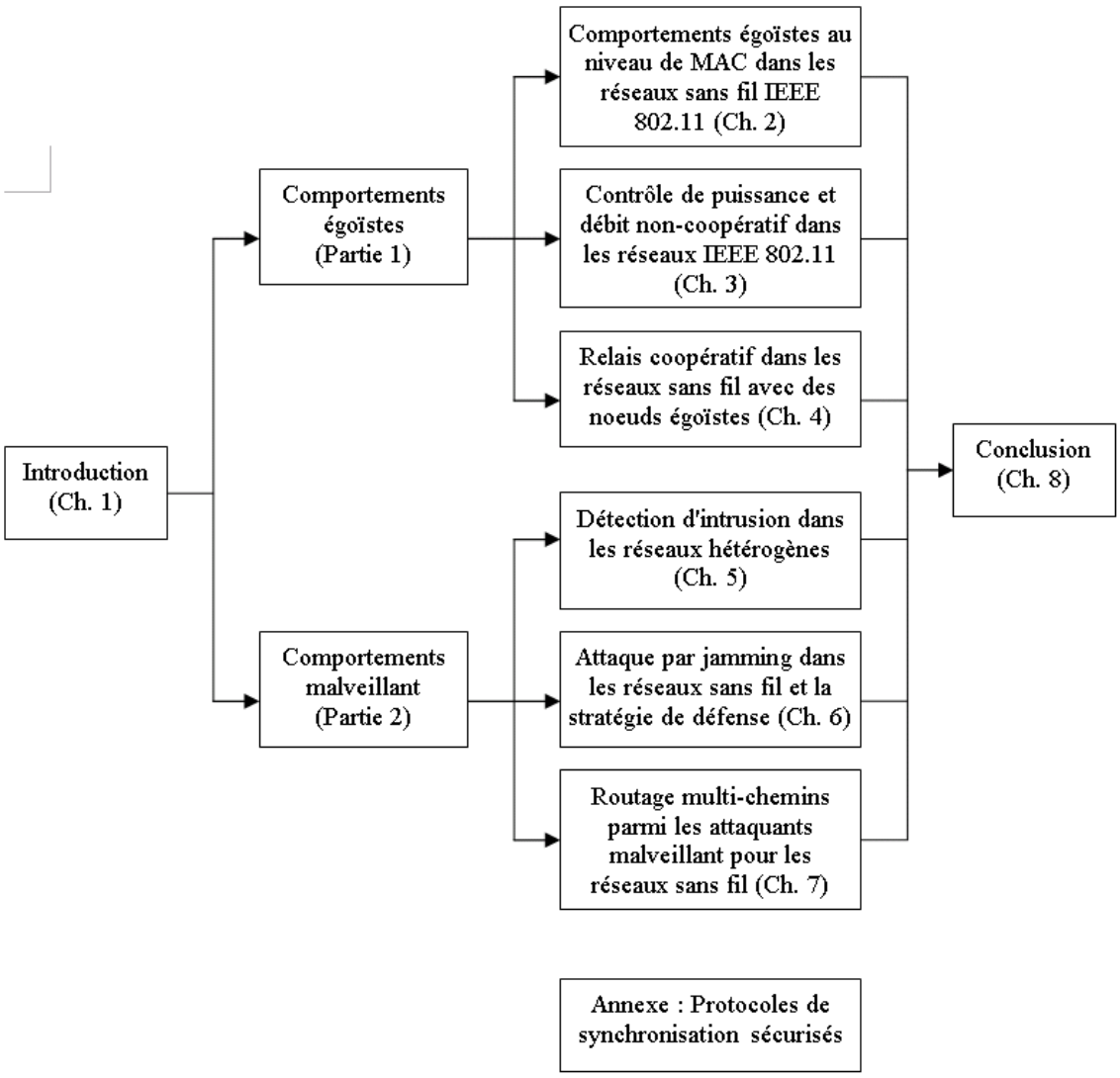

FIGURE 1 – Structure de thèse

2 Comportements égoïstes au niveau de MAC dans les réseaux sans fil IEEE 802.11

Pour les réseaux sans fil où le canal de communication est partagé par tous les participants du réseau, le contrôle d'accès au médium (MAC) joue un rôle clé dans la coordination de la transmission et détermine les propriétés de transmission de données les plus fondamentales, comme l'équité, l'optimalité et la stabilité. Au cours des dernières années, avec le développement explosif des infrastructures sans fil basées sur le norme IEEE 802.11, IEEE 802.11 DCF (Distributed Coordination Function) est devenu l'un des protocoles les plus populaires de la couche MAC pour les réseaux sans fil. Pour garantir un usage efficace et équitable du canal sans fil entre les participants du réseau, IEEE 802.11 DCF exige que tous les participants respectent ses règles. Cependant, cette hypothèse n'est pas toujours valide, surtout dans les environnements ouverts d'aujourd'hui où les utilisateurs du réseau n'appartiennent pas à la même autorité. De plus, les interfaces de réseau deviennent de plus en plus programmables, ce qui permet à un utilisateur égoïste de facilement modifier l'interface sans fil pour maximiser son propre utilité. Dans cette circonstance, une question naturelle mais cruciale est quelle est la performance d'IEEE 802.11 DCF si tous les participants du réseau sont égoïstes. Le réseau peut-t-il survivre ou s'effondre-t-il ?

Le chapitre 2 se focalise sur la question posée en modélisant IEEE 802.11 DCF comme un jeu non-coopératif multi-étaps et en étudiant la performance du réseau au NE. Nos résultats principaux sont les suivants :

– dans les réseaux sans fil uni-saut, l'égoïsme ne cause pas toujours l'effondre-

ment du réseau ; au contraire, il peut aider le réseau à opérer à un NE efficace qui est aussi le point optimal, ce à condition que les joueurs aient une vision à long terme et suivent la stratégie TIT-FOR-TAT (une stratégies considérée comme une des meilleures dans les environnements non-coopératifs) ;

- nous proposons un algorithme simple pour approcher le NE efficace.
- dans le cas multi-sauts, sous la même condition, le réseau opère à un NE qui n'est pas nécessairement le point optimal ; mais nous montrons via des résultats numériques que ce NE est quasi-optimal dans le sens où l'utilité globale est seulement légèrement inférieure à celle du point optimal.

En plus, le modèle établi dans le chapitre 2 est un cadre générique qui peut être étendu pour étudier d'autres comportements égoïstes en redéfinissant ou en adaptant les fonctions d'utilité.

3 Contrôle de puissance et débit non-coopératif distribué dans les réseaux IEEE 802.11

Dans les réseaux sans fil d'aujourd'hui, la plupart des noeuds du réseau, comme des portables et PDAs, sont alimentés par la batterie et ainsi limités dans leurs réserves d'énergies. Donc, il est important pour les noeuds égoïstes d'adopter la stratégie de transmission la plus efficace en terme d'énergie. Dans le chapitre 3, nous nous intéressons aux comportements égoïstes dans les réseaux sans fil IEEE 802.11 où chaque participant du réseau configure sa puissance et débit de transmission de façon non-coopérative pour maximiser son propre débit tout en minimisant sa consommation d'énergie.

Le problème de contrôle de puissance et débit a été largement abordé dans les réseaux cellulaires tant du point de vue de l'optimisation que delui de la théorie des jeux. Cependant, dans le contexte des réseaux sans fil IEEE 802.11 où l'accès au médium est basé sur la contention, le problème de contrôle de puissance et débit est radicalement différent du fait des raisons suivantes :

- dans les réseaux cellulaires, la transmission d'un noeud interfère de celles des autres, mais les réseaux sans fil IEEE 802.11 WLANs [1] sont des environnements sans interférence (explicite) dans le sens où il n'y a aucune interférence pendant une transmission réussie.
- En revanche, l'accès au médium basé sur la contention crée une caractéristique importante que nous l'appelons *l'interférence de débit* qui n'existe pas dans les réseaux cellulaires. Le débit de transmission (à la couche PHY) d'un noeud détermine non seulement son propre débit (au niveau de MAC), mais influence aussi les débits des autres noeuds dans le même réseau.

Il y a donc un besoin d'un modèle quantitatif pour le contrôle de puissance et débit dans de tels environnements. Dans le chapitre 3, nous adressons ce besoin en établissant un cadre quantitatif de la théorie des jeux pour ce problème, dans lequel nous étudions trois jeux spécifiques : le jeu de contrôle de puissance avec le débit fixe (G_{NPC}), le jeu de contrôle de débit avec la puissance fixe (G_{NRC}) et le jeu de contrôle de puissance et débit conjoint (G_{NJPRC}). Les deux premiers jeux correspondent respectivement aux problèmes de contrôle de puissance et ce d'adaptation de débit classiques. Dans le troisième jeu, nous traitons le cas général où les noeuds peuvent configurer tant leur puissance de transmission que leur débit.

1. Dans cette thèse, nous considérons le cas uni-saut et uni-canal.

Nous nous intéressons dans nos études plus particulièrement aux problèmes suivants : existe-t-il des NEs dans les trois jeux formulés ? Si oui, est-t-il unique, et les joueurs peuvent-ils converger vers le NE ? Le NE est-il efficace ? Si non, comment améliorer son efficacité ?

Nos contributions sont les suivantes :

– nous établissons un modèle du contrôle de puissance et débit pour les réseaux sans fil IEEE 802.11 en se basant sur la théorie des jeux non-coopératifs et caractérisons l'existence, l'unicité, l'efficacité et la convergence du NE. Dans G_{NRC} où le NE n'est pas optimal, nous proposons un mécanisme de tarification pour améliorer son efficacité.

– nous développons un algorithme du contrôle de puissance et débit conjoint pour approcher le NE du jeu G_{NJPRC}, dont l'efficacité est prouvée (i.e., la NE de G_{NJPRC} est aussi le point optimal). L'algorithme proposé est distribué et peut être incorporé facilement dans le protocole MAC de IEEE 802.11.

En outre, nous montrons dans ce contexte que donner plus de flexibilité dans la configuration des paramètres aux joueurs non-coopératifs peut en effet guider le système vers le point optimal plutôt que causer l'effondrement du système.

4 Relais coopératifs dans les réseaux sans fil avec des noeuds égoïstes

Les *relais coopératifs* ont émergé au cours des dernières années comme une technique importante pour les réseaux sans fil avec des liens instables. Les relais coopératifs profitent de la caractéristique de diffusion du médium sans fil et four-

nissent la diversité supplémentaire contre le “link outages” (provoqué, par exemple, par le “fading” dynamique ou l’effet d’ombres) en autorisant des noeuds voisins entendant une transmission à relayer le paquet entendu à sa destination. De nombreuses méthodes de coopération ont été proposées dans la littérature. Parmi celle proposées dans le cas d’uni-relayeur, les mécanismes “décode-et-envoie” (*decode-and-forward*) et la coopération codée (*coded cooperation*) où le relayeur ajoute les codes correcteurs d’erreurs au paquet entendu. Les idées ci-dessus ont été étendues et adaptées aux transmissions coopératives dans le cas de multi-relayeurs, où le récepteur décode les données en combinant les signaux relayés reçus sur différents sous-canaux séparés multiplexés, ou sur le même sous-canal avec des antennes de réception multiples utilisant des codes espace-temps.

Cependant, pratiquement touts les travaux existants traitent ce sujet de la perspective d’optimisation, supposant simplement que les noeuds relayeurs sont altruistes et ignorent le besoin *d’incitation* de coopération. Cette hypothèse n’est clairement pas valide dans les réseaux avec des noeuds égoïstes, qui ne veulent pas relayer les paquets pour d’autres tout en dépensant ses propres énergies. Dans cette optique, il est impératif de s’attaquer au problème suivant : comment fournir une incitation aux noeuds relayeurs pour qu’ils participent aux relais coopératifs ?

Motivés par le constat ci-dessus, nous proposons dans le chapitre 4 un cadre de tarification basé sur l’idée de “payer pour la coopération” à fin d’encourager la coopération des noeuds relayeurs dans les réseaux sans fil composés des noeuds égoïstes. Dans le cadre proposé, chaque flux (correspondant à une paire de destination-source) offre un paiement pour chaque paquet arrivé à sa destination avec succès, qui est partagé de la façon équitable parmi tous les noeuds coopératifs

qui ont participé dans la retransmission de ce paquet. Dans nos études, l'utilité d'un noeud relayeur est défini comme sa part de paiement reçu moins sa propre dépense de la coopération (par exemple, en terme d'énergie dépensée pour la transmission). Pour un flux, son utilité est la différence entre sa récompense, définie par une fonction concave générique du taux de livraison de paquet, et le paiement payé aux noeuds relayeurs. Nous modélisons les interactions entre les flux et les noeuds relayeurs comme un jeu de Stackelberg, dans lequel les noeuds relayeurs sont les suiveurs qui réagissent en fonction de paiement mis par les flux [2] et les flux sont les leadeurs qui choisissent le paiement pour maximiser leur propre utilité tout en anticipant les réponses des suiveurs au NE.

Dans le chapitre 4, nous présentons une étude systématique et détaillée du jeu de Stackelberg formulé et les propriétés d'équilibres du jeu. Plus précisément, nous montrons que le jeu de suiveurs admet deux types d'équilibres :

- l'équilibre symétrique où tous les noeuds relayeurs jouent la même stratégie (c'est-à-dire coopèrent avec le même sous-ensemble de flux),
- l'équilibre de bordure où chaque noeud relayeur est complètement dédié à un seul flux.

Nous montrons aussi que l'équilibre symétrique est unique. En suite, nous établissons que, de la perspective des leaders, l'existence d'un équilibre de Stackelberg n'est pas garantie si les suiveurs jouent l'équilibre de bordure. En revanche l'existence est toujours garantie si les suiveurs jouent l'équilibre symétrique. Nous soulignons que ces propriétés et structures des équilibres se distinguent radicalement des autres

2. C'est-à-dire, chaque noeud relayeur choisit quel flux ou quel sous-ensemble de flux pour les quels il coopère afin de maximiser son utilité, étant donné le paiement offert par chaque flux et les actions de ses pairs en concurrence.

mécanismes de tarification proposés dans la littérature. Nous présentons à la fin du chapitre une étude numérique pour plusieurs scénarios typiques, dont les résultats de simulations montrent que le cadre de tarification proposé permet au réseau d'opérer sur un équilibre raisonnablement efficace.

5 Détection d'intrusion dans les réseaux hétérogènes

Les réseaux d'aujourd'hui, surtout les réseaux sans fil, deviennent de plus en plus dynamiques, distribués et hétérogènes, ce qui augmente significativement les risques de sécurité en rendant le contrôle et l'administration de réseaux beaucoup plus complexes et sophistiqués que jamais. Par conséquent, les réseaux sont beaucoup plus vulnérables aux différentes attaques comme l'inondation de SYN dans TCP, SSPing et le déni de service (DoS), etc. Les années dernières ont été témoins d'une augmentation significative des attaques et des dommages résultants. Dans un tel contexte, les systèmes de détection d'intrusion (IDS) sont largement déployés comme une ligne de défense complémentaire aux approches de sécurité classiques visant à supprimer les vulnérabilités.

Dans presque tous les réseaux contemporains, les noeuds du réseau (les cibles du point de vue des attaquants) ont normalement des niveaux de sensibilité différents ou, autrement dit, possèdent de différentes valeurs de sécurité selon leurs rôles et les données qu'ils possèdent. C'est-à-dire, les réseaux sont dans beaucoup de cas hétérogènes en terme de sécurité. Certaines cibles sont plus "attrayantes" aux attaquants que d'autres, par exemple, les serveurs contenant des données sensibles et confidentielles, les noeuds de haute hiérarchie dans les réseaux militaires, $\cdots$,

etc. Ces cibles sont aussi mieux protégées et ainsi plus difficiles et coûteuses d'attaquer. Dans de tels environnements hétérogènes, deux questions naturelles mais cruciales sont les suivantes : Quelles sont les comportements attendus d'attaquants rationnels ? Quelle est la stratégie optimale des défenseurs (IDSs) ?

Dans ce chapitre, nous nous intéressons aux questions posées ci-dessus en développant un modèle du problème de détection d'intrusion dans les réseaux hétérogènes basé sur la théorie des jeux non-coopératifs, analysant l'équilibre du jeu et investiguant les implications derrière les résultats analytiques. La stratégie optimale pour les défenseurs est en suite déduite. Des directives pour la conception et le déploiement d'IDSs sont déduites de cette stratégie optimale. Nos résultats dans ce chapitre sont génériques. Aucun contexte spécifique ni d'attaques ni de réseaux n'est supposé dans nos analyses. Cependant, le modèle établi dans ce chapitre est particulièrement adapté aux réseaux sans fil où les interactions entre les attaquants et les défenseurs sont beaucoup plus complexes que dans les réseaux traditionnels fixes et, par conséquent, la stratégie optimale pour les défenseurs représente un compromis de plusieurs facteurs différents.

Nos contributions principales de ce chapitre sont les suivantes :

– en modélisant les interactions entre les attaquants et les défenseurs dans un réseau hétérogène comme un jeu non-coopératif à "somme non nulle", nous déduisons les NEs dans différents contextes, ce qui permet de déduire le comportement attendu de la part d'attaquants rationnels et caractériser le nombre minimum d'IDSs nécessaire pour protéger un système et la stratégie optimale pour qu'un IDS contre efficacement les attaquants ; la modélisation est validée par des résultats de simulation ;

– nous effectuons deux études de cas pour illustrer comment notre modèle peut être appliqué dans les réseaux sans fil pour configurer les IDSs via des scénarios réalistes ;

En résumé, le modèle établi dans ce chapitre peut servir de méthodologie pour guider la conception et la validation d'IDSs dans les réseaux hétérogènes.

6 Attaque par jamming dans les réseaux sans fil et la stratégie de défense

Dans ce chapitre, nous nous intéressons à l'attaque par brouillage, aussi appelé l'attaque par jamming, une attaque facilement montable qui a un effet néfaste sur le réseau victime. L'attaque par jamming est une attaque malveillante dont l'objectif est de bloquer la communication du réseau victime en provoquant intentionnellement des interférences ou collisions avec les transmission légitimes. Souvent lancée aux niveaux PHY et MAC, l'attaque par jamming n'exige aucun matériel spécial et peut pratiquement paralyser n'importe quel réseau sans fil.

Les stratégies de défense contre l'attaque par jamming existants dans la littérature consistent principalement à reculer devant l'attaquant (jammer) après la détection du jamming ou ré-acheminer le trafic pour contourner la zone dont les communications sont bloquées par l'attaquant. Un inconvénient de ces solutions est qu'elles exigent la capacité du saut de fréquences ou une mobilité suffisante des noeuds afin d'éviter d'affronter l'attaquant. Cette exigence peut être coûteuse ou même irréaliste à implémenter dans certains cas comme les réseaux sans fil IEEE 802.11 avec un seul canal. En plus, leur efficacité peut être significativement réduite si l'attaque est

stratégique, par exemple, le retraite et le ré-acheminement de trafic sont beaucoup moins efficaces si l'attaquant continue à bouger d'une manière imprévisible.

Motivés par ce constat, nous traitons le problème sous un autre angle. Nous basons nos analyses sur l'observation que bien qu'un paquet très court est suffisant pour brouiller une transmission légitime, la transmission des paquets continuellement pour bloquer la communication du réseau victime épuise rapidement l'énergie de l'attaquant qui est souvent alimenté par la batterie. Par conséquent, un attaquant dont la batterie est limitée n'arrive jamais à bloquer le réseau de victime pour une longue période. Ceci est surtout vrai dans le cas où la configuration de l'attaquant est restreinte à celle d'un noeud ordinaire du réseau avec une ressource limitée en terme d'énergie, comme un portable et PDA. Étant donné les arguments ci-dessus, une stratégie de défense alternative contre l'attaque par jamming est de lutter activement contre l'attaquant face à face en épuisant son énergie le plus rapidement possible.

Suivant cette ligne de défense, nous conduisons notre analyse dans ce chapitre comme suit. D'abord, nous formulons l'attaque par jamming comme un problème d'optimisation pour l'attaquant dont le but est de bloquer la communication du réseau victime le plus longue temps possible sous sa contrainte d'énergie. A cette fin, l'attaquant contrôle la probabilité de la transmission de paquets de jamming pour chercher un compromis entre augmenter la probabilité de blocage et limiter la dépense d'énergie. Au côté du réseau victime, chaque noeud adapte ses probabilité d'accès au canal pour maximiser sa propre utilité sous l'attaque jamming. Nous modélisons les interactions entre l'attaquant et le réseau de victime comme un jeu non-coopératif G. Nous montrons que G admet deux NEs et à un d'entre

eux, l'attaquant peut paralyser le réseau avec peu de dépense d'énergie. Pour éviter cette NE inefficace de la perspective du réseau victime, nous proposons ensuite une stratégie de défense contre l'attaque par jamming en introduisant l'anti-jammer, un noeud spécial dont le rôle est d'épuiser l'énergie de l'attaquant. Pour accomplir son but, l'anti-jammer configure la probabilité de la transmission des paquets d'appât pour pousser l'attaquant à émettre des paquets de jamming. Nous formulons alors le nouveau jeu de jamming G' en présence de l'anti-jammer et montrons que G' admet un NE unique. A cet équilibre, si l'anti-jammer choisit sa stratégie judicieusement, l'utilité de réseau reste le même que celle dans G, mais la dépense d'énergie de la part de l'attaquant augmente significativement. La stratégie proposée peut éliminer le NE défavorable pour le réseau (le NE inefficace dans G) et augmenter la dépense d'énergie de l'attaquant au NE restant (l'unique NE dans G') sans dégrader la performance du réseau. Ensuite, nous examinons la dynamique de G' en développant les mécanismes distribués avec lesquels l'anti-jammer et les noeuds du réseau calculent leurs stratégies de transmission en se basant sur seulement sur les informations de canal observables. Les résultats analytiques sont confirmés par les simulations que nous effectuons, qui démontrent l'efficacité de la stratégie de défense proposée.

7 Routage multi-chemins parmi les attaquants malicieux pour les réseaux sans fil

Les réseaux sans fil actuels se caractérisent de plus en plus par la présence des attaquants malveillant et les liens instables. Il s'avère donc important de développer

des algorithmes de routage adaptés à ces environnements, tout en satisfaisant les exigences suivantes : d'un côté, le chemin le plus sécurisé doit être choisi tel que la probabilité qu'un paquet soit compromis par les attaquants est minimisée. De l'autre côté, étant donné l'instabilité des liens sans fil, le chemin le plus fiable doit être choisi tel que la probabilité qu'un paquet arrive à sa destination est maximisée.

Une approche naturelle est d'utiliser des chemins multiples pour augmenter la robustesse et la résilience aux attaques malveillantes et la non fiabilité des liens. Cependant, comment choisir les chemins à la fois sécurisés et fiables parmi les candidats d'ordre exponentiel et comment distribuer le trafic parmi eux restent un problème difficile mais crucial.

Dans ce chapitre, nous abordons le problème du routage multi-chemins dans les réseaux sans fil en nous focalisant sur deux métriques : la sécurité et la fiabilité. Nous commençons par le cas où il y a seulement un attaquant et puis étendons nos études au cas où il y plusieurs attaquants.

Nous concentrons d'abord au routage multi-chemins minimisant le risque de sécurité, c'est-à-dire, la probabilité qu'un paquet soit capturé par l'attaquant, étant donné que l'attaquant fait tous ses efforts pour maximiser cette probabilité. Nous modélisons ce problème de routage multi-chemins comme un problème de mini-maximisation et le formulons ensuite comme un problème de flux maximum dans un réseaux avec perte ("lossy network"). Nous déduisons un algorithme de routage multi-chemins pour résoudre le problème de mini-maximisation en temps polynômial.

Bien que la solution obtenue consiste en l'ensemble des chemins les plus sécurisés, ce qui est essentiel pour les applications sensibles en terme de sécurité, la fiabilité des

chemins, définie par la probabilité qu'un paquet arrive à sa destination, est autant importante, et ne peut absolument pas être ignorée, surtout dans les réseaux sans fil où les liens sont instables. Dans cette optique, nous étudions le routage multi-chemins maximiser la disponibilité, étant donné que l'attaquant fait tous ses efforts pour minimiser cette probabilité. En constatant que ce problème ne peut pas être résolu en temps polynômial, nous proposons un algorithme de routage heuristique pour calculer l'ensemble de chemins de la façon la plus optimale possible en temps polynômial.

Ensuite, nous étendons nos analyses pour investiguer le problème suivant : comment trouver un compromis entre la sécurité du chemin et la fiabilité du chemin. Dans cette perspective, nous déduisons un algorithme de routage pour maximiser la fiabilité tout en limitant le risque de sécurité sous un seuil donné. De plus, en guise de limite théorique du routage multi-chemins avec des noeuds disjonctifs (c'est-à-dire, aucun noeud n'appartient à plus d'un chemin), nous établissons la relation entre la disponibilité de chemin dans le pire cas a^* et le risque de sécurité r^* comme suit :

$$a^* \leq r^*(|\mathcal{P}^{nd}| - 1),$$

où $|\mathcal{P}^{nd}|$ dénote le nombre maximal de chemins avec des noeuds disjonctifs dans le réseau.

A la fin du chapitre, nous évaluons la performance des algorithmes de routage multi-chemins proposés par des simulations. Les résultats montrent une bonne performance dans le pire cas en terme de la sécurité et la fiabilité.

8 Protocoles de synchronisation sécurisés pour les réseaux sans fil

L'implémentation de certains des protocoles proposés dans ma thèse nécessite un protocole de synchronisation entre les nuds du réseau. Ce protocole doit être lui-même sécurisé. Nous avons donc proposé à la fin de cette thèse (dans l'annexe) une suite de protocoles de synchronisation "scalable" et sécurisés pour les réseaux sans fil. Les performances des protocoles proposés ont été analysées théoriquement et évaluées par simulation.

9 Conclusion et perspectives

Les réseaux sans fil ont connu un succès sans précédent ces deux dernières décennies grâce à la prolifération des dispositifs sans fil peu coûteux et largement disponibles. Avec une telle croissance explosive, les réseaux sans fil daujourdhui deviennent de plus en plus ouverts, dynamiques et hétérogènes, ce qui pose de nouveaux problèmes de sécurité.

Dans cette thèse, nous introduisons un axe de recherche où la théorie des jeux non-coopératifs est appliquée comme un outil systématique pour modéliser les comportements égoïstes et malveillants dans les réseaux sans fil. Nos contributions majeures portent sur, d'une part, la modélisation des comportements égoïstes et malveillants dans les réseaux sans fil, et, d'autre part, la conception des protocoles efficaces pour lutter contre ces comportements.

Cette thèse consiste en deux parties, respectivement dédiées aux comportements

égoïstes et malveillants :

- la première partie est consacrée aux comportements égoïstes, avec le chapitre 2 adressant les comportements égoïstes à la couche MAC dans les réseaux sans fil IEEE 802.11, le chapitre 3 se focalisant sur le contrôle non-coopératif de puissance et débit dans les réseaux IEEE 802.11, le chapitre 4 proposant un cadre de tarification pour les relais coopératifs dans les réseaux sans fil avec des noeuds égoïstes ; dans ces problèmes d'allocation de ressources, nous avons étudié l'impact des comportement égoïstes sur la performance du réseau ; dans le cas où le NE déduit est inefficace, nous avons développé et analysé des protocoles d'incitation et des mécanismes de tarification spécifiques pour orienter le NE inefficace vers le point optimal ou quasi-optimal ;
- la deuxième partie est dédiée aux comportements malveillants, avec le chapitre 5 établissant un modèle générique pour la détection d'intrusion dans les réseaux hétérogènes, le chapitre 6 analysant l'attaque par jamming dans les réseaux sans fil et proposant une stratégie de défense active, le chapitre 7 s'attaquant au problème du routage multi-chemins parmi les attaquants malveillants pour les réseaux sans fil ; dans ces problèmes de sécurité, nous avons appliqué la théorie des jeux pour analyser les comportements attendus des attaquants malveillant, pour développer et valider des stratégies de défense proposées permettant de limiter les dommages provoqués par les attaquants.

Les travaux réalisés dans cette thèse ouvrent la voie à de nouvelles recherches.

9.1 Contrôle non-coopératif de puissance, débit et MAC conjoint dans les réseaux sans fil

Les chapitre 2 et 3 se focalisent respectivement sur les comportements égoïstes où les joueurs peuvent configurer leur valeurs de fenêtre de contention (CW) et la puissance et le débit de transmission. Une extension naturelle élaborant le problème du contrôle non-coopératif de puissance, débit et MAC conjoint ouvrirait une nouvelle dimension de recherche. En particulier, il serait intéressant d'examiner si les résultats des chapitre 2 et 3 restent valides dans ce nouveau contexte. Par ailleurs, dans le cas où le nouveau jeu admettrait un NE inefficace, comment concevoir les fonctions de tarification incorporant la probabilité d'accès au médium, la puissance et le débit de transmission afin d'augmenter l'efficacité de la NE.

Plus profondément, analyser le jeu non-coopératif dans ce contexte nous permettrait de développer les protocoles de contrôle d'accès au médium efficaces couplés avec le contrôle de puissance et débit ayant les propriétés suivants :

- *convergence et stabilité* : le protocole doit converger vers un équilibre stable ;
- *optimalité sociale et l'équité* : l'équilibre doit être le point optimal ou quasi-optimal pour le réseau où les utilités globales sont partagées entre les participants équitablement ;
- *survivabilité* : le protocole doit garantir que les joueurs obéissent aux règles même si ils sont égoïstes et non-coopératifs ; autrement dit, le protocole lui-même consiste en une stratégie qu'aucun joueur n'a intérêt de refuser.

A cet égard, comment la théorie des jeux non-coopératifs et nos résultats peuvent être appliqués à l'établissement d'une méthodologie pour la conception de protocoles

MAC efficaces reste un problème ouvert.

9.2 Vers un modèle de théorie des jeux hybride

Dans nos études de la première partie de cette thèse, tous les joueurs dans le réseau sont égoïstes et vise à maximiser leur propre utilités, souvent aux dépenses des autres joueurs. Dans un contexte plus général, une question plus ouverte est quelle est la performance du réseau si certains joueurs sont égoïstes, d'autres sont "responsables socialement" suivant différents degrés. Cette situation pourrait être modélisée comme un jeu hybride (coopération et non-coopération) où les comportements des joueurs varient de la coopération totale, pour ceux qui sont entièrement altruistes, à la non-coopération pure, pour ceux qui sont égoïstes et visent seulement à maximiser leur propre utilité. L'analyse de tels jeux relie la théorie des jeux coopératifs et non-coopératifs. Caractériser les NEs dans de tels jeux hybrides nous permettrait d'étudier l'efficacité et la survivabilité des réseaux dans les environnements ouverts et dynamiques. En outre, incorporer les attaquants malveillants dans de tels jeux hybrides en les modélisant comme des joueurs "non-coopératifs" visant à paralyser le réseau ouvre une nouvelle dimension de recherche.

9.3 Limitations de la théorie des jeux classique

Dans nos travaux, nous avons suivi la procédure suivante : premièrement, nous avons formulé le problème comme un jeu non-coopératif et déduit les NEs en utilisant principalement la théorie des jeux classique ; ensuite, nous avons incorporé les limitation de la théorie des jeux classique (par example, la rationalité parfaite) et les contraintes spécifiques imposées par les réseaux sans fil en investiguant quels sont

les impacts sur les stratégies des joueurs et comment développer des mécanismes adaptés aux réseaux sans fil. Par exemple, dans le chapitre 2, la stratégie "Generous TIT-FOR-TAT" (GTFT) est introduite comme une version tolérante de la stratégie TFT. Avec GTFT, le NE du jeu est plus robuste et plus facile à approcher. Dans les chapitre 3 et 6, nous avons développer des mécanismes spécifiques permettant aux joueurs de configurer leurs stratégies en utilisant seulement les informations observables et vérifiables, sans avoir besoin de connaître les stratégies des autres. En plus, la version asynchronisée de ces mécanismes est étudiées car il est parfois irréaliste de maintenir la synchronisation pour des réseaux sans fil.

Malgré les efforts consacrés à l'adaptation de la théorie des jeux dans les réseaux sans fil et l'évaluation des impacts de ses limitations sur les résultats obtenus, nous considerons qu'il reste un problème crucial et ouvert consistant à étudier des jeux "non-classiques" et plus dynamiques.

9.4 Remarques finales

La contribution principale de cette thèse porte sur l'étude des comportements égoïstes et malveillants dans les réseaux sans fil, ou plus généralement, sur les interactions des noeuds du réseau ayant des objectifs mutuellement conflictuels. Bien que les analyses dans cette thèse se focalisent sur des problèmes spécifiques, de l'allocation de ressource sans fil non-coopérative à la détection d'intrusion dans des réseaux hétérogènes, la méthodologie employée et les résultats obtenus sont applicables dans d'autres domaines émergents des réseaux modernes et des systèmes distribués bien au-delà de cette thèse. Etudier la coopération et la sécurité dans ces domaines émergents est un développement important de cette thèse et représente

une voie prometteuse pour la recherche future.

Contents

1 Introduction **2**

1.1 Background and Motivation . . . 2
1.2 Thesis Methodology . . . 3
1.3 Summary of Contributions . . . 4

I Selfishness, Friend and Foe **10**

2 Modeling Selfish MAC Layer Behaviors in IEEE 802.11 Wireless Networks **12**

2.1 Introduction . . . 12
2.2 Related Work . . . 13
2.3 Modeling IEEE 802.11 DCF with Selfish Nodes . . . 13
2.4 Game theoretic model and problem formulation . . . 14
2.5 Solving the IEEE 802.11 MAC Game G_{MAC} . . . 16
2.5.1 Nash Equilibrium Analysis . . . 16
2.5.2 Nash Equilibrium Refinement . . . 17
2.5.3 Approaching the Efficient Nash Equilibrium . . . 18
2.5.4 Impact of Short-sighted (Myopic) Players . . . 19
2.5.5 Impact of Malicious Players . . . 20
2.5.6 RTS/CTS Case . . . 20
2.6 Multi-hop Case . . . 20
2.6.1 Model Adaptation . . . 20
2.6.2 Formulating and Solving the Game . . . 21
2.7 Numerical Results . . . 22
2.7.1 Single-hop Case . . . 22
2.7.2 Multi-hop Case . . . 23
2.8 Discussion . . . 23
2.9 Conclusion . . . 24
2.10 Proofs . . . 24
2.10.1 Proof of Lemma 2.2 . . . 24
2.10.2 Proof of Theorem 2.1 . . . 25
2.10.3 Proof of Lemma 2.4 . . . 25
2.10.4 Proof of Theorem 2.2 . . . 26

3 Non-cooperative Distributed Power and Rate Control in IEEE 802.11 WLANs 28
3.1 Introduction . . . 28
3.1.1 Background and Motivation . . . 28
3.1.2 Summary of Contributions . . . 29
3.2 Problem Formulation . . . 30
3.2.1 IEEE 802.11 Medium Access Control . . . 30
3.2.2 Utility Function . . . 31
3.2.3 Non-cooperative Power and Rate Control Game . . . 32
3.3 Non-cooperative Fixed-rate Power Control Game . . . 33
3.4 Non-cooperative Fixed-power Rate Control Game . . . 33
3.4.1 Best Response Strategy . . . 33
3.4.2 Nash Equilibrium Analysis . . . 34
3.4.3 Inefficiency of the Nash Equilibrium . . . 35
3.4.4 Improving the Efficiency of NE in G_{NRC} . . . 36
3.5 Joint power and rate Control Game . . . 37
3.5.1 Subgradient Update: Better Response Strategy . . . 37
3.5.2 Game Theory Based Joint power and rate Control Procedure for IEEE 802.11 WLAN . . . 39
3.6 Numerical Results . . . 40
3.7 Conclusion . . . 42
3.8 Proofs . . . 42
3.8.1 Proof of Theorem 3.1 . . . 42
3.8.2 Proof of Lemma 3.3 . . . 43
3.8.3 Proof of Theorem 3.2 . . . 43
3.8.4 Proof of Theorem 3.3 . . . 45
3.8.5 Proof of Corollary 3.2 . . . 46
3.8.6 Proof of Theorem 3.8 . . . 46

4 A Pricing Framework for Cooperative Relaying in Wireless Networks with Selfish Nodes 48
4.1 Introduction . . . 48
4.2 System Model and Pricing Framework . . . 50
4.2.1 Wireless network model . . . 50
4.2.2 Pricing framework . . . 51
4.2.3 Stackelberg game formulation . . . 52
4.3 Equilibrium Analysis of the Followers' Game . . . 52
4.3.1 Symmetrical Equilibria . . . 53
4.3.2 Boundary Equilibria . . . 55
4.4 Analysis of the Leaders' Game . . . 56
4.4.1 Followers play symmetrical equilibrium . . . 57
4.4.2 Followers play boundary equilibrium . . . 59
4.5 Numerical Examples . . . 60
4.5.1 Competition between heterogeneous flows: Single relay . . . 61
4.5.2 Two flows and two relay nodes . . . 62

4.6 Conclusion . . . 62
4.7 Proofs . . . 63
4.7.1 Proof of Lemma 4.1 . . . 63
4.7.2 Proof of Lemma 4.2 . . . 63
4.7.3 Proof of Lemma 4.4 . . . 64

II Playing with Enemy 66

5 On Intrusion Detection in Heterogenous Networks 68
5.1 Introduction . . . 68
5.2 Related Work . . . 69
5.3 Network Intrusion Detection Game Model . . . 70
5.4 Solving the Intrusion Detection Game with one Attacker/Defender . . . 72
5.4.1 Sensible Target Set . . . 72
5.4.2 Nash Equilibrium Analysis . . . 73
5.4.3 Further Security Implications Behind NE . . . 77
5.5 Intrusion Detection Game with Multiple Attackers/Defenders . . . 78
5.5.1 Case 1 . . . 78
5.5.2 Case 2 . . . 79
5.6 Model Application: Case Study . . . 81
5.6.1 Case Study 1 . . . 81
5.6.2 Case Study 2 . . . 82
5.7 Network Intrusion Detection as a Stackelberg Game . . . 83
5.7.1 Leader: Attacker Side; Follower: Defender Side . . . 84
5.7.2 Leader: Defender Side; Follower: Attacker Side . . . 85
5.7.3 Lead or Follow . . . 85
5.8 Numerical Study . . . 86
5.8.1 One Attacker, One Defender . . . 86
5.8.2 Multiple Attackers/Defenders . . . 88
5.9 Conclusion . . . 89
5.10 Proofs . . . 90
5.10.1 Proof of Lemma 5.1 . . . 90
5.10.2 Proof of Theorem 5.1 . . . 91
5.10.3 Proof Sketch of Corollary 5.1 . . . 92

6 A Defense Strategy against Jamming Attack in Wireless Networks 94
6.1 Introduction . . . 94
6.2 Network Model and Problem Formulation . . . 96
6.3 Jamming Game Analysis . . . 97
6.4 Proposed Jamming Defense Strategy . . . 98
6.4.1 Jamming Game with Anti-jammer . . . 99
6.4.2 NE Analysis: Comparison with G . . . 100
6.4.3 Choosing Optimal Value of q . . . 101
6.4.4 Further Discussion and Limitation of Proposed Strategy . . . 101

6.5 Game Dynamics and Distributed Strategy Update Mechanism . . . 102
6.6 Implementation Issue . . . 104
6.7 Numerical Results . . . 105
6.7.1 NE Analysis of G and G' . . . 105
6.7.2 Performance Evaluation of Proposed Defense Strategy . . . 105
6.7.3 Game Dynamics . . . 106
6.8 Conclusion . . . 107
6.9 Proofs . . . 107
6.9.1 Proof of Theorem 6.1 . . . 108
6.9.2 Proof of Theorem 6.2 . . . 109
6.9.3 Proof of Corollary 6.1 . . . 109
6.9.4 Proof of Theorem 6.3 . . . 109
6.9.5 Proof of Corollary 6.2 . . . 110
6.9.6 Proof of Theorem 6.4 . . . 110
6.9.7 Proof of Theorem 6.5 . . . 111
6.9.8 Proof of Theorem 6.6 . . . 112

7 On Multipath Routing in Multihop Wireless Networks: Security, Availability and Limit 114
7.1 Introduction . . . 114
7.1.1 Chapter Overview . . . 114
7.1.2 Background and Motivation . . . 115
7.2 System Model and Assumptions . . . 116
7.3 Multipath Routing with Minimum Security Risk . . . 116
7.3.1 Solving the Multipath Routing Problem . . . 118
7.3.2 A Game theoretic Interpretation . . . 119
7.3.3 Complexity Analysis . . . 120
7.3.4 Discussion . . . 121
7.4 Multipath Routing with Maximum Availability . . . 122
7.4.1 Solving the Maximinimization Problem $\mathbf{MP_2}$ . . . 122
7.4.2 Heuristic Path Set Computation Algorithm . . . 123
7.5 Achieving Security/Availability Tradeoff . . . 125
7.6 theoretic Limit of node-disjoint Multipath Routing . . . 126
7.7 Multipath Routing with Multiple Attackers . . . 127
7.7.1 Minimizing Security Risk . . . 127
7.7.2 Maximizing Route Availability . . . 128
7.8 Performance Evaluation . . . 128
7.8.1 Single-Attacker Case . . . 128
7.8.2 Multiple-Attacker Case . . . 130
7.9 Conclusion . . . 130
7.10 Proofs . . . 131
7.10.1 Proof of Theorem 7.2 . . . 131
7.10.2 Proof of Theorem 7.4 . . . 132
7.10.3 Proof of Lemma 7.2 . . . 133

8 Conclusion **136**
8.1 Thesis Summary . . . 136
8.2 Open Issues and Directions for Future Research . . . 137
8.2.1 Non-cooperative Joint MAC/Power/Rate Control . . . 137
8.2.2 Towards a Hybrid Game Theoretic Model . . . 137
8.2.3 Limitations of Classical Game Theory . . . 138
8.3 Concluding Remark . . . 139

A Toward Secure and Scalable Time Synchronization in MANET **140**
A.1 Introduction . . . 140
A.2 Related Work . . . 141
A.2.1 IEEE 802.11 TSF In Ad Hoc Mode . . . 141
A.2.2 Scalable Time Synchronization for Ad Hoc Networks . . . 142
A.2.3 Secure and Fault Tolerant Time Synchronization . . . 143
A.3 System Model . . . 143
A.3.1 Clock Model . . . 143
A.3.2 Time Synchronization Model . . . 144
A.3.3 Attacker Model . . . 144
A.4 Single-hop Secure Time Synchronization Procedure . . . 145
A.4.1 Design Philosophy . . . 145
A.4.2 Assumptions and Requirements . . . 146
A.4.3 Synchronization Procedure . . . 147
A.4.4 Effectiveness of SSTSP . . . 150
A.4.5 Traffic and Storage Overhead . . . 150
A.4.6 Security Analysis . . . 151
A.4.7 Performance Analysis . . . 151
A.4.8 Simulation Study . . . 152
A.5 Multi-hop Secure Time Synchronization Procedure . . . 153
A.5.1 Overview . . . 154
A.5.2 MSTSP . . . 155
A.5.3 Security Analysis . . . 157
A.5.4 Performance Evaluation . . . 158
A.6 Discussion . . . 159
A.7 Conclusion . . . 160
A.8 Proofs . . . 160
A.8.1 Proof of Lemma A.1 . . . 160
A.8.2 Proof of Lemma A.2 . . . 161
A.8.3 Proof of Lemma A.3 . . . 162
A.8.4 Proof of Theorem A.2 . . . 163

Bibliography **164**

List of Figures

1.1 Thesis organization 4

2.1 Global payoff versus CW value, left: basic case; right: RTS/CTS case 23

3.1 NE of G_{NPC} 40
3.2 Trajectory of G_{NRC} under the best response strategy 40
3.3 Trajectory of G_{NRC} with pricing under best response update 41
3.4 Approaching the social optimal point applying Theorem 3.3 41
3.5 Trajectory of G_{NJPRC} under the subgradient update scheme 41

4.1 Prices C^1, C^2 at the SNE (single relay case) 61
4.2 Utility partition among flows and relay 61
4.3 Prices C^1, C^2 at SNE (2-relay scenario) 62
4.4 Price of Anarchy for 2-relay scenario 62

5.1 Sensitivity analysis on the error of a (left) and b (right) 88
5.2 $-U_D$ as function of x, y, left: scenario 1; right: scenario 2 88

6.1 Non-border NE of G 105
6.2 NE of G' under q^* 105
6.3 Comparison of U_J in G and G' 106
6.4 U_J in G' as a function of q 106
6.5 Strategy trajectory of network nodes under (6.6) 107
6.6 Strategy trajectory of jammer under (6.7) 107
6.7 Performance evaluation of the adaptive recursive research 107

7.1 Node splitting 118
7.2 Limitation 121
7.3 Multiple-attacker case: scenario 1 130
7.4 Multiple-attacker case: scenario 2 130
7.5 Two paths forms a cycle 132
7.6 P_1, P_2 shares the edge e 133

A.1 Hash chain scheme 147
A.2 Maximum clock difference: IEEE 802.11 TSF, 100 nodes 152
A.3 Maximum clock difference: IEEE 802.11 TSF, 300 nodes 152
A.4 Maximum clock difference: SSTSP, 500 nodes, m = 4 153
A.5 Maximum clock difference: SSTSP, 500 nodes, m = 1 153

A.6 Maximum clock difference: IEEE 802.11 TSF, 100 nodes, an attacker 154
A.7 Maximum clock difference: SSTSP, 500 nodes, an attacker 154
A.8 Inter-cluster synchronization 155
A.9 Maximum clock difference, IEEE 802.11 TSF 158
A.10 Maximum clock difference, MSTSP 158
A.11 Traffic overhead, MSTSP, 200 nodes 159
A.12 Maximum synchronization error, MSTSP, 200 nodes, 10% attackers 159

List of Tables

2.1 Network parameters 22
2.2 NE: basic case 22
2.3 NE: RTS/CTS case 22

3.1 BER (P_e) for various modulation schemes 31
3.2 NE efficiency for three games 42

5.1 Strategic form of the game for target i 71
5.2 Payoff Matrix of the lead-or-follow game 85
5.3 NE 87
5.4 Payoff degradation due to deviation from NE 87
5.5 Optimal strategy for defenders 88
5.6 Payoff degradation due to resource constraint 89

7.1 Simulation Parameters 129
7.2 Simulation Results: Single-Attacker Case 129

A.1 Synchronization attacks 144
A.2 Maximum clock difference Vs m 153
A.3 Synchronization error: MSTSP 158

List of Algorithms

1 Approaching the efficient Nash Equilibrium $\{W_c^*\}$ 18
2 Adaptive Search Method of p_i 37
3 Game Theory Based Joint Power and Rate Control Procedure 39
4 Max-flow: Most-Improving Augmenting Path 119
5 Heuristic Path Set Computation Algorithm 124

Chapter 1

Introduction

1.1 Background and Motivation

The last two decades have witnessed an unprecedented success of wireless networks due to the proliferation of inexpensive, widely available wireless devices. With such an explosive growth, the traditional paradigm of centralized, fixed networks can no longer satisfy the dramatically increasing demand for wireless services and connections, which poses imminent challenges on network management and control. As a consequence, various networking architectures and techniques have been proposed or refined in recent years to provide more open and flexible network access, more efficient spectrum usage and better network performance. Among them, IEEE 802.11 WLANs provide a cost-effective way of accessing to the Internet via hotspots in public area like libraries, airports, hotels, etc. Mobile ad hoc networks (MANETs) extend the wireless connection to multi-hop scenarios by a set of mobile nodes without centralized architecture or fixed network infrastructure. Cooperative transmission at the physical (PHY) or medium access control (MAC) layer offers an opportunity for users to cooperate with each other to get a better performance in terms of channel capacity, energy consumption and packet delivery delay.

In such open, dynamic and distributed environments as wireless networks, security is a primary concern (see [BH07] for a detailed survey on the security issues in wireless networks).

On one hand, today's wireless networks are becoming more and more open, with network participants belonging to different organizations. Consequently, network nodes may tend to behave selfishly by maximizing his own benefit. In this context, the central questions are: How the individual selfish behaviors influence the network performance? Do they lead to network collapse? If yes, how to avoid such collapse and encourage the selfish nodes to behave cooperatively? Albeit the large body of works in existing literature, the answer of the posed questions is far from completion and some remains open, especially for PHY and MAC layer selfish behaviors which is one of the focus of this thesis. We believe that an in-depth investigation on the above fundamental problems will provide insightful guidance for the proper design of modern wireless networks.

On the other hand, the unique characteristics of nowadays wireless networks, such as distributed and dynamic network architecture, broadcast nature of wireless medium and stringent resource constraints of wireless devices, makes them extremely attractive and vulnerable to malicious attacks, ranging from the easily mountable jamming attacks to the sophisticated manipulation of routing information. With this recognition, we argue that significant efforts should be directed to, on one side, characterize and analyze malicious behaviors under a well established quantitative model

incorporating the specific features of wireless networks, and on the other side, design and refine defense mechanisms based on the analytical results. This motivates the other facet of our thesis work.

1.2 Thesis Methodology

The goal of this thesis is to bring forth the understanding of the selfish and malicious behaviors in wireless networks as well as the design of efficient protocols based on the understanding to cope with them. To this end, we introduce and present an axis of research where the non-cooperative game theory is applied as a systematic framework to model and analyze the selfish and malicious behaviors. The motivation of tackling the security problems in wireless networks from the (non-cooperative) game theoretic perspective is three-fold:

- Game theory is a powerful tool to model the interactions of decision makers with mutually conflicting objectives, e.g., the interaction among selfish nodes and that between the malicious attackers at one side, the defender or the victim network at the other side.
- Non-cooperative game theory can model the features or constraints of wireless networks such as lack of coordination and network feedback. In fact, in such environments, non-cooperative behavior is much more robust and scalable than any centralized cooperative control, which is very expensive or even impossible to implement.
- Game theory can serve as a validation tool to evaluate the proposed solutions.

Naturally, the thesis is divided into two parts, respectively dedicated to selfish and malicious behaviors. Here, without going into analytical details, we give a overview of the methodology employed in both parts.

In the first part, the network is considered as a site where each selfish node adjust its strategy under the non-cooperative paradigm to maximize its own payoff. In such game theoretic studies, the central issue is to derive and characterize the resulting equilibria, termed as Nash equilibrium (NE) in game theory, where no one has incentive to deviate unilaterally. Studies on the existence, uniqueness and the efficiency of NE provide internal structure of the selfish behaviors. If the NE does not coincide with the social optima, incentive mechanisms such as pricing and the Tit-For-Tat (TFT) strategy are then employed in the design of distributed algorithms incorporating the specific features of wireless networks to steer the selfish nodes toward the global optima.

In the second part, two-person non-cooperative games are formulated between the malicious attackers at one side aiming at maximizing the damage caused to the victim network, and the defenders or the victim network at the other side aiming at minimizing the damage. Studies conducted with this game theoretic model provide a quantitative framework to predict attackers behaviors at the resulting NE and serves as foundations for the design and validation of new defense mechanisms that seeks to eliminate the unfavorable NE from the defender's perspective if multiple NEs exist and limit the damage caused by malicious behaviors at the resulting NE.

In summary, this thesis addresses a topic at the nexus of wireless networking, distributed system, security, mathematical modeling and economics. Concave and non-concave optimization techniques are applied solving the formulated optimization problems and analyzing the structural

properties of the solutions and the correspondent tradeoffs; Dynamical system analysis and distributed computation methods are employed in the investigation of the convergence and stability of the proposed algorithms and mechanisms; Economic techniques such as pricing play an essential role in providing the selfish nodes the incentive to behave socially; In fact, our work in this thesis can be regarded as the application of various specific tools in different disciplines under the non-cooperative game theoretic umbrella to address a cross-disciplinary topic.

1.3 Summary of Contributions

Our contributions lie in both the non-cooperative game theoretic modeling and analysis on the selfish and malicious behaviors and the practical protocol/mechanism design and validation to address the challenges raised in Section 1.1 upon theoretically grounded measurement, modeling and simulation techniques. More specifically, we provide a systematic study on the following pressing selfish/malicious behaviors in wireless networks under the non-cooperative game theoretic framework:

- Selfish behaviors
  - MAC layer selfish behaviors in IEEE 802.11 wireless networks
  - Non-cooperative power and rate control in IEEE 802.11 networks
  - Cooperative transmission in wireless networks with selfish users
- Malicious behaviors
  - Intrusion detection in heterogeneous networks
  - Jamming attacks in wireless networks and defense strategy
  - Multihop routing amid malicious attackers in wireless networks

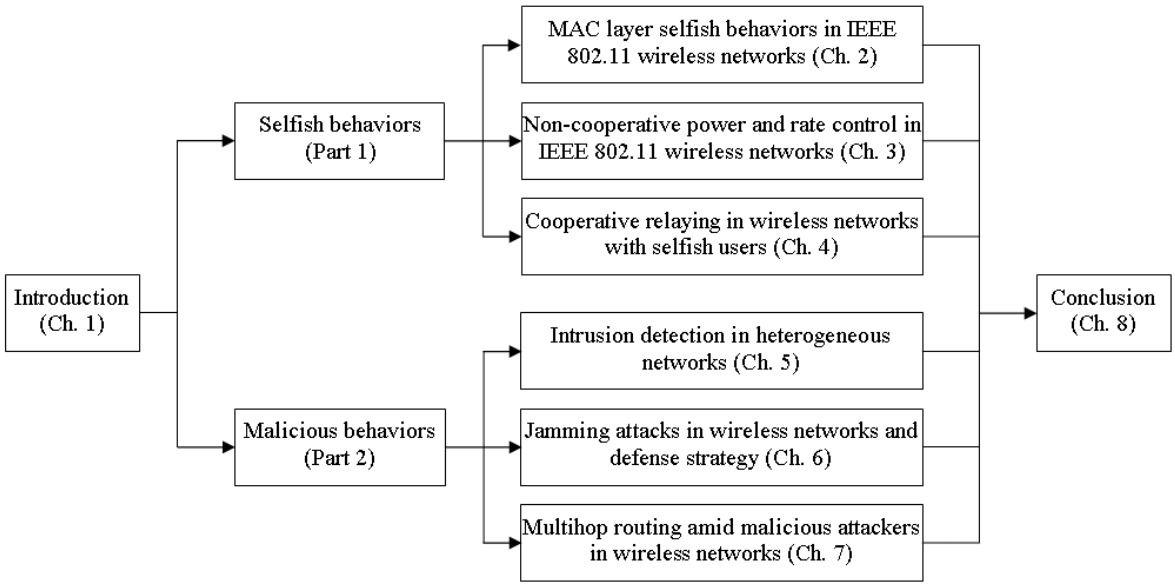

Figure 1.1: Thesis organization

Fig. 1.1 illustrates the organization of the thesis. The main results of this thesis are presented in Chapters 2-7. We adopt a modularized structure to present the results such that the chapters are arranged as independent modules, each dedicated to a specific topic outlined above. In particular, each chapter has its own introduction and conclusion sections, describing the related work and the importance of the results with the specific context of that chapter. For this reason, we are not providing a detailed background, or a survey of past work here. Moreover, the thesis assumes the knowledge of the basic notions and concepts of game theory, as detailed in the textbook [OR94] and the tutorial [FH06] with the emphasis on its application in wireless networks. Finally, we conclude this section of introduction with a summary of contributions and the outline of the thesis.

MAC layer selfish behaviors in IEEE 802.11 wireless networks

The IEEE 802.11 DCF (Distributed Coordination Function), the most popular MAC layer protocol of ad hoc networks, requires all network participants to respect the rules of the protocol. However, network adapters are becoming more and more programmable, which makes a selfish node extremely easy to tamper the wireless interface, especially modifying the Contention Window (CW) value, to maximize its own benefit. Under this circumstance, a natural and crucial question we pose is that how well or how bad IEEE 802.11 DCF performs if all nodes are selfish. More specifically, in such distributed environment as wireless networks where coordination or punishment mechanisms are expensive or even impossible to implement, can IEEE 802.11 DCF survive or does it lead to network collapse? Do we have to modify or even redesign the protocol? In Chapter 2, we study these questions by modeling the selfish MAC protocol as a non-cooperative repeated game where players follow the TIT-FOR-TAT (TFT) strategy which is regarded as the best strategy in such environments. We show for single-hop wireless networks the game admits a unique NE maximizing both local and global payoff. We then extend our efforts to multi-hop case by showing that the network converges to a NE which may not be globally optimal but quasi-optimal in the sense that the global payoff is only slightly less than the optimal case. As main results, we answer the posed questions by showing that selfishness does not always lead to network collapse. On the contrary, selfishness can help the network operate at a NE which is glomal optimal or quasi-optimal under the condition that players are long-sighted and follow the TFT strategy.

Non-cooperative power and rate control in IEEE 802.11 networks

In Chapter 3, we present a game theoretic study on the power and rate control problem in IEEE 802.11 WLANs where network participants choose appropriate transmission power and data rate in a selfish and non-cooperative way to achieve maximum throughput with minimum energy consumption. In such game theoretic study, the central issues are the existence, uniqueness of the NE, the convergence to the NE and the system performance at the NE. We conduct our study for three specific games: the fixed-rate power control game G_{NPC}, the fixed-power rate control game G_{NRC} and the joint power rate control game G_{NJPRC}. The first two games correspond to the classical power control and rate adaptation problem, respectively. We make two main contributions. Firstly, we establish *a non-cooperative game theoretic framework* for the power and rate control in IEEE 802.11 WLANs, based on which we study the existence, uniqueness and convergence of the NE for the three games. In G_{NRC} where the NE is inefficient, we provide pricing scheme to improve the efficiency. Secondly, we propose a *joint power and rate control procedure* to approach the NE

of G_{NJPRC} which is proven to be social optimal. The procedure is distributed in nature and can be incorporated into the IEEE 802.11 MAC protocol easily. We also show that in this context, providing more flexibility in parameter configuration to non-cooperative players in fact helps the system operate optimally rather than lead to system collapse.

Cooperative relaying in wireless networks with selfish users

Extensive research in recent years has shown the benefits of *cooperative relaying* in wireless networks, where a transmission between two nodes is overheard and relayed by a common neighbor. However, most existing studies on the topic tackle the problem from an optimization perspective, assuming that the relay nodes are willing to help the source and ignoring the issue of their cooperation *incentive*. This assumption is inadequate for networks with selfish nodes, which are generally not willing to forward packets of other nodes. In Chapter 4, we propose a pricing framework based on the idea of "pay for cooperation" to encourage cooperation by relay nodes. Under this framework, a relay node is offered a payment by the source in exchange for a cooperative transmission that allows the destination to successfully decode the transmitted packet. We formulate the resulting scenario as a Stackelberg game, in which the source nodes set the payment rates they offer for cooperation, and the relay nodes respond by choosing their cooperation strategies. We provide a systematic analysis of the game, focusing on the fundamental structural properties of the equilibrium. We further demonstrate by a numerical study that the resulting equilibria are reasonably efficient in several typical scenarios.

Intrusion detection in heterogeneous networks

We then set out to extend our game theoretic analysis to malicious behaviors in wireless networks. Today's wireless networks are becoming more and more dynamic, distributed and heterogeneous, which increases significantly the security risk by making the network control and management much more challenging than ever. In such context, the intrusion detection system (IDS) is widely deployed as a complementary line of defense to the classical security approaches aiming at removing the vulnerabilities which may not be very effective or even fail to function in some cases. In almost all contemporary networks, network nodes (targets from the attackers's point of view) usually have different sensibility levels or possess different security assets depending on their roles and the data or information they hold, i.e., they are heterogeneous in terms of security. Some targets are more "attractive" to attackers than others. These targets are usually also better protected and are thus more difficult or costly to attack. In such heterogeneous environments, two natural but crucial questions are: What are the expected behaviors of rational attackers? What is the optimal strategy of the defenders (IDSs)? This is the topic of Chapter 5, in which we provide a game theoretic framework on the network intrusion detection problem by analyzing the equilibria of the game in different settings and investigating the engineering implications behind the analytical results. Under the framework, we derive the expected behaviors of malicious attackers and the optimal strategy of the defenders. We also provide two case studies to illustrate how our game theoretic framework can be applied to configure the intrusion detection strategies in realistic scenarios.

Analysis of jamming attacks and defense strategy

It is widely recognized that the broadcast nature of the shared wireless medium makes wireless networks extremely vulnerable to various attacks. In Chapter 6, we focus on an easily mountable malicious attack that exploit the wireless medium to cause detrimental damage to the victim network, jamming, alternatively termed Denial-of-Service (DoS). Existing defense strategies against jamming mainly consist of retreating from the jammer after detecting the jamming attacks or rerouting traffic around the jammed area. We take a different approach. Motivated by the high energy-consuming nature of jamming, we propose our defense strategy to defeat the jammer by draining its energy as fast as possible. To gain an in-depth insight on the jamming and to evaluate the proposed defense strategy, we model the interaction between the jammer and the victim network as a non-cooperative game which is proven to admit two equilibria. We demonstrated mathematically that the propose defense strategy can eliminate the undesirable equilibrium from the network's point of view and increase the energy dispense of the jammer at the other equilibrium without degrading the network performance. To incorporate the specific constraints of wireless networks, we develop a distributed update mechanism for players to adjust their strategies to converge to the equilibrium based on only observable channel information. Despite the limitations discussed in Chapter 6, we believe that the proposed defense strategy provides an alternative and active line of defense whose effectiveness is well demonstrated both analytically and numerically.

Multi-hop routing amid malicious attackers

In Chapter 7, we address the challenging task of routing amid malicious attackers in multi-hop wireless networks with unreliable links, such as ad hoc networks. Here, the fundamental and crucial problem is how to choose secure and reliable paths among exponentially many candidates and how to allocate traffic among them. We formulate the multi-path routing problem as three specific optimization problems. In the first problem, we study the multi-path routing solution minimizing the security risk, i.e., the probability that a packet is captured by the attacker under the condition that the attacker makes all its efforts to maximize this probability. We model such multi-path routing problem as an minimaximization problem and formulate it as a maximum flow problem in lossy networks based on which a routing algorithm with polynomial time complexity is derived to solve it. While the obtained solution provides the most security routes, which is crucial for security sensitive applications, the availability is another important issue that definitively cannot be ignored, especially in wireless networks with instable links. To this end, in the second problem, we investigate the multi-path routing solution maximizing the worst-case route availability, i.e., the packet survival probability under the condition that the attacker makes all its efforts to minimize this probability. Game theoretic tools are employed to derive an heuristic algorithm computing the optimal path set with polynomial time complexity. In the third problem, we seek a tradeoff between the route security and availability by deriving the routing solution maximizing the route availability while limiting the security risk under given threshold. As another contribution, we establish the relationship between the security risk and worst-case route availability, which gives the theoretic limit of node-disjoint multi-path routing in multi-hop wireless networks.

We conclude the thesis in Chapter 8 by summarizing the overall results and the methods used to obtain them, and providing possible directions for future research.

In Appendix, we present a secure time synchronization protocol for wireless ad hoc networks that may serve as a building block for the protocols proposed in this thesis, e.g., the synchronized version of the power/rate control protocols to converge to the unique NE. In a broader sense, time synchronization is a key function in wireless networks, from power management, QoS support to realization of cryptography and authentication processes. The two key properties of the proposed time synchronization protocols are the resilience to malicious attackers and the scalability, which make them especially suitable in the context of the thesis.

Part of our research work presented in this thesis is published or to be published in various journals and conferences. Specifically, our work on the MAC layer selfish behaviors in IEEE 802.11 wireless networks was presented in the *27th International Conference on Distributed Computing Systems (ICDCS), June, 2007, Toronto* [CL07c]. Our work on the non-cooperative power and rate control in IEEE 802.11 WLANs was presented in part in the *16th International Conference on Computer Communications and Networks (ICCCN), August, 2007, Hawaii [CL07b], the 15th International Conference on Network Protocols (ICNP), October, 2007, Beijing* [CL07a] with the extended version to be published in *IEEE Journal on Selected Areas in Communication (JSAC), special issue on Game Theory in Communication Systems* [CL08]. Our work on the intrusion detection in heterogeneous networks is currently under revision of *IEEE Transaction on Information Forensics and Security*. Our work on the secure time synchronization protocol for wireless ad hoc networks was published in *Computer Communication (ComCom), Elsevier* [CL07d].

Part I

Selfishness, Friend and Foe

As mentioned in the section of introduction, a fundamental security issue in modern wireless networks with selfish participants is how these selfish nodes interact with each other and what is the impact of their selfish behaviors on the network performance.

In this part, we address this challenge by provide a systematic study on the selfish behaviors where non-cooperative game theory is employed as a basis for analysis. Delving into existing literatures, we find a large body of work on the cooperation enforcement/stimulation for packet forwarding in autonomous wireless networks such as MANETs (see [BH03], [FHB06], [SNCR03] and the references in them), most of which are pricing-based and reputation-based mechanisms. However, selfish behaviors at physical and MAC layers are much less addressed except for some specific areas such as the power control in CDMA networks, even though the answer of the posed challenge is far from completion and some essential questions remains open. Our work in this thesis tries to fill this gap by investigating several PHY/MAC layer selfish behaviors. Chapter 2 focuses on the MAC layer selfish behaviors in IEEE 802.11 ad hoc networks. Chapter 3 focuses on the non-cooperative power and rate control in IEEE 802.11 networks. Chapter 4 focuses on the cooperative relaying in wireless networks with selfish users.

As main results, we show that selfishness does not always lead to network collapse. On the contrary, selfishness can help the network operate efficiently under certain conditions. Moreover, in our analysis, we also incorporate the specific constraints posed by wireless networks which may render the classic game theoretic analysis unrealistic in our context. For example, the best response strategy and the better response strategy elaborated in the thesis can be seen a "limited memory" interpretation [Rub98] of bounded rationality, where players only remember situations in recent iterations. As another example, a tolerated version of the TFT strategy is applied in our context to take into account the various factors in wireless networks that influence the observation of the opponents' actions.

Chapter 2

Modeling Selfish MAC Layer Behaviors in IEEE 802.11 Wireless Networks

2.1 Introduction

For wireless networks where the communication medium is shared by all network participants, medium access control (MAC) plays a key role of transmission coordination and determines the most fundamental performance of data transmission, such as fairness, social optimality and stability. In recent years, with the rapid deployment of wireless infrastructures based on the IEEE 802.11 standard [80299], IEEE 802.11 DCF (Distributed Coordination Function) has become one of the most popular and *de facto* MAC layer protocols for wireless networks. To ensure an efficient and fair usage of the wireless channel among network participants, IEEE 802.11 DCF requires all participants to respect its rules. However, this assumption is not always valid, especially in today's open environments where network users do not belong to a single authority. Moreover, network adapters are becoming more and more programmable, which makes a selfish user extremely easy to tamper the wireless interface to maximize its own benefit. Under this circumstance, a natural and crucial question is how well or how bad IEEE 802.11 DCF performs if all network participants are selfish. Can IEEE 802.11 DCF survive or does it lead to network collapse?

In this chapter, we answer the question by establishing a non-cooperative game theoretic model of IEEE 802.11 DCF and investigating the network performance at the Nash Equilibria (NE). We show both analytically and numerically that selfishness does not always lead to network collapse. On the contrary, it can help the network operate at an efficient NE globally optimal or quasi-optimal under the condition that players are long-sighted and follow the TIT-FOR-TAT (TFT) strategy which is regarded as one of the best strategies in non-cooperative environments.

The rest of this chapter is organized as follows. In Section 2.2, we briefly review the related work. In Section 2.3, we model the selfish behavior in IEEE 802.11 DCF by extending Bianchi's model to selfish environments where network nodes may operate on different Contention Window (CW) values. Based on this model, we formulate the non-cooperative multi-stage MAC game in Section 2.4. In Section 2.5, we solve the game by showing the existence of NE and performing NE refinement to eliminate the inefficient NEs. We then extend our work to multi-hop wireless networks in Section 2.6. Section 2.7 provides numerical results. Section 2.8 discusses some related

issues. Section 2.9 concludes the chapter.

2.2 Related Work

As a powerful tool in modeling interactions among self-interested users and predicting their choice of strategies, game theory is widely employed to study the non-cooperative behaviors on the network and transport layers, particularly the non-cooperative flow control and non-cooperative routing (see [Lib] for a detailed survey on them). In contrast, much less work has been done on the MAC layer, among which [JK02] studies the non-cooperative equilibria of Aloha networks for heterogeneous users. [MW03] studies the stability of multi-packet slotted Aloha with selfish users and perfect information, [AEAJ03] reconsider the same Aloha game with partial information, where the transmission probability is adapted according to collision feedback.

In the context of IEEE 802.11 MAC protocol, [TG05] shows that IEEE 802.11 DCF leads to inefficient equilibria if users configure their packet size and data rate to maximize their own throughput. [CGAH05] shows that the existence of small population of selfish nodes leads to network collapse. The authors thus propose a penalizing scheme to guide the selfish nodes to a Pareto optimal NE.

Existing work shows that without coordination among nodes, selfish behaviors degrade the network performance or even paralyze the system. Thus punish or incentive mechanisms are needed to encourage nodes to adopt socially optimal behaviors. However, in our work, by introducing the TFT strategy, a natural strategy in non-cooperative environments, we show that even without any coordination or incentive mechanisms which may be expensive or even impossible to implement in some cases such as ad hoc networks, selfishness does not lead to network collapse. On the contrary, selfishness can help the network operate at an equilibrium which is globally optimal or quasi-optimal under the condition that players are long-sighted and follow the TFT strategy.

2.3 Modeling IEEE 802.11 DCF with Selfish Nodes

We consider a wireless network consisting of a set $\mathcal{N} = \{1, 2, \cdots, n\}$ of selfish nodes within the same communication range, i.e., each node can hear any other node. By selfish we mean that each node can configure its own CW value and $CW_{min} = CW_{max}$, i.e., network nodes do not double their CW value upon a collision. We assume that the network is saturated, i.e., each node always has packets to send and the packets are of the same size.

In this context, let W_i denote the CW value of node i, τ_i denotes the transmission probability of i in a random slot, p_i denotes the collision probability of i when it transmits a packet in a random slot, based on the Bianchi's Markov chain model [Bia00] of IEEE 802.11 DCF, we have:

$$\begin{cases} \tau_i = \dfrac{2}{W_i + 1} \\ p_i = 1 - \displaystyle\prod_{j \in \mathcal{N}, j \neq i} (1 - \tau_j) \end{cases} \qquad \forall i \in \mathcal{N}. \tag{2.1}$$

As an application, (2.1) can be used to calculate the normalized network throughput S, defined

as the fraction of time the channel is used to successfully transmit packets:

$$S = \frac{S_{slot}}{T_{slot}} = \frac{P_s P_{tr} E[P]}{(1-P_{tr})\sigma + P_{tr} P_s T_s + P_{tr}(1-P_s)T_c},$$

where S_{slot} is the time to successfully transmit a packet, T_{slot} is the average slot length, $E[P]$ the average packet size, $P_{tr} = 1 - \prod_{j\in\mathcal{N}}(1-\tau_j)$ is the probability that there is at least one transmission in the considered slot time, $P_s = \frac{\sum_{i\in\mathcal{N}} \tau_i \prod_{j\in\mathcal{N}, j\neq i}(1-\tau_j)}{P_{tr}}$ is the probability that exactly one node transmits on the channel conditioned by at least one node transmits. The average length of a slot time is obtained considering that, with probability $1-P_{tr}$, the slot time is empty, with probability $P_{tr}P_s$, it contains a successful transmission, and with probability $P_{tr}(1-P_s)$, it contains a collision. In the formula, T_s is the average time the channel is sensed busy due to a successful transmission, T_c is the average time the channel is sensed busy by each node during a collision. σ is the duration of an empty slot time. In basic IEEE 802.11 DCF access mechanism without the RTS/CTS dialog, assuming that the packet size is the same for all packets, let H denote the time to transmit the packet header including the PHY and MAC header and P denote the time to transmit a packet, neglecting the propagation delay, we have:

$$\begin{cases} T_s = H + P + SIFS + ACK + DIFS \\ T_c = H + P + SIFS \end{cases}. \tag{2.2}$$

2.4 Game theoretic model and problem formulation

In this section, we establish a non-cooperative game theoretic model on the selfish IEEE 802.11 MAC behavior in which all network nodes are selfish, rational and do not cooperative in managing their communication. Each node i chooses its CW value W_i to maximize its own benefit described by a utility function defined as

$$u_i = \frac{\tau_i[(1-p_i)g_i - e_i]}{T_{slot}}, \tag{2.3}$$

where g_i is the gain of node i when successfully transmitting a packet, e_i is the cost of transmitting a packet, T_{slot} is the average slot length. u_i, expressed as the expected gain during a slot time divided by the slot length, can be regarded as the expected payoff per unit time. To simplify the problem, we assume that g_i and e_i are the same for all $i \in \mathcal{N}$, denoted respectively as g and e. Throughout this chapter, we assume that $e \ll g$. Next we introduce the non-cooperative IEEE 802.11 MAC game.

We model the IEEE 802.11 MAC protocol with selfish nodes as a repeated non-cooperative game G_{MAC} with unpredictable end time, meaning that the players cannot predict the end time of the game. This is often the case in strategic interactions, in particular networking operations. In game theory this can be modeled as an infinite multi-stage game with discount. The discount factor is usually very close to 1, indicating that the players are in general long-sighted. The game starts at time 0 and each stage lasts T. In our context, the players of the game are all the nodes in the network. The strategy set of the players is the CW value set $\mathcal{W} = \{1, 2, \cdots, +\infty\}$. The strategy profile $\mathbf{W^k}$ played in stage k is thus the n-tuple consisting of each player's stage game

strategies[1], i.e.,

$$\mathbf{W^k} = (W_1^k, \cdots, W_n^k) \quad W_i^k \in \mathcal{W}.$$

We denote the correspondent transmission probability profile and collision probability profile in stage k as $\tau^{\mathbf{k}} = (\tau_1^k, \cdots, \tau_n^k)$ and $\mathbf{p^k} = (p_1^k, \cdots, p_n^k)$.

In G_{MAC}, each player i chooses its CW value $W_i^k \in \mathcal{W}$ for stage k at the beginning of the stage and operates on W_i^k for the whole stage. The decision of W_i^k is made based on previous actions of other players. In the following, we give the formal definition of G_{MAC}.

Definition 2.1. *The non-cooperative IEEE 802.11 MAC game G_{MAC} is a 4-tuple $(\mathcal{P}, \mathcal{S}, \mathcal{U}, \delta)$, where $\mathcal{P} = \mathcal{N}$ is the player set, $\mathcal{S} = \times_{i \in \mathcal{P}} \mathcal{W}$ is the strategy space, $\mathcal{U}$=$\{U_1, \cdots, U_n\}$ is the utility function space where $U_i = \sum_{k=0}^{+\infty} \delta^k U_i^s(\mathbf{W^k})$ is the utility function expressed as the sum of the utility in each stage k, $U_i^s(\mathbf{W^k}) = u_i(\mathbf{W^k})T$ is the stage utility function, δ is the discounting factor which is close to 1 for long-sighted players.*

In G_{MAC}, players are self-interested and rational, thus they adopt the strategy that maximizes their own payoff. In this chapter, we focus on the TFT strategy, a well known strategy in game theory which is regarded as one of the best strategies in non-cooperative environments and is the root of an ever growing amount of other successful strategies. The core idea of TFT is to cooperate for the first stage and then follow the opponent's last move for the coming stage. Before tailoring the TFT strategy for our context and describing how i adjusts its strategy W_i^k according to it, we introduce the following lemma to get a more in-depth insight on the stage payoff U_s.

Lemma 2.1. *For any two players i, j, if $W_i^k > W_j^k$, then it holds that $p_i^k > p_j^k$, $\tau_i^k < \tau_j^k$ and $U_i^s(W^k) < U_j^s(W^k)$.*

Proof. The lemma follows straightforwardly from (2.1), (2.3) noticing that $e \ll g$. □

Now we are ready to introduce the following TFT strategy in our context:

- In each stage k, each player i measures the CW value of any other player j in the last stage[2]
- Set $W_i^k = min_{j \in \mathcal{N}}\{W_j^{k-1}\}$

The engineering implication behind the above TFT strategy is that in non-cooperative environments each rational player is expected to take action to increase its payoff if any other player gets more and will follow the previous action if no player get more payoff than itself. The above introduced TFT strategy in G_{MAC} has the following desirable properties:

- The decision is made solely on local measurement.
- It is simple to implement and only the measurement of the last stage needs to be stored.
- It is especially suitable for wireless networks in that the broadcast nature makes the observation feasible in promiscuous mode.

[1] Throughout the thesis, we use boldface letters (e.g., $\mathbf{a}$) to denote vectors and matrixes. The inequality between two vectors is defined as the inequality in all components of the vectors. We also use $\{a_i\}$ to denote a vector with the ith component being $a_i, i \in \mathcal{N}$.

[2] How to observe the CW values in saturated networks is addressed in [KV03].

- It ensures the fairness among players in that by applying it all players converge to the same CW value, otherwise the players with greater CW values will decrease them according to their measurement in order not to be disfavored. Thus within finite number of stages all players will operate on the same CW value which yields the same utility and throughput.

In practice, taking into account the various factors influencing the measurement, a more tolerant version of the TFT strategy called the Generous TFT strategy (GTFT) can be applied, as shown in the following:

- Each player i measures the CW value of any other player in the last r_0 stages from stage $k - r_0$ to stage $k - 1$ and calculates $\overline{W}_j \triangleq \frac{1}{r_0} \sum_{r=k-r_0}^{k-1} W_j^r, \forall j \in \mathcal{N}$
- If there exists player l such that $\overline{W}_l < \beta \overline{W}_i$, then set $W_i^k = min_{j \in \mathcal{P}}\{\overline{W}_j\}$
- Otherwise set $W_i^k = W_i^{k-1}$

$\beta < 1$ is the tolerance parameter close to 1. By increasing r_0 or decreasing β, the derived GTFT strategy becomes more tolerant.

2.5 Solving the IEEE 802.11 MAC Game G_{MAC}

2.5.1 Nash Equilibrium Analysis

Game theoretic models are often analyzed using the concept of NE, which can be seen as optimal "agreements" between the opponents of the game. The NE concept offers a predictable, stable outcome of a game where multiple agents with conflicting interests compete through self-optimization and reach a point where no player wishes to deviate. However, such an equilibrium point does not necessarily exist. First, we investigate the existence of NE in G_{MAC}.

As discussed in last section, all players converge to the same CW value after sufficient long time. Assume that from the stage t_0, the CW values of all nodes converge to W_c. The transmission probability of all nodes converges to τ_c, i.e., $\tau_i^k = \tau_i = \tau_c$ for all $i \in \mathcal{N}$ when $k \geq t_0$. The utility function of i can be expressed as a function of τ_i:

$$U_i = \sum_{k=0}^{+\infty} \delta^k U_i^k T = \sum_{k=0}^{t_0-1} \delta^k U_i^k T + \sum_{k=t_0}^{+\infty} \delta^k U_i^k T = \sum_{k=0}^{t_0-1} \delta^k U_i^k T + \frac{\delta^{t_0} T}{1-\delta} \frac{\tau_i[(1-p_i)g - e]}{T_{slot}}.$$

Noticing that in our study, δ is close to 1 for long-sighted players, we can ignore $\sum_{k=0}^{t_0-1} \delta^k U_i^k T$ in the utility function. After some mathematic operations calculating T_{slot}, we obtain

$$U_i(\tau_i) = \frac{\delta^{t_0} T}{1-\delta} \frac{\tau_i \prod_{j=1, j\neq i}^{n} (1-\tau_j) g - \tau_i e}{\prod_{j=1}^{n}(1-\tau_j)\sigma + \sum_{j=1}^{n} \tau_j \prod_{k=1, k\neq j}^{n} (1-\tau_k)(T_s - T_c) + \left[1 - \prod_{j=1}^{n}(1-\tau_j)\right] T_c}. \quad (2.4)$$

The following lemma studies the basic structural property of U_i.

Lemma 2.2. *Let* $\Gamma_c \triangleq \{\tau_i = \tau_c, \forall i \in \mathcal{N}\}$*, it holds that* $U_i(\Gamma_c)$ *admits a unique maximizer* $\tau_c = \tau_c^*$ *and* $0 < \tau_c^* < 1$*. Moreover,* U_i *is monotonously increasing in* τ_c *before it is maximized and monotonously decreasing after that.*

Proof. Please refer to Section 2.10.1 for the detailed the proof. □

Noticing the relation between W_c and τ_c, we have the following lemma.

Lemma 2.3. *Let* $\mathbf{W_c} \triangleq \{W_i = W_c, \forall i \in \mathcal{N}\}$ *and regard* U_i *as a function of* W_c*, it holds that* $U_i(\mathbf{W_c})$ *admits a unique positive maximizer* $W_c = W_c^*$*. Moreover,* U_i *is monotonously increasing in* W_c *before it is maximized and monotonously decreasing after that.*

Proof. It follows from (2.1) that $\frac{\partial \tau_c}{\partial W_c} < 0$. Noticing that $\frac{\partial U_i}{\partial W_c} = \frac{\partial U_i}{\partial \tau_c}\frac{\partial \tau_c}{\partial W_c}$, Lemma 2.3 is proven. □

The following theorem characterizes the NEs of G_{MAC}.

Theorem 2.1. *Let* $\mathbf{W_c^0} \triangleq \{W_c^0\}$ *where* $U_i(W_c^0, \cdots, W_c^0) > 0$ *and* $U_i(W_c^0 - 1, \cdots, W_c^0 - 1) < 0$*, any strategy profile* $\mathbf{W_c} = \{W_c\}$ *satisfying* $W_c^0 \leq W_c \leq W_c^*$ *consists of a NE of* G_{MAC}*.*

Proof. The proof consists of showing that no player has incentive to deviate from W_c. Please refer to Section 2.10.2 for the detailed proof. □

Recall the assumption $e \ll g$, we have $U_i(\{W_c^*\}) > 0$. It follows from Theorem 2.1 that G_{MAC} has $(W_c^* - W_c^0 + 1)$ NEs. Usually not all of them are good. Our next step is to remove those NEs that are less less efficient to achieve a socially desirable result. This is achieved by the NE refinement elaborated in the next subsection.

2.5.2 Nash Equilibrium Refinement

In this subsection, we perform NE refinement by imposing the following optimality criteria: *fairness*, *social optimality* and *Pareto optimality*.

- *Fairness*: It is clear that all the NEs $\mathbf{W_c}$ ensure fairness among players due to the TFT strategy in that each player chooses the same CW value and gets the same payoff after the convergence.
- *Social Optimality*: A social optimal strategy profile maximizes the global payoff. Among the NEs, Lemma 2.3 shows that $\{W_c^*\}$ maximizes both individual payoff U_i and the global payoff $\sum_{i \in \mathcal{P}} U_i = nU_i$. In fact it is the only NE maximizing the global payoff.
- *Pareto Optimality:* It is easy to check that $\{W_c^*\}$ is the only Pareto optimal NE. All other NE are not Pareto optimal in that for any $W_c \neq W_c^*$, $U_i(\{W_c\}) < U_i(\{W_c^*\})$.

The NE refinement leads to a unique efficient NE $\{W_c^*\}$ maximizing both local and global payoff.

2.5.3 Approaching the Efficient Nash Equilibrium

In this section, we address the issue on how to reach the efficient NE $\{W_c^*\}$. If the number of the nodes n in the network is known to players, the task becomes trivial in that the CW value of the efficient NE can be computed given n[3]. In many cases, the network participants do not know the number of nodes in the network, so they cannot directly calculate W_c^*. In this subsection, we provide a simple algorithm to approach to the efficient NE without the knowledge of n.

The core idea of the proposed algorithm is that one node l starts the search and then all nodes search for the CW value that maximizes l's payoff under the condition that they operate on the same CW value. According to the previous analysis, this value is W_c^*. We would like to point out here that the algorithm requires all players to act cooperatively. This does not contradict to the selfish nature of players in that players are selfish in the sense that their goal is to maximize their own payoff, thus they have incentive to act cooperatively to reach the efficient NE maximizing both their own payoff and the global payoff.

Algorithm 1 Approaching the efficient Nash Equilibrium $\{W_c^*\}$

1: Any node l sends a message Start-Search containing the CW value of the starting point $W_l = W_0$ and starts the search.

2: Right-Search: l increases W_l by 1 and sends a message Ready including the new W_l. Other nodes set their CW values to W_l when receiving the message Ready.

   l waits a short period of time t for others to change their CW values and measures its payoff in the following t_m time. The payoff can be calculated as follows: $\overline{U_l} = (n_s g - n_e e)/t_m$, where n_s is the number of packets successfully emitted, n_e is the number of packets emitted. If the payoff is greater than the last measured payoff with the old W_l, l continues the search until the payoff decreases. l notes the last CW value W_m before decreasing.

3: Left-Search: If $W_m \neq W_0 + 1$, skip Left-search. Otherwise l decreases W_l by 1 and sends the message Ready including the new W_l. Others set their CW values to W_l when receiving the message Ready.

   l waits a short period t of time for other nodes to change their CW values and measures its payoff in the following t_m time. If the payoff is greater than the last measured payoff, l continues the search until the payoff decreases. l notes the last CW value W_m before decreasing.

4: l broadcasts W_m as the CW value of the efficient NE.

Remark 1: In the proposed algorithm, one may ask what is the consequence if l broadcasts $W'_m \neq W_m = W_c^*$ while operates on W_c^* itself. Actually l has no incentive to broadcast $W_m < W_c^*$ since this will lead the players to operate on W_m according to the TFT strategy. As a result, l gets less payoff compared with the case where it reports W_c^* and operates on W_c^*. If l broadcasts $W_m > W_c^*$ while operating on W_c^*, the CW values will converge to W_c^*. The only benefit of l is that it may get certain amount of payoff before the convergence. However, for long-sighted players, the payoff obtained before the convergence is negligible compared with the total payoff.

Remark 2: The analysis up to now neglects the cases where W_c^* is not an integer. In such cases, if $U_i(\{\lfloor W_c^* \rfloor\})$[4] $= U_i(\{\lfloor W_c^* \rfloor + 1\})$, then G_{MAC} has two efficient NEs $\{\lfloor W_c^* \rfloor\}$ and $\{\lfloor W_c^* \rfloor + 1\}$. Algorithm 1 will find one of them. If $U_i(\{\lfloor W_c^* \rfloor\}) \neq U_i(\{\lfloor W_c^* \rfloor + 1\})$, then G_{MAC} has one efficient NE $\{\lfloor W_c^* \rfloor\}$ if $U_i(\{\lfloor W_c^* \rfloor\}) > U_i(\{\lfloor W_c^* \rfloor + 1\})$ and $\{\lfloor W_c^* \rfloor + 1\}$ otherwise. Algorithm 1 will find the

[3] W_c^* can be solved by combining the equation $Q(\tau_c) = 0$ in the proof of Lemma 2.3 with (2.1).
[4] $\lfloor W_c^* \rfloor$ denotes the largest integer not larger than W_c^*.

unique efficient NE in this case.

2.5.4 Impact of Short-sighted (Myopic) Players

In previous sections a basic assumption is that all players are long-sighted ($\delta \to 1$). In this section we relax this assumption to study the impact of short-sighted players on the network performance. We first introduce the following lemma as the basis of the analysis in this subsection.

Lemma 2.4. *Let* $\mathbf{W} \triangleq \{W\}$ *and* $\mathbf{W}'$ *denote the strategy profile in which player* i *deviates from* W *to* W'*, while other players stick to* W*, it holds that*

1. $W' > W \Longrightarrow U_i^s(\mathbf{W}') < U_i^s(\mathbf{W}) < U_j^s(\mathbf{W}'),\ \forall j \in \mathcal{N}, j \neq i;$
2. $W' < W \Longrightarrow U_j^s(\mathbf{W}') < U_i^s(\mathbf{W}) < U_i^s(\mathbf{W}'),\ \forall j \in \mathcal{N}, j \neq i.$

Proof. Please refer to Section 2.10.3 for the detailed proof. □

We consider the scenario where there is one short-sighted player s with the discount factor δ_s. s operates on $W_s < W_c^*$ rather than W_c^* to get more payoff.

We also assume that other nodes need m stages ($m \geq 1$) to react according to the TFT/GTFT strategy to set their CW value to W_s. Thus the game G_{MAC} in this new context becomes the following: in the first m stages s operates on W_s while others on W_c^*; in the following stages, all players operate on W_s. Thus the payoff of s is:

$$\begin{aligned} U_s &= \sum_{r=0}^{m-1} U_s^s(W_c^*, \cdots, W_s, \cdots, W_c^*) + \sum_{r=m}^{\infty} U_s^s(W_s, \cdots, W_s) \\ &= \frac{1}{1-\delta_s}\Big[(1-\delta_s^m)U_s^s(W_c^*, \cdots, W_s, \cdots, W_c^*) + \delta_s^m U_s^s(W_s, \cdots, W_s)\Big]. \end{aligned}$$

On the other hand, if s operate on W_c^* for all stages, its payoff is:

$$U_s' = \frac{U_s^s(W_c^*, \cdots, W_c^*)}{(1-\delta_s)}.$$

We consider the following two cases:

- If s is extremely short-sighted, we have $\delta_s \to 0$, then according to Lemma 2.4, we have

$$W_s < W_c^* \longrightarrow U_s^s(W_c^*, \cdots, W_s, \cdots, W_c^*) > U_s^s(W_c, \cdots, W_c).$$

  Noticing $\delta_s \to 0$, it follows that $U_s > U_s'$. Hence by operating on W_s, s gets more payoff at the expense of others and the sub-optimality of the network as a whole.

- If s is long-sight ($\delta_s \to 1$), then it will choose W_s to maximize $\delta_s^m u_s(W_s, \cdots, W_s)$ where W_c^* is the unique maximizer.

Generally, given δ_s, s can configure W_s to maximize its payoff by imposing $\dfrac{\partial U_s}{\partial W_s} = 0$. To conclude, a short-sighted player has negative impact on the network as it can degrade the performance or even lead to network collapse.

2.5.5 Impact of Malicious Players

Unlike selfish players, the malicious players aim at collapsing the network. Hence they have no incentive to operate on the efficient NE W_c^*. To this end, they will surely deviate from W_c^* to fulfill their goal.

We consider the scenario where malicious player i operates on $W_i < W_c^*$. Under this condition, other players will decrease their CW values to W_i based on the TFT strategy. As consequence, the network performance is degraded as the global payoff decreases. If W_i is sufficiently small, the network is paralyzed.

2.5.6 RTS/CTS Case

Our analysis for basic case is also applicable in the RTS/CTS case. What differs in the RTS/CTS case is that collisions occur on RTS frames, thus

$$\begin{cases} T_s' = RTS + SIFS + CTS + H + P + SIFS + ACK + DIFS \\ T_c' = RTS + DIFS \end{cases}.$$

By performing the same analysis as the basic case, we derive the same results for RTS/CTS case.

2.6 Multi-hop Case

In this section, we extend our previous work to multi-hop wireless networks. More specifically, we consider a connected multi-hop wireless network operating under the RTS/CTS access mechanism. We assume that network nodes know the number of neighbor nodes[5].

2.6.1 Model Adaptation

We need to modify the model on selfish nodes derived in Section 2.3 to extend it to multi-hop case. First, under the assumption that the channel states sensed by the neighbors of a node is the same as that sensed by the node, we can rewrite the second equation in (2.1) as

$$p_i \approx 1 - \prod_{j \in M_i, j \neq i} (1 - \tau_j), \tag{2.5}$$

where M_i denotes the neighbor set of i.

We then modify the utility function as following to take into account the hidden-node problem of multi-hop wireless networks:

$$u_i = \frac{\tau_i[(1-p_i)p_{hn}^i u_i - e_i]}{T_{slot}},$$

where p_{hn}^i is the degradation factor indicating that $1 - p_{hn}^i\%$ of transmitted packets experience collisions at the receivers due to the hidden-node problem. The stage and total utility function is derived in the same way as single-hop case. A key approximation in our model is that p_{hn}^i is independent of the CW values of players. We will show in next section via simulation that this approximation is accurate when n is large enough and CW values are not too small. Note that we cannot solve p_i in multi-hop case without the knowledge of the network topology. However, as

[5]The neighbor information can typically be obtained via routing protocols or MAC layer beacons

shown in the following demonstration, we can still establish the NE of the game in the multi-hop case using the adapted model, which is our goal.

2.6.2 Formulating and Solving the Game

The non-cooperative IEEE 802.11 MAC game in the multi-hop case, denoted as G'_{MAC}, can be formulated in the same way as its counterpart in the single-hop case G_{MAC}. However, it is obvious that the solution of G_{MAC} is no more applicable for G'_{MAC}. Nevertheless, as long as players in G'_{MAC} follow the TFT strategy, their CW values will converge to the smallest one of all players after sufficiently long time although the converged value may not be optimal for all players. This can be shown intuitively: consider player s operates on the smallest CW value W_s. The neighbor of s will decrease their CW values to W_s if they operate on higher values according to the TFT strategy. Once their CW values are decreased, they have no incentive to increase it any more. Then the CW values of the two-hop neighbors of s will converge to W_s. As a result, as long as the network is not partitioned, the CW values of all players will converge to W_s after sufficiently long time.

In multi-hop case, it is not possible to apply Algorithm 1 to reach an equilibrium point due to the fact that the optimal CW value of l may not be optimal for other players. Thus they have no incentive to operate on this CW value or will not even participate in the search. Instead, any player i relies solely on local information to choose its CW value W_i. Under such circumstance, a natural way is to choose the initial value of W_i that maximizes its payoff assuming its neighbors also operate on W_i and to follow the TFT strategy in following stages. Taking into consideration the approximation that p^i_{hn} is independent of CW values and $g \gg e$, W_i is obtained by maximizing $\frac{\tau_i(1-p_i)u_i}{T_{slot}}$, which is the same utility function in the single-hop game G_{MAC} analyzed previously. Hence, W_i is set to the CW value at the efficient NE of the single-hop game G_{MAC} in which the players are i and its neighbors[6]. The result is not surprising in that in multi-hop environments without coordination among nodes, the best strategy for a rational player is to operate on local optimal point based on local information. Under this circumstance, after sufficient long time, the CW value will converge to $W_m = \min_{i \in \mathcal{N}} W_i$. In the following theorem we prove that all players operating on W_m constitutes of a NE of G'_{MAC}.

Theorem 2.2. *In G'_{MAC}, the CW values of all players converge to $W_m = min_{i \in \mathcal{N}} W_i$, where W_i is i's CW value at the efficient NE of the single-hop game G_{MAC} in which the players are i and its neighbors. It holds that $\mathbf{W_m} = \{W_m\}$ is a NE of G'_{MAC}.*

Proof. Please refer to Section 2.10.4 for the detailed proof. □

Furthermore it can be shown that the above NE is Pareto optimal, but not necessarily globally optimal. Nevertheless, we will show in next section via simulation that the NE is quasi-optimal in the sense that the global payoff is only slightly outweighed by the optimal case and the fairness of the NE is ensured in the sense that each player gets almost the same payoff as the maximum payoff it can get.

[6]Here we implicitly assume that if node i and its neighbor nodes operate on the same CW values, they have the same collision probability p_i. This assumption is accurate if n is sufficiently large and the density of the network does not vary too much.

2.7 Numerical Results

In this section we present the numerical results on our game theoretic model. The network parameters are listed in Table 2.1.

2.7.1 Single-hop Case

We first study the efficient NE when the CW value of all players is converged. We conduct simulation in NS-2 and compare simulation results with our analytical results. Table 2.2 and 2.3 show the main results in which W_c^* is the efficient NE according to our theoretic model, $\overline{W_c^*}$ is the average CW values of each node that maximizes its own payoff in the simulation, $Var(W_c^*)$ is the variance of W_c^*. We can see that in both cases, the simulation results coincide with the analytical results quite well.

Packet size	8184 bits
MAC header	272 bits
PHY header	128 bits
ACK	112 bits + PHY header
RTS	160 bits + PHY header
CTS	112 bits + PHY header
Channel bit rate	1 Mbits/s
σ	$50\mu s$
SFIS	$28\mu s$
DIFS	$128\mu s$
g	1
e	0.01
T	10s
δ	0.9999
Simulation time	1000s

Table 2.1: Network parameters

n	W_c^*	$\overline{W_c^*}$	$Var(W_c^*)$
5	79	78.4	3.41
20	342	343.4	2.92
50	886	888.7	2.72

Table 2.2: NE: basic case

n	W_c^*	$\overline{W_c^*}$	$Var(W_c^*)$
5	23	23.7	1.57
20	50	49.2	1.79
50	121	119.4	1.71

Table 2.3: NE: RTS/CTS case

We also plot the global payoff as a function of CW values base on our model in Figure 2.1, where the Y-axis is U/C where U denotes the global payoff and $C = \dfrac{gT}{\sigma(1-\delta)}$ is a constant. From the results, especially the CTS/RTS case, we can see that operating at W_c^* also achieves the global social optimality. Furthermore, the efficient NE is quite robust in the sense that the CW values near W_c^* yield almost the same global and local payoff. Consequently, a rational players should be satisfied as long as it operates not too far from W_c^*. This robust and tolerant feature may significantly facilitate the design and implementation of TFT/GTFT strategy and the algorithm to reach W_c^*.

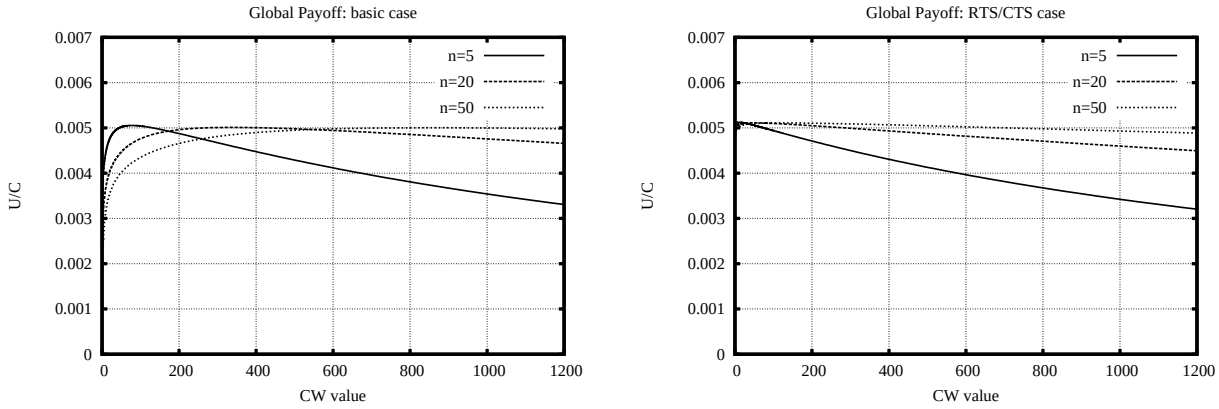

Figure 2.1: Global payoff versus CW value, left: basic case; right: RTS/CTS case

2.7.2 Multi-hop Case

We simulate for 1000s a network of 100 nodes with the same transmission range of 250m moving at a speed randomly picked from [0,5m/s] according to the random way-point model in a 1000m×1000m area. Each node has information of its neighbors from which it calculates the local optimal CW value.

We simulate the converged case by setting the converged CW value to the smallest one among the nodes. This value, 29 in our scenario, is the NE according to our analytical model. We then vary CW values to simulate both local and global payoff and compare the results with that at NE. We report that operating at NE, each node gets at least 96% of the maximal local payoff it can get by varying its CW value and the global payoff is only 3% less than the maximal global payoff. We also observe from the simulation that both the local and global payoff in RTS/CTS case is almost independent with respect to CW values when n is large enough in both single-hop and multi-hop cases. This independence justifies our key approximation in Section 2.6.1.

The above numerical results show that selfishness leads to a NE which is at least quasi-optimal if not optimal in the sense that the both local and global payoff is only slightly outweighed by the optimal case.

2.8 Discussion

In the section of Related Work, we mentioned that [CGAH05] shows the existence of even a small population of selfish nodes leads to network collapse. Their results seem contradictory to ours. In fact their results are coherent to ours. The point is that in their work, the players are selfish and short-sighted, thus they set their CW values to small values to maximize the short-term payoff. In our work, we provide a more generic analysis in both single-hop and multi-hop networks: we first assume that the players are selfish and long-sighted and show that selfishness does not lead to network collapse; we then study the impact of the short-sighted players on the network performance in Section 2.5.4 and obtain the same result as [CGAH05].

In our work, we choose a generic utility function and do not take into account the packet delay and other factors. As a result, the CW value of NE may seem too long in some cases. To derive a more desirable NE, more factors need to be considered depending on the target application and

other requirements.

2.9 Conclusion

In this chapter, we focus on the posed question: how well or how bad does IEEE 802.11 DCF perform if all nodes are selfish? We proceed our analysis under a non-cooperative game theoretic framework. Our main results are as follows:

- In single-hop wireless networks, selfishness does not always lead to network collapse. On the contrary, it can help network operate at an efficient NE which is also global optimal under the condition that players are long-sighted and follow the TFT strategy.
- We provide a simple algorithm to approach the efficient NE.
- In multi-hop case, under the same condition, the network operates on a NE not necessarily globally optimal. However, we show by numerical results that the NE is quasi-optimal in the sense that the global payoff is only slightly less than the optimal case.

Furthermore, we believe that the game theoretic model proposed in this chapter is a general framework that can be extended to model other selfish behaviors such as rate control by redefining the proper utility function.

2.10 Proofs

This section completes the detailed proofs omitted from the main text.

2.10.1 Proof of Lemma 2.2

Injecting Γ_c into (2.4), recall the assumption $e \ll g$, we can derive $U_i(\Gamma_c)$ for $\tau_c > 0$ as

$$\begin{aligned} U_i(\Gamma_c) &= \frac{\tau_c(1-\tau_c)^{n-1}g - \tau_c e}{(1-\tau_c)^n\sigma + n\tau_c(1-\tau_c)^{n-1}(T_s - T_c) + [1-(1-\tau_c)^n]T_c} \\ &\simeq \frac{\tau_c(1-\tau_c)^{n-1}g}{(1-\tau_c)^n\sigma + n\tau_c(1-\tau_c)^{n-1}(T_s - T_c) + [1-(1-\tau_c)^n]T_c} \\ &= \frac{g}{n(T_s - T_c) + \dfrac{(1-\tau_c)^n\sigma + [1-(1-\tau_c)^n]T_c}{\tau_c(1-\tau_c)^{n-1}}} \end{aligned}$$

After some straightforward mathematic manipulations, $\dfrac{\partial U_i}{\partial \tau_c}$ can be calculated as

$$\frac{\partial U_i}{\partial \tau_c} = \frac{g\left\{(1-\tau_c)^n\sigma - [n\tau_c + (1-\tau_c)^n]T_c + T_c\right\}}{\left\{n(T_s - T_c) + \dfrac{(1-\tau_c)^n\sigma + [1-(1-\tau_c)^n]T_c}{\tau_c(1-\tau_c)^{n-1}}\right\}^2 \tau_c^2(1-\tau_c)^n}$$

Let $Q(\tau_c) \triangleq (1-\tau_c)^n\sigma - [n\tau_c + (1-\tau_c)^n]T_c + T_c$, we have

$$Q'(\tau_c) = -(n-1)(1-\tau_c)^{n-1}\sigma - T_c n + (n-1)(1-\tau_c)^{n-1}T_c < -T_c n + T_c(n-1) < 0$$

Hence, $Q(\tau_c)$ is monotonously decreasing in τ_c. Noticing that $Q(0) = \sigma > 0$ and $Q(1) = -(n-1)T_c < 0$, there exists a unique $0 < \tau_c^* < 1$ satisfying $Q(\tau_c^*) = 0$ and $\left.\frac{\partial U_i}{\partial \tau_c}\right|_{\tau_c=\tau_c^*} = 0$. Moreover, for $\tau_c < \tau_c^*$, both $Q(\tau_c)$ and $\frac{\partial U_i}{\partial \tau_c}$ is positive, U_i is monotonously increasing in τ_c; for $\tau_c > \tau_c^*$, both $Q(\tau_c)$ and $\frac{\partial U_i}{\partial \tau_c}$ is negative, $U_i(\Gamma_c)$ is monotonously decreasing. Hence, τ_c^* is the unique maximizer of $U_i(\Gamma_c)$.

2.10.2 Proof of Theorem 2.1

We prove the theorem by showing that no player has incentive to deviate from $W_c^0 \le W_c \le W_c^*$.

- If any player i increases its CW value to $W_c' > W_c$, it will get less payoff[7] and set its CW value back to W_c according to the TFT strategy.
- On the other hand, if i decreases its CW value to $W_c' < W_c$, other players will react by decreasing their CW values to W_c' based on the TFT strategy, leading to the decrease of the payoff for all players including i in the following stages due to the fact that U_i is monotonously increasing in W_c before W_c^*. Recall the assumption that the players are long-sighted, the decrease of payoff in the following stages, as will be shown in Section 2.5.4 in a similar scenario, outweighs the gain obtained during the stages when i operates on W_c' while others on W_c. Thus i gets less overall payoff by decreasing its CW value from W_c.

We then show that any strategy profile $\{W_c\}$ with $W_c < W_c^0$ or $W_c > W_c^*$ is not a NE of G_{MAC}.

- Operating on $\{W_c\}$ where $W_c < W_c^0$ leads to a negative payoff noticing that $U_i^s(\{W_c\}) \le U_i^s(\{W_c - 1\}) < 0$ (Lemma 2.3), hence any player is better off setting its CW value to $+\infty$, indicating that $\{W_c\}$ cannot be a NE.
- For $\{W_c\}$ where $W_c > W_c^*$, from Lemma 2.4, any player gets more payoff by decreasing its CW value to W_c^*, hence $\{W_c\}$ cannot be a NE.

Combining the above analysis concludes our proof.

2.10.3 Proof of Lemma 2.4

It follows from (2.1) that

$$\begin{cases} W' > W \Longrightarrow \tau_i' < \tau_i = \tau_j = \tau_j' \\ W' < W \Longrightarrow \tau_i' > \tau_i = \tau_j = \tau_j' \end{cases}.$$

[7] This is formally proved in Lemma 2.4. Since the results of Lemma 2.4 are also used in Section 2.5.4, we present the lemma there in the main text to maintain the presentation continuity and clarity.

Noticing that under the condition $e \ll g$, U_s can be rewritten as follows:

$$\begin{aligned} U_s &= \frac{\tau_i \prod_{j=1,j\neq i}^{n}(1-\tau_j)g - \tau_i e}{\prod_{j=1}^{n}(1-\tau_j)\sigma + \sum_{j=1}^{n}\tau_j \prod_{k=1,k\neq j}^{n}(1-\tau_k)(T_s - T_c) + \left[1 - \prod_{j=1}^{n}(1-\tau_j)\right] T_c} \\ &= \frac{g}{\sum_{j\in\mathcal{N}} \frac{\tau_j(1-\tau_i)}{\tau_i(1-\tau_j)}(T_s - T_c) + \sigma\frac{1-\tau_i}{\tau_i} + \frac{\left[1 - \prod_{j=1}^{n}(1-\tau_j)\right] T_c}{\tau_i \prod_{j=1,j\neq i}^{n}(1-\tau_j)}}, \end{aligned}$$

we have:

$$\begin{cases} U_i^s(\mathbf{W}) = \dfrac{g}{n(T_s - T_c) + \dfrac{1-\tau_i}{\tau_i}\sigma + \dfrac{[1-(1-\tau_i)^n]T_c}{\tau_i(1-\tau_i)^{n-1}}} \\ U_i^s(\mathbf{W}') = \dfrac{g}{\left[1 + (n-1)\dfrac{\tau_j'(1-\tau_i')}{\tau_i'(1-\tau_j')}\right](T_s - T_c) + \dfrac{1-\tau_i'}{\tau_i'}\sigma + \dfrac{[1-(1-\tau_i')(1-\tau_j')^{n-1}]T_c}{\tau_i'(1-\tau_j')^{n-1}}} \\ U_j^s(\mathbf{W}') = \dfrac{g}{\left[(n-1) + \dfrac{\tau_i'(1-\tau_j')}{\tau_j'(1-\tau_i')}\right](T_s - T_c) + \dfrac{1-\tau_j'}{\tau_j'}\sigma + \dfrac{[1-(1-\tau_i')(1-\tau_j')^{n-1}]T_c}{\tau_j'(1-\tau_i')(1-\tau_j')^{n-2}}} \end{cases} . \quad (2.6)$$

In IEEE 802.11 DCF, it holds that $T_s > T_c$. It then follows from (2.6) that

$$\begin{cases} W' > W \Longrightarrow \tau_i' < \tau_i = \tau_j = \tau_j' \Longrightarrow U_i^s(\mathbf{W}') < U_i^s(\mathbf{W}) < U_j^s(\mathbf{W}') \\ W' < W \Longrightarrow \tau_i' > \tau_i = \tau_j = \tau_j' \Longrightarrow U_i^s(\mathbf{W}') > U_i^s(\mathbf{W}) > U_j^s(\mathbf{W}') \end{cases},$$

which concludes our proof.

2.10.4 Proof of Theorem 2.2

We prove the theorem by showing that any node j has no incentive to deviate from W_m. If W_m is node j's efficient NE of local single-hop game, it is clear that j has no incentive to deviate from W_m. In other cases, j has no incentive to increase its CW value in that it will be dragged back to W_m according to the TFT strategy when j meets players operating on W_m; If j decrease its CW value to $W_j' < W_m$, then according to the TFT strategy, other nodes also decrease their CW values to W_j'. It follows from Lemma 2.3 that under the condition that all players choose the same CW value, the payoff of j is monotonously increasing until it is maximized at W_j. Since $W_j' < W_m = \min_{i\in\mathcal{N}} W_i < W_j$, the payoff of j operating on W_j' is less than that on W_m. Hence j has no incentive to decrease its CW value from W_m to W_j'. $\mathbf{W_m}$ is thereby a NE of G'_{MAC}.

Chapter 3

Non-cooperative Distributed Power and Rate Control in IEEE 802.11 WLANs

3.1 Introduction

In today's wireless networks, most network nodes, such as laptops, PDAs and palmtops, are battery powered and thus limited in their energy supply. Therefore, it is natural and important for selfish nodes to adopt the most energy-efficient transmission strategy. In this chapter, we investigate such selfish behavior in IEEE 802.11 WLANs that network participants choose their transmission power and data rate in a non-cooperative (selfish) way to maximize their own throughput with minimum energy consumption.

3.1.1 Background and Motivation

Such power and rate control problem have been widely investigated in cellular networks under both optimization and game theoretic frameworks [SMG02a], [ABD06], [HA04], [Yat95]. The seminal paper [SMG02a] studies the power control in a single-cell CDMA network and introduces pricing to improve the efficiency of the equilibrium, but even with pricing, the game is still unable to achieve a socially optimum solution. [HA04] addresses the joint power and rate control in CDMA networks and models the problem as two games. All nodes first find the data rate and then apply power control to allocate the powers.

In the context of IEEE 802.11 WLANs using contention based medium access mechanism, the power and rate control problem is by nature different in that:

- In cellular networks, the transmission of one node interferes those of others, but IEEE 802.11 WLANs[1] are interference-free environments where there is no interference during a successful transmission.
- The contention based medium access control of IEEE 802.11 creates an important feature which we refer to as *data rate interference* that does not exist in cellular networks, i.e., the data rate (PHY layer) of one node not only determines its own throughput (MAC layer), but also influences the throughput of others, as will be shown in Section 3.2.1.

[1] In our work, we consider the single hop, single channel case.

Therefore, there is a need for a quantitative model for the power and rate control in such environments as IEEE 802.11 WLANs.

There exist a number of power control and rate adaptation mechanisms proposed for IEEE 802.11 WLANs to achieve high performance at lower level of energy consumption, [HVB01], [QCJS03]. However, most of them rely on simulation and experimental results. To our knowledge, very little work has been done on modeling the power and rate control in IEEE 802.11 WLANs although the problem in this context is by nature different from that in cellular networks. Among them, [TG05] shows that in a non-cooperative environment under IEEE 802.11 DCF (Distributed Coordination Function), a selfish node may achieve higher throughput by transmitting at lower data rate at the expense of reducing overall network throughput. In [TG05], the energy consumption is not taken into account when maximizing the node's throughput. [EAV05] restudies the problem using both cooperative and non-cooperative approach. The emphasis is on the cooperative control and little analysis is done on the non-cooperative control. Our previous work [CL07b] studies rate control assuming that power consumption can be approximated by a linear function of the data rate. However, this assumption does not hold in general case. None of them performs a profound study on the power and rate control for IEEE 802.11 WLANs based on a well-established model.

3.1.2 Summary of Contributions

In this chapter, motivated by the need of a quantitative model for the power and rate control in IEEE 802.11 WLANs and the lack of related work in the literature, we address the problem by establishing a quantitative game theoretic framework. Our motivation of using game theoretic approach rather than global optimization approach is two-fold:

- Game theory is a powerful tool to model selfish behaviors and their impact on the system performance in distributed environments with self-interested players.
- Game theory can model the features or constraints of IEEE 802.11 WLANs such as lack of coordination and network feedback.

In fact in such environments, due to the distributed nature, selfish behavior is much more robust and scalable than any centralized cooperative control, which is very expensive or even impossible to implement.

We investigate three specific games in this chapter. In G_{NPC} and G_{NRC}, players choose their transmission power/rate under fixed transmission rate/power to maximize their payoff. These two games correspond to the classical power control and rate adaptation problem, respectively. In the third game G_{NJPRC}, we address the general case, joint power and rate control, where players can adjust both data rate and transmission power. For the three games, a Nash equilibrium (NE) is defined as a set of strategies at which no player can improve its utility by deviating unilaterally.

In our work, we are interested in the following questions. Do there exist NEs for the three games (existence of NE)? If so, is it unique and can players converge to the NE (uniqueness and convergence to NE)? Moreover, is the NE efficient (social optimality at NE)? If not, how to improve the efficiency? Our work contributes to existing literature as follows:

- *Game theoretic framework:* We establish a game theoretic model for the power and rate control in IEEE 802.11 WLANs, based on which we study the existence, uniqueness and

convergence of the NE for the three games. In G_{NRC} where the NE is inefficient, we provide a pricing scheme to improve the efficiency.

- *Joint power and rate control procedure:* We propose a joint power and rate control procedure to approach the NE of G_{NJPRC} which is proven to be social optimal. The procedure is distributed in nature and can be incorporated into the IEEE 802.11 MAC protocol easily.

3.2 Problem Formulation

3.2.1 IEEE 802.11 Medium Access Control

We consider a saturated IEEE 802.11 WLAN of n nodes, denoted as $\mathcal{N}$, using IEEE 802.11 DCF with RTS/CTS dialog as the MAC layer protocol. Recent work of Kumar et al. [KAMG05] has shown that (under decoupling assumptions) the IEEE 802.11 DCF can be modelled by the following fixed point equation

$$\begin{cases} \theta = 1 - (1-\tau)^{n-1} \\ \tau = \dfrac{1 + \theta + \cdots + \theta^K}{b_0 + b_1\theta + \cdots + b_K\theta^K} \end{cases},$$

where θ is the collision probability observed by a given node, τ is the transmission attempt probability, $b_i = \min\left\{\dfrac{2^i CW_{min}+1}{2}, \dfrac{CW_{max}+1}{2}\right\}$.

Applying the above model, assuming that all nodes use the same back-off parameters and the packets are of the same size L, the expected throughput of node i can be calculated as

$$S_i = \frac{\tau(1-\tau)^{n-1}L}{T_{slot}} = \frac{\tau(1-\tau)^{n-1}L}{1 + n\tau(1-\tau)^{n-1}(T_o - T_c + \frac{1}{n}\sum_{j=1}^{n}\frac{L}{C_j}) + (1-(1-\tau)^{n-1})T_c}, \quad (3.1)$$

where T_{slot} is the average virtual slot length, C_i is the data rate of i. T_o is the transmission overhead in slots (SIFS/DIFS, etc), T_c is the fixed overhead for an RTS collision. (3.1) shows clearly that the contention based medium access control creates the data rate interference: the data rate of node i C_i not only determines its own throughput S_i, but also influences the throughput of other nodes $j \neq i$. In other words, node i's throughput depends not only on its own data rate C_i, but also on the data rate of other network participants C_j. Note that (3.1) can be extended to basic access cases by modifying T_o and T_c.

Furthermore, let P_s denote the frame success rate (FSR), the probability of correct reception of a frame at its destination. The effective throughput of i S_i^{eff} can be expressed as $S_i^{eff} = P_s S_i$. Assuming perfect error detection and no error correction, we have $P_s = (1-P_e)^L$, where P_e is the bit error rate (BER). P_e is a function of E_b/N_0, the bit-energy-to-noise ratio of the received signal. Typical P_e for different modulation schemes are shown in Table 3.1. Assuming an additive white Gaussian noise (AWGN) channel, in our context, the bit-energy-to-noise ratio of i $\left(\dfrac{E_b}{N_0}\right)_i$ of the received signal is derived from the SNR (Signal-to-Noise Ratio) as follows:

$$\left(\frac{E_b}{N_0}\right)_i = SNR\frac{B_t}{C_i} = \frac{h_i P_i}{\sigma^2}\frac{B_t}{C_i} = \frac{h_i B_t}{\sigma^2}\frac{P_i}{C_i},$$

where C_i is the bit rate of the modulation scheme and B_t is the unspread bandwidth of the signal,

P_i is the transmission power of i, h_i is the channel gain from the sender i to the receiver and σ^2 is the AWGN power at the receiver. Let $\gamma_i \triangleq \frac{h_i B_t}{\sigma^2}\frac{P_i}{C_i}$, we can express the FSR of i as a function of γ_i: $P_s = f_i(\gamma_i)$

In our work, in order to perform a closed-form analysis on the power and rate control, we assume that each user applies the non-coherent FSK modulation scheme where $f_i(\gamma_i) = f(\gamma_i) = \left(1 - \frac{1}{2}e^{-\gamma_i/2}\right)^L$. However, our analysis is applicable for other forms of $f(\gamma_i)$.

Modulation	BER (P_e)
BPSK	$Q(\sqrt{2E_b/N_0})$
DPSK	$\frac{1}{2}e^{-E_b/N_0}$
Coherent FSK	$Q(\sqrt{E_b/N_0})$
Non-coherent FSK	$\frac{1}{2}e^{-E_b/2N_0}$

Table 3.1: BER (P_e) for various modulation schemes

Generally, we observe the following features on $f(\gamma_i)$ which is easy to check.

Lemma 3.1. *For the FSR function $f(\gamma_i)$, if L is sufficiently large, it holds that*

- $f(0) \to 0$, $f(\infty) \to 1$. $f(\gamma_i)$ *is monotonously increasing w.r.t* γ_i;
- $f'(0^+) \to 0$, $f'(\infty) \to 0$, $f'(\gamma_i)$ *has a unique maximizer* $\overline{f'}$ *and* $f'(\gamma_i)$ *is monotonously increasing w.r.t* γ_i *before reaching* $\overline{f'}$ *and monotonously decreasing after that;*
- *For* $\gamma_i \in (0, +\infty)$, $f''(\gamma_i)$ *is first positive and* $f''(\gamma_i) = 0$ *at* $\gamma_i'' = 2ln(L/2)$ *then turns negative in* $(\gamma_i'', +\infty)$;

We now turn to the energy consumption of frame transmission. Consider a virtual slot time T_{slot}, the possibility of transmitting a frame with success for i is $P_{tr} = \tau(1-\tau)^{n-1}$, the frame transmission time is L/C_i; the possibility of collision is $P_c = 1 - (1-\tau)^n - n\tau(1-\tau)^{n-1}$, the collision duration is the RTS frame duration $t_{RTS} \ll L/C_i$. Thus the expected energy consumption per unit time for transmission of i is

$$Q_i = \frac{P_i P_{tr}\frac{L}{C_i} + P_c t_{RTS}}{T_{slot}} \simeq \frac{P_i P_{tr}\frac{L}{C_i}}{T_{slot}} = \frac{\tau(1-\tau)^{n-1} L P_i}{C_i T_{slot}}.$$

3.2.2 Utility Function

In game theory, the utility function is used to describe the satisfaction level of the player as a result of its actions. In an IEEE 802.11 WLANs, the objective of a node is to achieve maximum effective throughput and meanwhile minimize the energy consumption. This is a typical multi-objective optimization (MOP) problem: $\max_{P_i,C_i}[S_i^{eff}, -Q_i]$. A standard technique for MOP as above is to maximize a positively weighted sum of the objectives, i.e.,

$$\max_{P_i,C_i} \quad \alpha_i^1 S_i^{eff} - \alpha_i^2 Q_i \quad \alpha_i^1, \alpha_i^2 > 0.$$

In our context, α_i^1 can be interpreted as the reward of successfully transmitting one bit information, α_i^2 can be interpreted as the cost of dispensing one Joule energy for the transmission. From a monetary point of view, the unit for α_i^1, α_i^2 can be *euro/bit* and *euro/Joule*. $\alpha_i^1 S_i^{eff} - \alpha_i^2 Q_i$ is

thus the net benefit per unit time that node i enjoys by operating on (P_i, C_i). Different players may have different value of α_i^1 and α_i^2 depending on its own evaluation. Based on the above analysis, let $\zeta_i = \alpha_i^2/\alpha_i^1$ represent the player's individual preference between the reward and energy cost, we define the utility function of node i as:

$$U_i = S_i^{eff} - \zeta_i Q_i = \frac{\tau(1-\tau)^{n-1} L f_i(\gamma_i) - \zeta_i P_i \tau (1-\tau)^{n-1} \frac{L}{C_i}}{1 + \tau(1-\tau)^{n-1}\left[n(T_o - t_c) + \sum_{j=1}^{n} \frac{L}{C_j}\right] + [1-(1-\tau)^{n-1}]T_c} = \frac{f(\gamma_i) - k_i \gamma_i}{\frac{q_2}{q_1} + \sum_{j\in\mathcal{N}} \frac{1}{C_j}},$$

where $q_1 \triangleq \tau(1-\tau)^{n-1}L$, $q_2 \triangleq 1 + n\tau(1-\tau)^{n-1}(T_0 - T_c) + (1-(1-\tau)^n)\,T_c$, $k_i \triangleq \dfrac{\sigma^2}{h_i B_t}\zeta_i$.

In our game theoretic model, players are self-interested and rational that they would never accept the negative utility. We thus define the *rational feasible set* or simply *feasible set* as the strategy space that leads to non-negative utility. To avoid the trivial case where the rational feasible set is empty, we assume that $(U_i)_{max} > 0$. A necessary condition for $(U_i)_{max} > 0$ is $\overline{f_i'} > k_i$. Moreover, if $(U_i)_{max} > 0$, the following lemma is immediate:

Lemma 3.2. *$\forall i \in \mathcal{N}$, there exist $0 < \gamma_i^{min} < \gamma_i^{max}$ such that $U_i(0) = U_i(\gamma_i^{min}) = U_i(\gamma_i^{max}) = 0$, $U_i(\gamma_i) > 0$ for $\gamma_i^{min} < \gamma_i < \gamma_i^{max}$ and $U_i(\gamma_i) < 0$ for $0 < \gamma_i < \gamma_i^{min}, \gamma_i^{max} < \gamma_i$.*

Compare the proposed utility function with the traditional utility function in the literature expressed as the ratio between the data rate and power consumption, indicating the transmitted bits per Joule of energy expended, we introduce the parameter ζ_i that reflects the user's individual preference between the transmission reward and energy cost. Moreover, instead of regarding the PHY rate as throughput as in cellular networks, we model the gain in the utility function by the effective MAC layer throughput, which reflects the actual benefit of players since a node can never attain its PHY layer rate as throughput in an IEEE 802.11 WLAN. We argue that this cross-layer modelling is more suitable in our context.

3.2.3 Non-cooperative Power and Rate Control Game

In this chapter, we model the power and rate control in IEEE 802.11 WLAN as non-cooperative games where players choose their transmission power and/or data rate to maximize the utility function defined previously. We conduct an in-depth study on three specific games. In G_{NPC} and G_{NRC}, players choose their transmission power/rate under fixed transmission rate/power to maximize their utility. These two games correspond to the classical power control and rate adaptation problem, respectively. In the third game G_{NJPRC}, we address the general case, joint power and rate control, where players can adjust both transmission power and rate.

For non-cooperative games, the most important concept is NE, a strategy profile form which no player has incentive to deviate. We use the concept of social optimality, formally defined in the following in our context, to characterize the efficiency of strategy profiles.

Definition 3.1. *The strategy profile $\boldsymbol{s}$ is social optimal if it maximizes the aggregated payoff $\sum_{i\in\mathcal{N}} \alpha_i^1 S_i^{eff} - \alpha_i^2 Q_i = \sum_{i\in\mathcal{N}} \alpha_i^1 U_i$. Social optimality implies Pareto-optimality.*

3.3 Non-cooperative Fixed-rate Power Control Game

We first study the non-cooperative fixed-rate power control game G_{NPC}. This corresponds to the power control problem where players select their transmission power to maximize their payoff under fixed data rate. Noticing that $\gamma_i = \frac{h_i B_t}{\sigma^2}\frac{P_i}{C_i}$, G_{NPC} can be formally expressed as:

$$G_{NPC}: \quad \max_{\gamma_i^{min} \le \gamma_i \le \gamma_i^{max}} U_i(\gamma_i, \gamma_{-i}), \quad i \in \mathcal{N}.$$

The following theorem studies the NE of G_{NPC}.

Theorem 3.1. *G_{NPC} admits a unique NE $\{\gamma_i = \gamma_i^*\}$ or $\left\{P_i = \frac{\sigma^2 C_i \gamma_i^*}{h_i B_t}\right\}$, where γ_i^* is the root of $f'(\gamma_i) = k_i$ in $(\gamma_i^{min}, \gamma_i^{max})$.*

Proof. Please refer to Section 3.8.1 for the detailed proof. □

It can be further shown that at the unique NE derived above, the aggregated utility $\sum_{i\in\mathcal{N}} \alpha_i^1 U_i$ is also maximized. The NE is thereby Pareto-optimal and social optimal under given data rate configuration $\{C_i\}$.

3.4 Non-cooperative Fixed-power Rate Control Game

In this section, we study the non-cooperative rate control game under fixed transmission power G_{NRC}. This corresponds to the rate adaptation problem where players select their data rate to maximize their payoff under fixed power $\{P_i\}$. G_{NRC} can be formally expressed as:

$$G_{NRC} \quad \max_{\gamma_i \in [\gamma_i^{min}, \gamma_i^{max}]} U_i = \frac{f(\gamma_i) - k_i\gamma_i}{\frac{q_2}{q_1} + \sum_{j\in\mathcal{N}} \frac{\sigma^2}{h_j B_t}\frac{\gamma_j}{P_j}}, i \in \mathcal{N}$$

3.4.1 Best Response Strategy

In order to solve G_{NRC}, we introduce the best response strategy. At the NE, the action chosen by a rational self-interested player constitutes the best response to the action currently chosen by other players. In G_{NRC}, player i's best response function $b_i : \gamma_{-i} \to \gamma_i$ is defined as follows:

$$b_i = \operatorname*{argmax}_{\gamma_i^{min} \le \gamma_i \le \gamma_i^{max}} U_i(\gamma_i, \gamma_{-i}).$$

In G_{NRC}, the best response of each player i is obtained by imposing $\frac{\partial U_i}{\partial \gamma_i} = 0$, which equals to solving the following equation

$$P_i \frac{h_i B_t}{\sigma^2}\frac{q_2}{q_1} + \sum_{j\in\mathcal{N}, j\neq i} \frac{P_i}{P_j}\frac{h_i}{h_j}\gamma_j = \frac{f(\gamma_i) - k_i\gamma_i}{f'(\gamma_i) - k_i} - \gamma_i. \tag{3.2}$$

Lemma 3.3. *$\forall i \in \mathcal{N}$, the best response function defined in (3.2) has a unique solution $\widetilde{\gamma_i} = b_i(\gamma_{-i})$ in the rational feasible set and it holds that $\gamma_i^{min} < \widetilde{\gamma_i} < \gamma_i^{*}$*[2].

Proof. Please refer to Section 3.8.2 for detailed proof. □

[2] γ_i^* is defined in Theorem 3.1

The following corollary based on the best response function is immediate.

Corollary 3.1. *If $\{\gamma_i\}$ updated according to $\{b_i(\gamma)\}$ converges to $\gamma = \{\gamma_i\}$, then γ is a NE.*

Consider G_{NRC} is played repeatedly, choosing the best response at each stage consists of a natural and rational strategy called the best response strategy where each player updates its data rate for the next time stage such that it maximizes its utility based on the data rate of opponents in the current time stage. It is commonly used to study the stability of NE.

3.4.2 Nash Equilibrium Analysis

The existence of NE in G_{NRC} follows the fact that the action set A_i is a nonempty compact convex subset of Euclidian space and U_i is continuous and quasi-concave in γ_i on A_i.

The following theorem studies the uniqueness of the NE and the convergence to the NE under the best response strategy.

Theorem 3.2. *If* $\forall i \in \mathcal{N},\ k_i > \dfrac{1}{2ln(L/2)}$ *and* $\dfrac{k_i - f'(\gamma_i^{min})}{P_i h_i f''(\gamma_i^{min})} \displaystyle\sum_{j\in\mathcal{N}, j\neq i} \frac{1}{\left(\frac{B_t}{\sigma^2}\frac{q_2}{q_1} + \sum_{j\in\mathcal{N}} \frac{\gamma_j^{min}}{P_j h_j}\right)} < 1,$

then it holds that

1. *The game G_{NRC} admits a unique NE.*
2. *Starting from any initial point, the iteration defined by best response function converges to the unique NE.*

Proof. Please refer to Section 3.8.3 for detailed proof. □

Remark: Theorem 3.2 establishes the sufficient condition for the uniqueness and convergence of the NE in G_{NRC}. It follows straightforwardly that under the condition, the unique NE is also stable in that any deviated point from the NE will be dragged back to the NE under best response strategy.

There are several interesting engineering implications in the above analysis:

- Theorem 3.2 provides a simple way to calculate the NE, i.e., to find the fixed point of the best response function, which can be solved recursively.
- It quantifies the relation between the NE and the various parameters, based on which the stability of the rate control scheme can be checked.
- It provides guidelines to configure the parameters to ensure system stability: e.g., with a larger value of L and P_i, the stability and the convergence to the NE is more likely to be guaranteed.

From an economic point of view, $\dfrac{k_i}{\frac{q_2}{q_1} + \sum_{j\in\mathcal{N}} \frac{\sigma^2}{h_j B_t}\frac{\gamma_j}{P_j}}$ can be regarded as the price for player i operating on γ_i. The NE is the point where the marginal effective throughput $\dfrac{\partial S_i^{eff}}{\partial C_i}$ equals to the price. From the players's point of view, operating at larger γ_i increases the effective throughput at the expense of paying more in terms of energy. Hence, to search the NE is actually to seek a compromised point between the gain (effective throughput) and the cost (energy consumption).

3.4.3 Inefficiency of the Nash Equilibrium

The obtained NE provides a solution where no player can increase its utility any further through individual effort. It is an outcome obtained as a result of distributed decision taking which may be less efficient than cooperative rate configuration among players. In some cases such as G_{NPC}, the NE is also the social optimal point, but in many cases, the NE does not coincide with the social optimal point. In fact, it is well known that in general the NE are inefficient. In this section, we will show that the NE of G_{NRC} is inefficient and in next section we will propose a pricing scheme to improve the efficiency of the NE.

Let $\widehat{\gamma} = \{\widehat{\gamma}_i\}$ denote the social optimal point of G_{NRC} maximizing the aggregated utility $\sum_{i\in\mathcal{N}} \alpha_i^1 U_i$ mentioned in Section 3.2, by imposing $\frac{\partial \sum_{i\in\mathcal{N}} \alpha_i^1 U_i}{\partial \gamma_i} = 0$, we obtain,

$$P_i \frac{h_i B_t}{\sigma^2}\frac{q_2}{q_1} + \sum_{j\in\mathcal{N}, j\neq i} \frac{P_i h_i}{P_j h_j}\gamma_j = \frac{\sum_{j\in\mathcal{N}} \frac{\alpha_j^1}{\alpha_i^1}\Big[f(\gamma_j) - k_j\gamma_j\Big]}{f'(\gamma_i) - k_i} - \gamma_i \tag{3.3}$$

Compare (3.3) with the best response function of G_{NRC} (3.2) and performing similar analysis, we have the following theorem on the social optimal point.

Theorem 3.3. *Regard* (3.3) *as the best response update scheme to maximize the global payoff, under the same condition as Theorem 3.2, it holds that:*

1. *There exists a unique fixed point in the update scheme* (3.3) *which is also the unique maximizer of* $\sum_{i\in\mathcal{N}} \alpha_i^1 U_i$.
2. *Starting from any initial point, the iteration defined by best response function* (3.3) *converges to the unique fixed point.*

Proof. Please refer to Section 3.8.3 for the detailed proof. □

Theorem 3.3 provides a distributed way to converge to the social optimal point. Furthermore, we have the following corollary on the relation between the NE of G_{NRC} $\gamma = (\gamma_1, \cdots, \gamma_n)$ and the global optimal point:

Corollary 3.2. *On the NE of* G_{NRC} $\gamma = \{\gamma_i\}$ *and the global optimal point* $\widehat{\gamma} = \{\widehat{\gamma}_i\}$*, it holds that* $\gamma_i > \widehat{\gamma}_i, \forall i \in \mathcal{N}$.

Proof. Please refer to Section 3.8.4 for the detailed proof. □

Corollary 3.2 shows that the NE is not social optimal. If all players switch from the NE to the global optimal point, the aggregated utility increases. This is due to the fact of lack of cooperation and the incentive to operate at social optimal point. The most important result in this subsection is summarized by the following theorem.

Theorem 3.4. *In* G_{NRC}*, the unique NE is inefficient.*

3.4.4 Improving the Efficiency of NE in G_{NRC}

Having shown the inefficiency of the NE in G_{NRC}, we turn to pricing, a technique widely used in game theory, to improve the efficiency of the NE. In our case, noticing that at the NE, players tend to transmit at lower rate than the transmission rate at the social optimal point ($\gamma_i > \widehat{\gamma}_i$), we encourage the players to increase their transmission rate via pricing to approach the NE to the social optimal point. In this new context, we develop a non-cooperative game with pricing G_{NRCP} with the utility function U_i' defined as $U_i' = U_i + \tau_i(\gamma)$, where $\tau_i(\gamma)$ is the pricing function. In our study, we propose the following non-linear pricing function

$$\tau_i(\gamma) = -p_i S_i \gamma_i = -\frac{p_i \gamma_i}{\frac{q_2}{q_1} + \sum_{j \in \mathcal{N}} \frac{\sigma^2}{h_j B_t} \frac{\gamma_i}{P_j}},$$

where $p_i > 0$ is the pricing factor used to encourage the players to transmit at a higher data rate (smaller γ_i). Let $k_i' = k_i + p_i$, the utility function of G_{NRCP} is

$$U_i' = \frac{f(\gamma_i) - k_i' \gamma_i}{\frac{q_2}{q_1} + \sum_{j \in \mathcal{N}} \frac{\sigma^2}{h_j B_t} \frac{\gamma_j}{P_j}}.$$

Performing the same analysis for G_{NRCP} as in G_{NRC}, we have the following theorem.

Theorem 3.5. *If* $\forall i \in \mathcal{N}$, $k_i' > \dfrac{1}{2ln(L/2)}$ *and* $\dfrac{k_i' - f'((\gamma_i^{min})')}{P_i h_i f''((\gamma_i^{min})')} \displaystyle\sum_{j \in \mathcal{N}, j \neq i} \frac{1}{\left(\frac{B_t}{\sigma^2} \frac{q_2}{q_1} + \sum_{j \in \mathcal{N}} \frac{(\gamma_j^{min})'}{P_j h_j} \right)} < 1$, *where* $(\gamma_j^{min})'$ *is the smaller one of the two non-zero roots of* $f'(\gamma_i) = k_i'$, *then it holds that*

1. *The game* G_{NRCP} *admits a unique NE.*
2. *Starting from any initial point, the iteration defined by best response function converges to the unique NE.*

Remark: In G_{NRCP}, p_i should be chosen such that $(U_i')_{max} > 0$ to ensure that the feasible strategy set for a rational self-interested player is not empty. This also implicitly guarantees that $f'(\gamma) = k_i'$ has two non-zero roots $(\gamma_i^{min})'$ and $(\gamma_i^{max})'$.

In the analysis of G_{NRC}, we can interpret $\dfrac{k_i}{\frac{q_2}{q_1} + \sum_{j \in \mathcal{N}} \frac{\sigma^2}{h_j B_t} \frac{\gamma_j}{P_j}}$ as the price for player i operating on γ_i. In G_{NRCP}, the above price increases to $\dfrac{k_i'}{\frac{q_2}{q_1} + \sum_{j \in \mathcal{N}} \frac{\sigma^2}{h_j B_t} \frac{\gamma_j}{P_j}}$. As the price increases, each player i tends to decrease its γ_i at the NE.

The gain of applying pricing in our context is indeed two-fold:

- It leads the game to a more efficient NE.
- It provides a tunable parameter p_i to control the stability (existence and convergence of NE) of the system.

One crucial issue concerning the proposed pricing scheme is that the pricing factor p_i should be carefully tuned such that each user's self interest leads to overall improvement of the system. How to choose p_i is not trivial at all and depends very much on the system parameters. In practice,

noticing that finding the optimal pricing factor may be impractical or even impossible, we propose the following adaptive search method to find the locally optimal value of p_i. We will evaluate the proposed method via simulation in Section 3.6.

Algorithm 2 Adaptive Search Method of p_i

1. Set $\Delta p, \varepsilon$ to some small values. Initialize $p_i^0 = 0, \forall i \in \mathcal{N}$.
2. At each iteration t, measure the effective network throughput $S^{eff}(t)$.
   If $S^{eff}(t) > S^{eff}(t-1)$, set $p_i^{t+1} = p_i^t + \Delta p$, $\forall i \in \mathcal{N}$.
   If $S^{eff}(t) < S^{eff}(t-1)$, set $p_i^{t+1} = p_i^t - \Delta p$, $\forall i \in \mathcal{N}$.
3. Stop until $|S^{eff}(t) - S^{eff}(t-1)| < \varepsilon S^{eff}(t)$.

3.5 Joint power and rate Control Game

In this section, we turn to the general and the most flexible case where each player can configure both its transmission power P_i and data rate C_i to maximize its payoff: the non-cooperative joint power and rate control game G_{NJPRC}. It is clear that G_{NJPRC} is not decomposable, i.e.,

$$\max_{C_i,P_i} U_i \neq \max_{C_i} \max_{P_i} U_i \quad \text{and} \quad \max_{C_i,P_i} U_i \neq \max_{P_i} \max_{C_i} U_i.$$

We thus consider the following game G'_{NJPRC} defined as

$$G'_{NJPRC}: \max_{\substack{\gamma_i^{min} \leq \gamma_i \leq \gamma_i^{max}, \\ C_i^{min} \leq C_i \leq C_i^{max}}} U_i = \frac{f(\gamma_i) - k_i \gamma_i}{\frac{q_2}{q_1} + \sum_{j \in \mathcal{N}} \frac{1}{C_j}}, i \in \mathcal{N}.$$

It is obvious that G'_{NJPRC} is equivalent to G_{NJPRC}. The following theorem studies the NE of G'_{NJPRC}.

Theorem 3.6. *There exists a unique efficient NE in G'_{NJPRC}, where $C_i = C_i^{max}$, $\gamma_i = \gamma_i^*$ $\forall i \in \mathcal{N}$.*

The proof follows the same way as Theorem 3.1. It is further easy to show that the NE of G'_{NJPRC} is also social optimal and Pareto optimal. Compared with G_{NPC} of which the NE maximizes the global payoff at given data transmission rate configuration and G_{NRC} of which the unique NE is not efficient, G'_{NJPRC} achieves the global optimality. In our context, providing more flexibility in parameter configuration to selfish players in fact helps the system operate optimally rather than lead to system collapse.

3.5.1 Subgradient Update: Better Response Strategy

In this section, motivated by the fact that G'_{NJPRC} achieves the global optimality at its unique NE, we perform an in-depth study on how to reach the unique efficient NE. One might propose to trivially set $C_i = C_i^{max}$ and $\gamma_i = \gamma_i^*$. However, in practice, it is not easy for a player to calculate γ_i^*. Moreover, best response strategy often leads to large fluctuations that may cause temporary system instability. Next we propose an alternative update scheme to approach the NE: the subgradient update scheme, consisting of

1. Setting $C_i = C_i^{max}$

2. Updating γ_i as $\gamma_i^{t+1} = \gamma_i^t + \lambda \frac{\partial U_i(\gamma_i)}{\partial \gamma_i}\Big|_{\gamma_i=\gamma_i^t}$, where λ is the step size usually sufficiently small.

At each iteration of the subgradient update scheme, each player takes a step in the direction of the positive subgradient. The engineering implication behind is that if the marginal effective throughput outweighs the price, player i increases its γ_i, otherwise it decreases γ_i. By setting the step size sufficiently small, the subgradient update experiences a smooth trajectory.

We now study the convergence of the subgradient scheme to the unique NE. Our analysis follows the technique in [ABD06]. We first define a function $x_i(\tau) : [0,1] \to \mathbb{R}$ for player i as

$$x_i(\tau) = \tau\gamma_i^t + (1-\tau)\gamma_i^* + \lambda \frac{\partial U_i(\gamma_i)}{\partial \gamma_i}\Big|_{\gamma_i=\tau\gamma_i^t+(1-\tau)\gamma_i^*},$$

where the unique NE γ_i^* is the fixed point of the mapping $\gamma_i^t \to \gamma_i^{t+1}$. Noticing that $\frac{\partial U_i(\gamma_i)}{\partial \gamma_i}\Big|_{\gamma_i^*} = 0$, we have

$$|\gamma_i^{t+1} - \gamma_i^*| = |x_i(1) - x_i(0)| = \left| \int_0^1 \frac{dx_i(\tau)}{d\tau} d\tau \right| \le \int_0^1 \left| \frac{dx_i(\tau)}{d\tau} \right| d\tau \le \max_{\tau\in[0,1]} \left| \frac{dx_i(\tau)}{d\tau} \right|.$$

Noticing that λ is usually sufficiently small, we have

$$\left| \frac{dx_i(\tau)}{d\tau} \right| = \left(1 + \lambda \frac{\partial^2 U_i(\gamma_i)}{\partial \gamma_i^2} \right) \Big|_{\gamma_i=\gamma_i^t} \cdot \left| \gamma_i^t - \gamma_i^* \right| = \left(1 + \lambda \frac{f_i''(\gamma_i^t)}{\frac{q_2}{q_1} + \sum_{j\in\mathcal{N}} \frac{1}{C_j}} \right) \cdot |\gamma_i^t - \gamma_i^*|.$$

Under the condition $f_i''(\gamma_i) < 0, \gamma_i^{min} \le \gamma_i \le \gamma_i^{max}, \forall i \in \mathcal{N}$, we have

$$\left|\gamma_i^{t+1} - \gamma_i^*\right| \le \rho_i \left|\gamma_i^t - \gamma_i^*\right|,$$

where $\rho_i = 1 + \lambda \frac{\max_{\gamma_i\in[\gamma_i^{min},\gamma_i^{max}]} f_i''(\gamma_i)}{\frac{q_2}{q_1} + \sum_{j\in\mathcal{N}} \frac{1}{C_{min}}} < 1$. It follows that starting from any initial value γ_i^0, $\lim_{n\to+\infty} \gamma_i^t = \gamma_i^*$. In the proof of Theorem 3.2 presented in Section 3.8.3, we have shown that

$$k_i > \frac{1}{2ln(L/2)} \Longrightarrow f_i''(\gamma_i) < 0, \gamma_i^{min} \le \gamma_i \le \gamma_i^{max}.$$

It thus follows that if $k_i > \frac{1}{2ln(L/2)}, \forall i \in \mathcal{N}$, the subgradient update scheme converges to the unique NE.

One issue left is how to calculate $\frac{\partial U_i(\gamma_i)}{\partial \gamma_i}\Big|_{\gamma_i=\gamma_i^t}$. In fact, assuming after sufficient long time, each player operates on C_i^{max} according to the subgradient update scheme, $\frac{\partial U_i(\gamma_i)}{\partial \gamma_i}\Big|_{\gamma_i=\gamma_i^t}$ can be estimated by $\frac{U_i(\gamma_i^t) - U_i(\gamma_i^{t-1})}{\gamma_i^t - \gamma_i^{t-1}}$. Noticing $P_i = \frac{\sigma^2}{h_i B_t} C_i \gamma_i$ is a linear function of γ_i, we have the following theorem:

Theorem 3.7. *In G'_{JNRPC}, if $k_i > \frac{1}{2ln(L/2)}, \forall i \in \mathcal{N}$, then the following subgradient update scheme converges to the unique NE $C_i = C_i^{max}$, $P_i = \frac{\sigma^2}{h_i B_t} C_i \gamma_i^*$:*

1. *Set* $C_i = C_i^{max}$

2. *At iteration* $t+1$, *set* $P_i^{t+1} = P_i^t + \lambda \dfrac{U_i(P_i^t) - U_i(P_i^{t-1})}{P_i^t - P_i^{t-1}}$

In the above subgradient update scheme, each player updates its γ_i at the same time instance. A natural and more practical generalization is the asynchronous subgradient update scheme where only a random subset of players perform update at a given time instance. This scheme is actually more realistic in that it is difficult for the players to synchronize their update in a practical implementation. In our context, concerning the convergence of the asynchronous subgradient update scheme, we have the following theorem.

Theorem 3.8. *In* G'_{NJPRC}, *under the same condition as in Theorem 3.7, the asynchronous subgradient update scheme converges to the unique NE.*

Proof. Please refer to Section 3.8.6 for detailed proof. □

3.5.2 Game Theory Based Joint power and rate Control Procedure for IEEE 802.11 WLAN

In this section, we provide a practical procedure of the joint power and rate control based on Theorem 3.8. From the game theoretic point of view, the proposed procedure consists of a distributed strategy update scheme to achieve the NE which is social optimal, too. The convergence of the procedure to the NE is proven in Section 3.5.1 under certain conditions. In the procedure, each user updates its transmission power according to the subgradient update scheme.

Algorithm 3 Game Theory Based Joint Power and Rate Control Procedure

Sender side:

Initiation:

Set the initial power to random value P_i^0

Schedule the power update at time $t_1, t_2, \cdots$

At t_m

Calculate $U_i(P_i^{m-1})$ as $U_i(P_i^{m-1}) = \dfrac{N_{suc}L - \zeta_i P_i^{m-1} N_{sent}\frac{L}{C_i}}{t_m - t_{m-1}}$

Update P_i as $P_i^m = P_i^{m-1} + \lambda \dfrac{U_i(P_i^{m-1}) - U_i(P_i^{m-2})}{P_i^{m-1} - P_i^{m-2}}$

Set the flag in RTS frame informing the receiver the new iteration begins at next frame

Receiver side:

When receiving RTS with flag set, include N_{suc} in CTS, then set N_{suc} to 0

At the reception of each frame, if the frame is not erroneous, $N_{suc} \leftarrow N_{suc} + 1$

The proposed joint power and rate control scheme has the following desirable properties:

- No system-dependent parameters are needed to approach the NE, such as $f(\gamma_i)$, h_i. The proposed scheme is thus totally transparent for users.
- Only minor changes are needed to incorporate the proposed procedure into the IEEE 802.11 MAC protocol.

- Each user only needs to temporarily buffer the number of frames sent during last iteration N_{sent}, the utility of the last two iterations and the number of frames received without error during the last iteration N_{suc}.
- The update can be performed asynchronously among users. No network-wide synchronization is required.

3.6 Numerical Results

In this section, we present numerical results for the investigated three non-cooperative games. The following parameter setting is used in our experiments: $L = 12000$ bits (1500 bytes), $h_i = d_{ij}^{-4}$ where d_{ij} is the distance between the source i and the destination j, $CW_{min} = 32$, $CW_{max} = 1024$, $K = 10$, the slot size is $20\mu s$, the data frame transmission overhead $T_o = 52$ slots, the RTS collision overhead $T_c = 17$ slots. We simulate a WLAN of 10 nodes randomly distributed in the $100m \times 100m$ field. α_i^1 is set to 1 for all nodes. ζ_i is randomly distributed in $[0.01, 0.05]$Mb/Joule if not explicitly stated. The noise is set to -174dBm/Hz.

We first plot the NE of G_{NPC} under the fixed data rate $C_i = 10$Mbps for all players in Figure 3.1 with five different ζ value settings. For setting k ($k = 1, \cdots, 5$), ζ_i is randomly chosen from $[0.01 * k, 0.05 * k]$Mb/Joule. We can see from the result that the NE is almost the same for different ζ values. However, the power value at the NE is significantly different among players. This interesting fact is due to the fact that in our scenario, the NE is much more sensible to the parameters such as h than ζ. The following two points can be drawn:

- Power control is in deed necessary in that the player's transmission power at NE differs significantly from one to another and depends very much on some system parameters and configurations such as h in our case.
- In general cases, how a player weighs the cost of energy consumption w.r.t. its gain in terms of effective throughput does not have significant impact on the transmission power at NE.

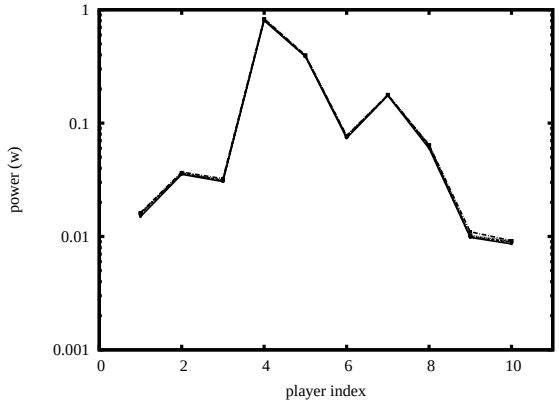

Figure 3.1: NE of G_{NPC}

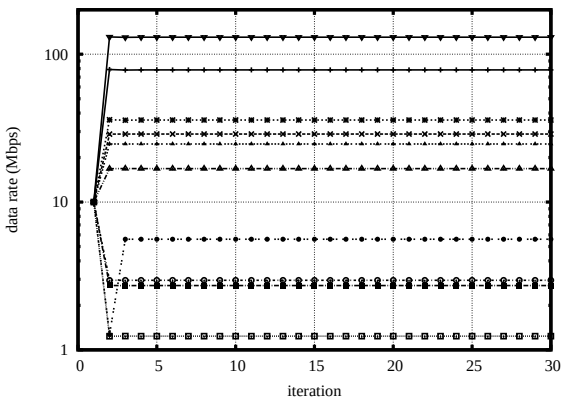

Figure 3.2: Trajectory of G_{NRC} under the best response strategy

We then study G_{NRC} under fixed transmission power $P_i = 100$mW for all players i. Figure 3.2 and 3.3 show the trajectories of the data rate of players under best response strategy without and with pricing ($p_i = 0.02$). Figure 3.4 shows the trajectory under (3.3) to approach the social optimal

point. In all cases, the data rate converges. According to our analysis, the converged data rate in Figure 3.2 and 3.3 is the unique NE. We can check that the sufficient condition of the convergence under the best response strategy does not hold in our scenario. However, The best response update scheme converges, indicating that the conditions in Theorem 3.2 are only sufficient conditions for the convergence and may be too stringent in some cases.

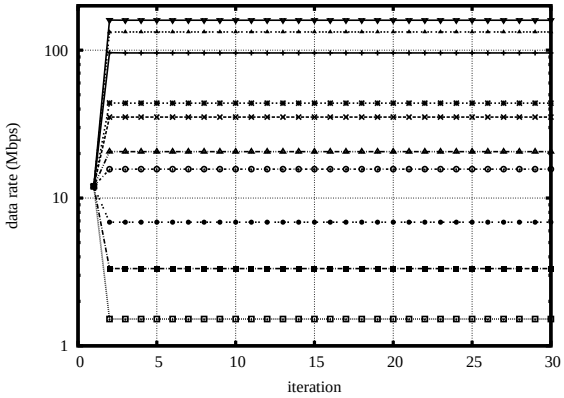

Figure 3.3: Trajectory of G_{NRC} with pricing under best response update

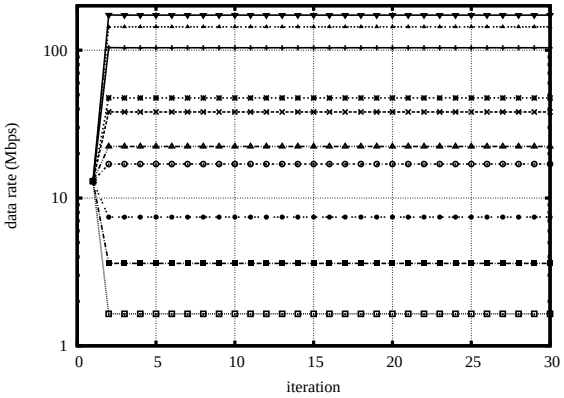

Figure 3.4: Approaching the social optimal point applying Theorem 3.3

Figure 3.5 studies G_{NJPRC} under the subgradient update scheme. C_{max} is set to 50Mbps for all players. As mentioned in the analysis, under the subgradient update scheme, the convergence to the NE achieves in a smooth way. As price, the convergence is achieved much more slowly. Once again, the transmission power converges although the sufficient condition does not hold. According to the analytical model, the converged value is the unique NE of G_{NJPRC}.

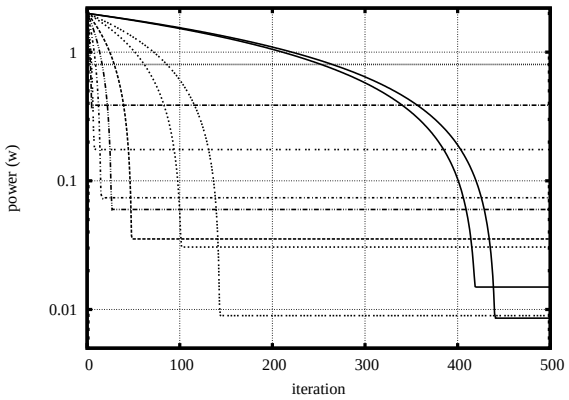

Figure 3.5: Trajectory of G_{NJPRC} under the subgradient update scheme

Finally, we study the efficiency of the NE of three specific games analyzed in this chapter. The game parameters are the same as the scenarios in Figure 3.1–3.5: $\zeta_i \in [0.01, 0.05]$Mb/Joule, for G_{NPC}, C_i is set to 10Mbps; for G_{NRC}, P_i is set to 100mW; for G_{NJPRC}, C_{max} is set to 50Mbps. The result is shown in Table 3.2. We can see that the NE of G_{NJPRC} shows the best system-wide performance. For G_{NRC}, the system is sub-optimal. We then apply the adaptive search method proposed in Section 3.4 ($\Delta p = 0.002$, $\varepsilon = 0.01$) to choose a local optimal pricing factor p_{opt}. By applying the pricing technique, the performance of G_{NRC} is significantly ameliorated, although still not optimal, as shown in the table. The numerical result confirms our analysis in Section 3.5 that providing more flexibility in parameter configuration to non-cooperative players in fact helps

the system operate optimally rather than leads to system collapse in our context.

Game	Aggregated utility $\sum_{i\in\mathcal{N}} \alpha_i^1 U_i$
G_{NPC}	$6.9 * 10^7$
G_{NRC}	$4.3 * 10^7$
G_{NRCP} $(p_i = 0.01)$	$4.5 * 10^7$
G_{NRCP} $(p_i = p_{opt})$	$6.1 * 10^7$
G_{NJPRC}	$2.5 * 10^8$

Table 3.2: NE efficiency for three games

3.7 Conclusion

In this chapter we formulated the power and rate control problem in IEEE 802.11 WLANs as three specific non-cooperative games: the fixed-rate power control game G_{NPC}, the fixed-power rate control game G_{NRC} and the joint power and rate control game G_{NJPRC}.

We demonstrated analytically that G_{NPC} admits a unique efficient NE under the given data rate configuration. For G_{NRC}, under certain conditions, the existence and the uniqueness of the NE is guaranteed. The convergence to the unique NE is also ensured under best response strategy. However, the unique NE is inefficient. We then propose a pricing scheme to improve the efficiency, but how to choose the pricing factor is not trivial. In contrast, G_{NJPRC} is shown to admit a unique NE which is also the system-wide optimal point. Motivated by this analysis, we proposed the game theory based joint power and rate control procedure, a distributed algorithm that can be incorporated into existing IEEE 802.11 MAC protocol easily to approach the NE. Both analytical and numerical results show that the proposed procedure can achieve system optimality. We also show that in our context, providing more flexibility in parameter configuration to non-cooperative players in fact helps the system operate optimally rather than lead to system collapse.

3.8 Proofs

This section completes the detailed proofs omitted from the main text.

3.8.1 Proof of Theorem 3.1

It can be verified that the strategy set $A_i = \{\gamma_i | \gamma_i^{min} \leq \gamma_i \leq \gamma_i^{max}\}$ of each player i is a nonempty compact convex subset of Euclidian space and the utility function U_i is quasi-concave in γ_i on A_i. Hence, by Theorem 1 in [Ros65], G_{NPC} is a n-person game and has a NE.

In G_{NPC}, each player aims at maximizing its utility function U_i. We begin by checking the local maximizer by imposing $\frac{\partial U_i}{\partial \gamma_i} = 0$, or $f'(\gamma_i) = k_i$. Following Lemma 3.1 and the assumption $\overline{f_i'} > k_i$, it holds that $f'(\gamma_i) = k_i$ has two roots γ_i^0 and γ_i^*. Without loss of generality, assume $\gamma_i^0 < \gamma_i^*$, applying Lagrange interpolation theorem, we have $0 < \gamma_i^0 < \gamma_i^{min} < \gamma_i^* < \gamma_i^{max}$. Furthermore, it holds that $f'(\gamma_i) < k_i$ when $\gamma_i < \gamma_i^0$, $\gamma_i > \gamma_i^*$ and $f'(\gamma_i) > k$ when $\gamma_i^0 < \gamma_i < \gamma_i^*$. It then follows that γ_i^0 is the local minimizer of U_i and γ_i^* is the local maximizer. Since at the border point γ_i^{min}

and γ_i^{max}, $U_i = 0$, γ_i^* is thus the unique global maximizer: i.e.,

$$U_i(\gamma_i, \gamma_{-i}) > U_i(\gamma_i', \gamma_{-i}), \gamma_i' \in [\gamma_i^{min}, \gamma_i^{max}], \gamma_i' \neq \gamma_i^*.$$

Hence, $\{\gamma_i = \gamma_i^*\}$ is the unique NE of G_{NPC}.

3.8.2 Proof of Lemma 3.3

Let $g(\gamma_i)$ denote the right hand side (RHS) of (3.2), we have

$$g'(\gamma_i) = -\frac{(f(\gamma_i) - k_i\gamma_i)f''(\gamma_i)}{(f'(\gamma_i) - k_i)^2}$$

Noticing the fact that $f(\gamma_i) - k_i\gamma_i > 0$ for $\gamma_i \in (\gamma_i^{min}, \gamma_i^{max})$ and applying Lemma 3.1, we have, for $\gamma_i \in (\gamma_i^{min}, \gamma_i^{max})$:

1. if $\gamma_i'' \leq \gamma_i^{min}$, then $g(\gamma_i)$ is monotonously increasing in γ_i.
2. if $\gamma_i^{min} < \gamma_i'' < \gamma_i^{max}$, then $g(\gamma_i)$ is first monotonously decreasing till γ_i'' and then monotonously increasing.

Note that $\gamma_i'' \geq \gamma_i^{max}$ is not possible since $f''(\gamma_i) < 0$ at γ_i^*[3], thus $\gamma_i'' < \gamma_i^* < \gamma_i^{max}$. In either case 1 or case 2, following that

$$\begin{cases} g(\gamma_i^{min}) = 0 < P_i\frac{h_iB_t}{\sigma^2}\frac{q_2}{q_1} + \sum_{j\in\mathcal{N}, j\neq i}\frac{P_i}{P_j}\frac{h_i}{h_j}\gamma_j \\ \lim_{\epsilon\to 0} g(\gamma_i^* - \epsilon) \to +\infty > P_i\frac{h_iB_t}{\sigma^2}\frac{q_2}{q_1} + \sum_{j\in\mathcal{N}, j\neq i}\frac{P_i}{P_j}\frac{h_i}{h_j}\gamma_j \end{cases} \quad \gamma_j^{min} \leq \gamma_j \leq \gamma_j^{max}, \forall j \in \mathcal{N}, j \neq i$$

and $g(\gamma_i) < 0$ for $\gamma_i > \gamma_i^*$, it holds that (3.2) always admits a unique solution $\gamma_i^{min} < \widetilde{\gamma_i} < \gamma_i^*$.

3.8.3 Proof of Theorem 3.2

It follows from $k_i > \frac{1}{2ln(L/2)}, \forall i \in \mathcal{N}$ that $k_i\gamma_i'' > 1 > f(\gamma_i'') = (1 - \frac{1}{2}e^{-\gamma_i''/2})^L$, leading to $U_i(\gamma_i'') < 0$. Noticing that $U_i(\gamma_i) \geq 0$ for $\gamma_i \in [\gamma_i^{min}, \gamma_i^{max}]$ and it is impossible that $\gamma_i'' \geq \gamma_i^{max}$[4], we have $\gamma_i'' < \gamma_i^{min}$. It then follows from Lemma 3.1 that $f''(\gamma_i) < 0$ for $\gamma_i \in [\gamma_i^{min}, \gamma_i^{max}]$.

We now turn to prove the uniqueness of the NE and the convergence to the unique NE under best response strategy. By definition, the NE has to satisfy $\gamma = \mathbf{b}(\gamma)$, where $\gamma = (\gamma_1, \cdots, \gamma_n)$ and $\mathbf{b}(\gamma) = (b_1(\gamma), b_2(\gamma), \cdots, b_n(\gamma))$ is the best response vector of all players. We use the following theorem in game theory concerning the uniqueness of NE [AC]:

Lemma 3.4. *If the best response function is a contraction, then the game admits a unique NE; Starting from any initial point, the iteration under the best response converges to the unique NE.*

The contraction is defined in [AC] as follows: let (X, d) be a metric space, f: $X \to X$ is a contraction if there exists a constant $k \in [0, 1)$ such that $\forall x, y \in X$, $d(f(x), f(y)) \leq kd(x, y)$, where $d(x, y) \stackrel{\triangle}{=} ||x - y|| = \max_i ||x_i - y_i||$.

[3]This can be shown by noticing that $f'(\gamma_i)$ is monotonously decreasing w.r.t. γ_i at γ_i^*, which is proven in the proof of Theorem 3.1 in Section 3.8.1.

[4]See the proof of Lemma 3.3 in Section 3.8.2

The key point to establish the uniqueness of the NE of G_{NRC} is to show $\mathbf{b}(\gamma)$ is a contraction. We have:

$$d(f(x), f(y)) = ||f(x) - f(y)|| \leq \left|\left|\frac{\partial f}{\partial x}\right|\right| \cdot ||x - y|| = \left|\left|\frac{\partial f}{\partial x}\right|\right| d(x, y).$$

Thus if the Jacobian $\left|\left|\frac{\partial f}{\partial x}\right|\right| \leq k$, then f is a contraction.

Next, we show that the best response function $\mathbf{b}(\gamma)$ is a contraction by proving $||J||_\infty \leq k$, where $J \triangleq \{J_{ij}\}$ is the Jacobian of $\mathbf{b}(\gamma)$ defined by $J_{ij} \triangleq \frac{\partial \gamma_i^{t+1}}{\partial \gamma_j^t}$.

Rewrite (3.2) at iteration t ($t \geq 0$), we have

$$P_i \frac{h_i B_t}{\sigma^2} \frac{q_2}{q_1} + \sum_{j \in \mathcal{N}, j \neq i} \frac{P_i h_i}{P_j h_j} \gamma_j^t = \frac{f(\gamma_i^{t+1}) - k_i \gamma_i^{t+1}}{f'(\gamma_i^{t+1}) - k_i} - \gamma_i^{t+1}. \tag{3.4}$$

From Lemma 3.3, we have

$$\gamma_i^{min} < \gamma_i^t < \gamma_i^* \quad \forall i \in \mathcal{N}, t \geq 1.$$

Moreover, by partially deriving both sides of (3.4) w.r.t. γ_j^t, $j \in \mathcal{N}$, J_{ij} can be solved as

$$J_{ij} = \begin{cases} -\frac{P_i h_i}{P_j h_j} \frac{(f'(\gamma_i^{t+1}) - k_i)^2}{(f(\gamma_i^{t+1}) - k_i \gamma_i^{t+1}) f''(\gamma_i^{t+1})} & i \neq j \\ 0 & i = j \end{cases}.$$

It follows that

$$||J||_\infty = \max_{i \in \mathcal{N}} \left\{ \sum_{j \in \mathcal{N}, j \neq i} \frac{P_i h_i}{P_j h_j} \left| \frac{(f'(\gamma_i^{t+1}) - k_i)^2}{(f(\gamma_i^{t+1}) - k_i \gamma_i^{t+1}) f''(\gamma_i^{t+1})} \right| \right\}.$$

From (3.4), we have

$$\begin{aligned} f(\gamma_i^{t+1}) - k_i \gamma_i^{t+1} &= (f'(\gamma_i^{t+1}) - k_i) \left(P_i \frac{h_i B_t}{\sigma^2} \frac{q_2}{q_1} + \sum_{j \in \mathcal{N}, j \neq i} \frac{P_i h_i}{P_j h_j} \gamma_j^t + \gamma_i^{t+1} \right) \\ &> (f'(\gamma_i^{t+1}) - k_i) \left(P_i h_i \left(\frac{B_t}{\sigma^2} \frac{q_2}{q_1} + \sum_{j \in \mathcal{N}} \frac{1}{P_j h_j} \gamma_j^{min} \right) \right). \end{aligned}$$

It follows that:

$$||J||_\infty < \max_{i \in \mathcal{N}} \left\{ \sum_{j \in \mathcal{N}, j \neq i} \frac{1}{P_i h_i} \frac{1}{\left(\frac{B_t}{\sigma^2} \frac{q_2}{q_1} + \sum_{j \in \mathcal{N}} \frac{\gamma_j^{min}}{P_j h_j} \right)} \left| \frac{f'(\gamma_i^{t+1}) - k_i}{f''(\gamma_i^{t+1})} \right| \right\}.$$

Let $R_i(\gamma_i^{t+1}) \triangleq \frac{f'(\gamma_i^{t+1}) - k_i}{f''(\gamma_i^{t+1})}$, we have

$$R_i'(\gamma_i^{t+1}) = \frac{(f''(\gamma_i^{t+1}))^2 - f'''(\gamma_i^{t+1})(f'(\gamma_i^{t+1}) - k_i)}{(f''(\gamma_i^{t+1}))^2}.$$

Let $y \triangleq \frac{1}{2}e^{-\frac{\gamma_i^{t+1}}{2}}$, we have

$$\begin{cases} f'(\gamma_i^{t+1}) = \frac{1}{2}Ly(1-y)^{L-1} \\ f''(\gamma_i^{t+1}) = -\frac{1}{4}Ly(1-Ly)(1-y)^{L-2} \\ f'''(\gamma_i^{t+1}) = \frac{1}{8}Ly(1-y)^{L-3}(L^2y^2-(3L-1)y+1) \end{cases}.$$

If $f'''(\gamma_i) > 0$, noticing $L \gg 1$, we have

$$\begin{aligned} (f''(\gamma_i))^2 - f'''(\gamma_i^{t+1})(f'(\gamma_i^{t+1}) - k_i) &> (f''(\gamma_i))^2 - f'''(\gamma_i^{t+1})f'(\gamma_i^{t+1}) \\ &= \frac{1}{64}L^2y^2(1-y)^{2L-4}(L-1)y > 0. \end{aligned}$$

If $f'''(\gamma_i) \leq 0$, we have

$$(f''(\gamma_i))^2 - f'''(\gamma_i^{t+1})(f'(\gamma_i^{t+1}) - k_i) \geq (f''(\gamma_i))^2 > 0.$$

Hence, we always have $R_i'(\gamma_i^{t+1}) > 0$. $R_i(\gamma_i^{t+1})$ is thus monotonously increasing in γ_i^{t+1}. On the other hand, in the beginning of the proof, we have shown that under the condition $k_i > \frac{1}{2ln(L/2)}$, $f''(\gamma_i) < 0$ for $\gamma_i \in [\gamma_i^{min}, \gamma_i^{max}]$. Noticing $R_i(\gamma_i^*) = 0$, we have

$$\max_{\gamma_i \in (\gamma_i^{min}, \gamma_i^*)} \left|R_i(\gamma_i^{t+1})\right| < -R_i(\gamma_i^{min}) = \frac{k_i - f'(\gamma_i^{min})}{f''(\gamma_i^{min})}.$$

Therefore, $||J||_\infty < \max_{i \in \mathcal{N}} \left\{ \sum_{j \in \mathcal{N}, j \neq i} \frac{1}{P_i h_i} \frac{k_i - f'(\gamma_i^{min})}{\left(\frac{B_t}{\sigma^2}\frac{q_2}{q_1} + \sum_{j \in \mathcal{N}} \frac{\gamma_j^{min}}{P_j h_j}\right) f''(\gamma_i^{min})} \right\}$.

Let $k \triangleq \max_{i \in \mathcal{N}} \left\{ \sum_{j \in \mathcal{N}, j \neq i} \frac{1}{P_i h_i} \frac{k_i - f'(\gamma_i^{min})}{\left(\frac{B_t}{\sigma^2}\frac{q_2}{q_1} + \sum_{j \in \mathcal{N}} \frac{\gamma_j^{min}}{P_j h_j}\right) f''(\gamma_i^{min})} \right\}$, if the condition in the theorem is met, i.e., $k < 1$, then we have $||J||_\infty < k < 1$, the best response function $\mathbf{b}$ is a contraction. Both the uniqueness and the convergence is guaranteed.

3.8.4 Proof of Theorem 3.3

Following the same way as Lemma 3.3, we can prove that at each iteration, the update function (3.3) admits a unique solution $\gamma_i \in (\gamma_i^{min}, \gamma_i^*)$.

Moreover, following the same mathematical operation as that in Theorem 3.2, we can calculate the Jacobian of (3.3) $J' = \{J'_{ij}\}$ as

$$J'_{ij} = \begin{cases} -\frac{P_i h_i}{P_j h_j} \frac{(f'(\gamma_i^{t+1}) - k_i)^2}{\left[\sum_{r \in \mathcal{N}}^{r \neq i} \frac{\alpha_r^1}{\alpha_i^1}(f(\gamma_r^t) - k_i\gamma_r^t) + f(\gamma_i^{t+1}) - k_i\gamma_i^{t+1}\right] f''(\gamma_i^{t+1})} & i \neq j \\ 0 & i = j \end{cases}.$$

Noticing that $f(\gamma_r^t) - k_i\gamma_r^t > 0$ for $\gamma_r \in (\gamma_r^{min}, \gamma_r^*), \forall r \in \mathcal{N}$, it holds that $0 < J'_{ij} < J_{ij}$ for $i \neq j$, where $\{J_{ij}\} = J$ is the Jacobian of (3.4) derived in Section 3.8.3. It follows that $||J'||_\infty < ||J||_\infty$.

If the condition of Theorem 3.2 holds, $||J'||_\infty < ||J||_\infty < k < 1$. (3.3) is a contraction. Theorem 3.3 is proven.

3.8.5 Proof of Corollary 3.2

We rewrite the best response function for γ_i and $\widehat{\gamma}_i$ as

$$\begin{cases} P_i \dfrac{h_i B_t}{\sigma^2}\dfrac{q_2}{q_1} + \displaystyle\sum_{j\in\mathcal{N},j\neq i} \dfrac{P_i h_i}{P_j h_j}\gamma_j^t = \dfrac{f(\gamma_i^{t+1}) - k_i\gamma_i^{t+1}}{f'(\gamma_i^{t+1}) - k_i} - \gamma_i^{t+1} \triangleq g(\gamma_i^{t+1}) \\ P_i \dfrac{h_i B_t}{\sigma^2}\dfrac{q_2}{q_1} + \displaystyle\sum_{j\in\mathcal{N},j\neq i} \dfrac{P_i h_i}{P_j h_j}\widehat{\gamma}_j{}^t = \dfrac{f(\widehat{\gamma}_i{}^{t+1}) - k_i\widehat{\gamma}_i{}^{t+1} + \sum_{j\in\mathcal{N},j\neq i}\frac{\alpha_j^1}{\alpha_i^1}(f(\gamma_j^t) - k_j\gamma_j^t)}{f'(\widehat{\gamma}_i{}^{t+1}) - k_i} - \widehat{\gamma}_i{}^{t+1} \triangleq \widehat{g}(\gamma_i^{t+1}) \end{cases}.$$

As in the proof of Lemma 3.3, we can show that under the condition of Theorem 3.2, both $g(\gamma_i)$ and $\widehat{g}(\gamma_i)$ is monotonously increasing in γ_i and $g(\gamma_i) < \widehat{g}(\widehat{\gamma}_i)$ if $\gamma_i = \widehat{\gamma}_i$. Moreover, in the same way as Lemma 3.3, we can prove that $\gamma_i^{min} < \widehat{\gamma}_i < \gamma_i^*$, $\forall i \in \mathcal{N}$.

We now prove by contradiction that if $\gamma_j^t \geq \widehat{\gamma}_j{}^t$, $\forall j \in \mathcal{N}, j \neq i$, then $\gamma_i^{t+1} > \widehat{\gamma}_i{}^{t+1}$. Otherwise, assume by contradiction that $\gamma_j^t \geq \widehat{\gamma}_j{}^t$, $\forall j \in \mathcal{N}, j \neq i$ and $\gamma_i^{t+1} \leq \widehat{\gamma}_i{}^{t+1}$. It follows that $g(\gamma_i^{t+1}) < \widehat{g}(\gamma_i^{t+1}) < \widehat{g}(\widehat{\gamma}_i{}^{t+1})$, thus we have

$$P_i \frac{h_i B_t}{\sigma^2}\frac{q_2}{q_1} + \sum_{j\in\mathcal{N},j\neq i} \frac{P_i h_i}{P_j h_j}\gamma_j^t < P_i \frac{h_i B_t}{\sigma^2}\frac{q_2}{q_1} + \sum_{j\in\mathcal{N},j\neq i} \frac{P_i h_i}{P_j h_j}\widehat{\gamma}_j{}^t,$$

which contradicts with the assumption that $\gamma_j^t \geq \widehat{\gamma}_j{}^t$, $\forall j \in \mathcal{N}, j \neq i$.

Therefore, starting with the same initial value $\gamma^0 = \widehat{\gamma}^0$, at each iteration t, it holds that $\gamma_i^t > \widehat{\gamma}_i{}^t$. Consequently, we have

$$\gamma_i = \lim_{t\to\infty} \gamma_i \geq \lim_{t\to\infty} \widehat{\gamma}_i{}^t = \widehat{\gamma}_i \quad \forall i \in \mathcal{N}.$$

Furthermore, noticing that it is impossible that $\widehat{\gamma} = \gamma$ for $\widehat{\gamma}_i, \gamma_i \in (\gamma_i^{min}, \gamma_i^*)$, it then holds that $\gamma_i > \widehat{\gamma}_i, \forall i \in \mathcal{N}$.

3.8.6 Proof of Theorem 3.8

For a sequence of non-empty sets $\{\mathbf{X}(\mathbf{k})\}$ with

$$\cdots \subset \mathbf{X}(\mathbf{k}+\mathbf{1}) \subset \mathbf{X}(\mathbf{k}) \subset \cdots \subset \mathbf{X}$$

satisfying the following two conditions:

- *Synchronous Convergence Condition:* We have $\mathbf{f}(\mathbf{x}) \in \mathbf{X}(\mathbf{k}+\mathbf{1}), \forall k$ and $\mathbf{x} \in \mathbf{X}(\mathbf{k})$.

  Furthermore, if $\{\mathbf{y^k}\}$ is a sequence such that $\mathbf{y^k} \in \mathbf{X}(\mathbf{k})$ for every k, then every limit point of $\{\mathbf{y^k}\}$ is a fixed point of $\mathbf{f}$.

- *Box Condition:* For every k, there exists sets $X_i(k) \subset X_i$ such that

$$\mathbf{X}(\mathbf{k}) = X_1(k) \times X_2(k) \times \cdots \times X_n(k)$$

and $\mathbf{x}(\mathbf{0}) = \{x_i(0), i = 1, 2, \cdots, n\} \in \mathbf{X}(\mathbf{0})$, the *Asynchronous Convergence Theorem* [BT97] states that every limit point of $\{\mathbf{x}(\mathbf{t})\}$ is a fixed point of $\mathbf{f}$.

Applying the above results in our context, let $\mathbf{X}(\mathbf{k}) \stackrel{\triangle}{=} \times_{i\in\mathcal{N}}[x_i^* - \delta(k), x_i^* + \delta(k)]$ where $\delta(k) = \max_{i\in} |\gamma_i^k - \gamma_i^*|$, $\mathbf{f}$ denote the mapping from $\{\gamma_i^t\}$ to $\{\gamma_i^{t+1}\}$ in the subgradient update scheme, $X_i = [\gamma_i^{min}, \gamma_i^{max}], i \in \mathcal{N}$, we can verify that $\{\mathbf{X}(\mathbf{k})\}$ satisfies the box condition. Moreover, in the analysis in Section 3.5.1, we have shown that $\delta(k)$ is monotonously decreasing in k under the condition in Theorem 3.7, thereby the synchronous convergence condition is also satisfied. Hence following from the asynchronous convergence theorem, γ_i converges to γ_i^*. Noticing that U_i is independent to P_{-i} and P_i is a linear function of γ_i, the subgradient update scheme defined in Theorem 3.7 converges to the unique NE, which is also the social optimal point.

Chapter 4

A Pricing Framework for Cooperative Relaying in Wireless Networks with Selfish Nodes[1]

4.1 Introduction

Cooperative relaying has emerged in recent years as an important technique for wireless networks with unstable links. Cooperative relaying takes advantage of the broadcast nature of the wireless medium and provides additional diversity against link outages (caused, e.g., by dynamic fading or shadowing effects) by allowing nodes in the vicinity of the link endpoints, which overhear the transmitted signal, to make additional transmissions to assist in delivering the data to its destination. The extensive research on the topic has resulted in a wide variety of proposed cooperation methods. For a single relay, these range from simple *decode-and-forward* of the data packet itself [NHH04, LLG06] to *coded cooperation* where the relay transmits additional error-correcting code bits rather than retransmitting the original data [HN06]. Similar ideas have been extended to multiple-relay cooperation, where the receiver decodes the data by combining the relayed signals received either over separate multiplexed subchannels (e.g. CDMA [SEA03] or TDMA [LTW04]), or over the same subchannel with multiple receiving antennas using space-time codes [LW03, JHHN04].

Despite the ample research literature on cooperative relaying, virtually all studies in this area have tackled the issue from an optimization perspective, assuming that the relay nodes are willing to help the source and ignoring the issue of cooperation *incentive* for the relay nodes. This assumption is clearly inadequate in networks with selfish nodes, which may not be willing to relay packets for other nodes, e.g. due to the energy cost they incur in the process. In light of the established importance of cooperative relaying for enhancing throughput and reliability in wireless environments with unstable links, it is imperative to attend to the question of how to provide the necessary incentives for selfish relay nodes to take part in cooperative relaying.

Motivated by the above observation, we propose a pricing framework based on the idea of "pay for cooperation" to encourage cooperation by relay nodes. Under this framework, each flow (corresponding to a source-destination pair) offers a payment per successfully received packet, which is shared equally among all cooperative nodes that participated in the relaying of that

[1]Part of the work in this chapter was done while visiting NICTA.

packet. Hence, the utility of a relay node is defined as its share of received payment minus its own cost of cooperation (e.g. due to energy spent for relaying). For a flow, the utility is defined as a generic concave function of the packet delivery rate minus the cost paid to the relay nodes. We model the resulting scenario as a Stackelberg game [Mye91], in which the relay nodes are the *followers* that respond to payment rates set by the flows (i.e. each relay chooses which flow or mix of flows to serve so as to maximize its utility, given the payment rates offered by the flows and the actions of its competing peers); and the flows are the *leaders* that set the payment rates to maximize their own utility in anticipation of the Nash equilibrium (NE) response of the followers.

The idea of pricing as a control mechanism, to encourage selfish network users to make decisions resulting in a social benefit for the entire network, has a long history. Its greatest success has been in the so-called Network Utility Maximization (NUM) framework, which originally developed from the seminal work by Kelly *et al* [KMT98] and has since been widely used in the contexts of congestion control and routing in the Internet (cf. [TWSC07, WLLD03] and references therein), as well as power and rate control in wireless networks [SMG02b, CL08]. In NUM, the network sets *shadow prices* for using its resources, while the users respond to those prices by adjusting their actions (e.g. flow rates). In many scenarios, the prices can be set in such a manner that the resulting individual optimization by the selfish users coincides with the distributed optimization of the network operating point. However, the NUM framework cannot be easily extended to ad hoc wireless networks with selfish nodes, since there is no independent entity of a "network" that can set prices for using its resources; rather, the network itself is comprised of the selfish nodes, and the distinction between the network "resources" and "users" is blurred.

Accordingly, the research on incentives in ad hoc networks has predominantly focused on encouraging honest forwarding of other nodes' packets through *reputation* and *credit*-based schemes (cf. [JS07] and references therein). Such schemes can be enforced in a traditional forwarding context, where node can detect whether their neighbors are honest simply by overhearing the respective transmissions. However, reputation-based methods are largely unsuitable in the context of cooperative relaying used to provide diversity against unstable links, since it is impossible to distinguish between a neighbor's selfish failure to relay a packet and an "innocent" case of a bad channel to that neighbor.

On the other hand, only a handful of recent studies have considered pricing in the context of ad hoc networks with selfish nodes, where nodes are paid for forwarding other nodes' packets and in turn pay their neighbors to forward theirs, with the payment rate determined by an auction or market-based scheme [MQ05, ZLLY07a, XY08]. These studies, as well as the one in this chapter, can be seen as adaptations of the "smart-market" mechanism originally proposed in [MMV94] in the context of Internet congestion management, where sources of flows bid for the amount they are willing to pay to have them delivered, so that the limited shared network resources (e.g. congested links in the Internet or relay nodes in ad hoc networks) are used to serve the highest bidders. However, to the best of our knowledge, the pricing framework we study in this chapter is the first to be applied to the cooperative relaying context, which introduces several important original features that distinguish it from any related methods studied in the past. First, unlike most pricing methods in existing literature that only involve one kind of selfish players, in our framework there are two types of players (the relay nodes and the flows), each of which is not only in competition with its peers but also with players of the other type, resembling a commodity market with multiple providers and clients. Furthermore, in most existing studies on pricing, the

expected utility of a player depends only on its own strategy once the prices are set, whereas in our case the payment from a flow is shared among all relay nodes participating in the relaying of that flow. As a result, a node's utility depends on the strategies of its peers, which leads to a competition scenario with more complex interactions among the players. Finally, we point out that the sharing of payment leads to relay utility functions that are non-concave, requiring an original study of the game equilibrium properties that cannot draw on existing well-known results.

Our contribution is twofold. First, we present a detailed study of the Stackelberg game involving the flows and relay nodes and its equilibrium properties. Specifically, we establish that the followers' game admits two types of Nash equilibria, including a unique symmetrical NE where all relay nodes play the same strategy (i.e. relay the same mix of flows), and a boundary NE where each relay node is fully dedicated to a single flow. We further establish that, from the leaders' perspective, a Stackelberg equilibrium does not exist if the followers play the boundary NE, yet it always exists if the followers converge to the symmetrical NE. We emphasize that these properties are substantially different from any other pricing method proposed in the literature. We then conduct a numerical study that demonstrates the prices and utilities achieved in several scenarios, and show that the equilibrium in general is reasonably efficient (i.e. has a low "price of anarchy" [Pap01]).

The rest of this chapter is structured as follows. Section 4.2 presents our system model and pricing framework and formulates the Stackelberg cooperative relaying game. Section 4.3 analyzes the properties of the followers' game and the corresponding equilibria, while Section 4.4 investigates the existence of an equilibrium in the leaders' game. Section 4.5 demonstrates the efficiency of the resulting equilibria with a numerical study of several scenarios. Finally, the chapter is concluded in Section 4.6.

4.2 System Model and Pricing Framework

4.2.1 Wireless network model

We consider a set $\mathcal{F}$ of flows in a synchronized slotted wireless network. We use S_f and D_f to denote the source and destination of flow $f \in \mathcal{F}$, respectively. Each flow transmits a continuous stream of packets, where each packet from any flow takes an identical transmission time (a slot). A set $\mathcal{R}$ of *relay nodes*, with $|\mathcal{R}| = R \geq 2$, serve as potential cooperative relays that may assist packets to reach their destinations by retransmitting them. We assume that the different flows coexist on different "channels" in the network, which can be, e.g., CDMA or FDMA. Thus, if relay node $i \in \mathcal{R}$ decides to cooperate with flow f, it must tune itself to receive the packets from S_f; a node cannot overhear multiple flows simultaneously. All nodes cooperating with flow f relay each packet from that flow to D_f immediately after receiving the packet, i.e. simultaneously to each other. We assume that the different relay signals do not mutually interfere; e.g., they can be multiplexed on separate sub-channels (as in [SEA03, LTW04]) or based on space-time coding with multiple antennas at the receiver [JHHN04]. Therefore, the packet is considered successfully received if it can be decoded error-free from at least one of the relay transmissions. (We do not consider coded cooperation in this chapter, where relay transmissions consist of error-correcting code bits rather than the packet data itself, so that the packet can be recovered from the combination of relay signals even if no individual one is error-free; this extension is left to future work.)

Accordingly, we consider a simple channel model in which any channel is either "good", which allows the transmitted packet to be decoded without error, or "bad" otherwise. We assume channels

between different pairs of nodes are mutually independent, which is realistic in most practical scenarios as long as nodes are spaced sufficiently far apart (i.e. by more than a wavelength of the carrier frequency). For the sake of simplicity, the analysis in this chapter assumes channels that are memoryless on the packet time scale (i.e. probability of being in the "good" state is fixed and independent between subsequent packet transmissions) We denote this probability by P_{sn}^f for the channel between S_f and any relay node, and P_{nd}^f for the channel between any relay node and D_f. Thus, we assume a symmetrical setting where channel probabilities are identical *a priori* among all relays (though not necessarily among all flows). The extension of our analysis to asymmetrical relay nodes is left for future work.

4.2.2 Pricing framework

We denote the cost (e.g. in terms of energy) for a relay node to transmit a packet from flow f by e^f. For a selfish relay node to make a cooperative transmission, it must expect to receive a payment in return that is greater than its energy cost. Each flow f offers a payment of C^f per successful packet, where C^f is decided by the flow itself (i.e. C^f is the *strategy*) of f). Hence, the utility function of flow $f \in \mathcal{F}$ is defined as the net payoff f gets per slot:

$$U_f \triangleq u_f(P_{suc}^f) - C^f P_{suc}^f, \tag{4.1}$$

where $P_{suc}^f = 1 - \prod_{i\in\mathcal{R}}(1 - P_{sn}^f P_{nd}^f r_i^f)$ is the probability that a packet of f successfully arrives at its destination, with r_i^f being the probability that relay node i cooperates with f. The function $u_f(P_{suc}^f)$ characterizes the application payoff (e.g. satisfaction level) of f from a delivery probability of P_{suc}^f. We assume $u_f(P_{suc}^f)$ is continuously differentiable, strictly increasing and weakly concave in P_{suc}^f (i.e. $u_f''(P_{suc}^f) \leq 0$), with $u_f(0) = 0$.

We now turn to the utility function of the relay nodes. If a packet is successful, the payment of C^f is shared equally among all nodes that successfully relayed it to D_f.[2] We denote by r_i^f the probability of relay i to retransmit a packet from flow f; thus, the vector $\mathbf{r_i} = \left\{r_i^f, f \in \mathcal{F}\right\}$, where $\sum_f r_i^f \leq 1$, is the *strategy* of relay node i. For brevity, we henceforth denote $K^f \triangleq P_{sn}^f P_{nd}^f$. Thus, the expected payoff for a relay node i in a slot is

$$V_i \triangleq \sum_{f\in\mathcal{F}} C^f K^f r_i^f \sum_{l=0}^{R-1} \frac{P^f(l)}{l+1} - e^f r_i^f, \tag{4.2}$$

where

$$P^f(l) \triangleq \sum_{\substack{\mathcal{T}\subseteq\mathcal{R}-\{i\} \\ |\mathcal{T}|=l}} \prod_{j_1\in\mathcal{T}} K^f r_{j_1}^f \prod_{\substack{j_2\notin\mathcal{T} \\ j_2\neq i}} (1 - K^f r_{j_2}^f)$$

is the probability that there are l additional nodes beside i that successfully relay the packet of f to its destination as well.

[2] We assume that the flow endpoints are honest, and indeed make the payments in equal shares to all successful relay nodes, as detected by D_f. We do not consider further the issue of *payment enforcement*, which may require a separate mechanism e.g. via a reputation-like metric where the relay nodes monitor the payment rate over time, and refuse to cooperate with flows that deviate too much from the value to be expected from the channel characteristics. The investigation of such payment enforcement schemes is beyond the scope of our work in this chapter.

4.2.3 Stackelberg game formulation

We model the cooperative relaying with pricing as a *Stackelberg game*, in which the *leaders* choose their strategy first, and the *followers* respond by choosing their strategies accordingly, knowing the leaders' strategies [Mye91]. In our setting, the game is defined as follows.

Follower's Problem:

Each follower (relay node i) chooses its strategy $\mathbf{r_i}$ to maximize its utility V_i in response to the given leaders' strategies $\mathbf{C} \triangleq \{C^f, f \in \mathcal{F}\}$ and the strategies of its peers $\mathbf{r_{-i}} \triangleq \{\mathbf{r_j}, j \neq i\}$. Thus, each relay node i solves the following problem:

$$\mathbf{r_i^*}(\mathbf{r_{-i}}, \mathbf{C}) = \operatorname{argmax} V_i(\mathbf{r_i}, \mathbf{r_{-i}}, \mathbf{C}), \tag{4.3}$$

and a vector of followers' strategies is a Nash equilibrium (NE) if it corresponds to a fixed point of (4.3).

Leader's Problem:

Each leader (source-destination pair corresponding to a flow f) chooses its strategy C^f to maximize its utility function U_f, given the strategies of its peers $\mathbf{C^{-f}} \triangleq \{C^{f'}, f' \neq f\}$ and anticipating that the followers will eventually respond with strategies that result in an NE according to (4.3). Thus, the leader's problem is described as

$$C^{f\,*} = \operatorname{argmax} U_f(C^f, \mathbf{C^{-f}}, \mathbf{r_i^*}(\langle C^f, \mathbf{C^{-f}} \rangle)). \tag{4.4}$$

The solution of the game is characterized by the *Stackelberg-Nash equilibrium (SNE)*, a strategy profile from which no player (leader or follower) has incentive to deviate unilaterally.

4.3 Equilibrium Analysis of the Followers' Game

The goal of our subsequent analysis is to find and characterize the properties of the SNE of the above game. To that end, we first study the followers' game and obtain the best response strategies and equilibrium properties for a given vector of leaders' strategies $\mathbf{C}$. Before proceeding, we point out that there exist generic well-known properties (e.g. equilibrium existence and uniqueness) for games with concave utility functions, which do not hold in our case since, in general, the relay utility V_i is not concave. To see this, consider the simple example of a single flow served by three nodes over perfectly reliable links ($K^f = 1$) with $C^f = 1$ and $e^f = 0$. Then, the utility function of relay node 1 reduces to

$$V_1 = r_1 \left[(1 - r_2)(1 - r_3) + \frac{r_2 + r_3 - 2r_2r_3}{2} + \frac{r_2 r_3}{3} \right],$$

which is in fact non-concave; for example, $V_1 \binom{r_1=1}{r_2=0.5}{r_3=0.5} = \frac{7}{12} < \frac{1}{2}\left[V_1 \binom{r_1=1}{r_2=0}{r_3=0} + V_1 \binom{r_1=1}{r_2=1}{r_3=1}\right] = \frac{2}{3}$. As a result, we resort to establishing the game properties using a direct analysis, without drawing on any prior theoretical results.

Before proceeding, we present a simple yet insightful example that demonstrates some of the properties to be rigorously proved later.

Example 1. *Consider a system with two flows offering identical payments of $C^1 = C^2 = 1$, $e^1 = e^2 = 0$, and two relay nodes with perfectly reliable links. In this system, there are three*

equilibria in the followers' game:

- $\mathbf{r_1} = \mathbf{r_2} = (\frac{1}{2}, \frac{1}{2})$ *(i.e. each node allocates half of its cooperation to each of the flows). To see that this is an NE, note that, for* $\mathbf{r_2}$ *fixed at* $(\frac{1}{2}, \frac{1}{2})$*, the utility function of node 1 reduces to* $V_1 = (r_1^1 + r_1^2) \cdot (\frac{1}{2} + \frac{1}{4})$*, which is maximized by any strategy with* $r_1^1 + r_1^2 = 1$ *(intuitively, the node maximizes the received payment by increasing its cooperation effort to the maximum, and is indifferent between the two flows). The same logic holds for node 2 with* $\mathbf{r_1}$ *fixed. We refer to this NE, where all nodes apply an identical strategy, as the* symmetrical *NE*

- $\mathbf{r_1} = (1, 0)$, $\mathbf{r_2} = (0, 1)$ *or vice versa (two equilibria that are identical up to permutation of the nodes). Indeed, when each node cooperates with one flow, there is no incentive for any of them to deviate by shifting some of the cooperation probability to the other flow, where the expected payment rate is lower due to competition with the other node. We refer to such an NE, where every node cooperates only with one flow, as a* boundary *NE.*

It is easily confirmed that no other equilibria exist in this system.

As we prove below, this simple system is indicative of the followers' game properties in general. Indeed, the main result of this section is that, in any system and for any vector $\mathbf{C}$*, the game always admits a unique symmetrical equilibrium, as well as at least one boundary equilibrium.*

4.3.1 Symmetrical Equilibria

We focus first on *symmetrical* strategy profiles, where all nodes use identical strategies. To that end, we define the function

$$g^f(x) \triangleq \left. \frac{\partial V_i}{\partial r_i^f} \right|_{r_j^f = x, \forall j \in \mathcal{R}} \tag{4.5}$$

(note the index i is dropped from the function definition since it does not depend on the choice of any specific i). This can be simplified as

$$g^f(x) = C^f K^f \sum_{l=0}^{R-1} \frac{1}{l+1} \binom{R-1}{l} (K^f x)^l (1 - K^f x)^{R-1-l} - e^f = C^f \frac{1 - (1 - K^f x)^R}{Rx} - e^f. \tag{4.6}$$

In particular, we note that $g^f(0) = C^f K^f - e^f$ and $g^f(1) = \frac{C^f K^f}{R} - e^f$. For convenience, we also define $h^f(x) \triangleq \frac{1-(1-K^f x)^R}{Rx}$; thus $g^f(x) = C^f h^f(x) - e^f$.

We state some monotonicity properties that will be useful in several subsequent proofs.

Lemma 4.1. *The following monotonicity properties hold:*

- $g^f(x)$ *and* $h^f(x)$ *are strictly decreasing in* x*;*
- $h'^f(x) = \frac{dh^f(x)}{dx}$ *is strictly increasing in* x*;*
- $\frac{h'^f(x)}{[h^f(x)]^2}$ *is strictly decreasing in* x*.*

Proof. Please refer to Section 4.7.1 for the detailed proof. □

We now state the first major result of this subsection.

Theorem 4.1. *For any vector of flow prices* $\mathbf{C}$*, there exist* $\{\rho^f, f \in \mathcal{F}\}$ *such that the symmetrical strategy profile* $r_j^f = \rho^f, \forall j \in \mathcal{R}$ *is a Nash equilibrium. Furthermore, there exist* $\lambda \geq 0, \{\mu^f \geq 0, f \in \mathcal{F}\}$*, such that:*

$$g^f(\rho^f) = \lambda - \mu^f \quad \forall f \in \mathcal{F} \tag{4.7}$$

$$\lambda \left(\sum_{f \in \mathcal{F}} \rho^f - 1 \right) = 0 \tag{4.8}$$

$$\mu^f \rho^f = 0 \quad \forall f \in \mathcal{F} \tag{4.9}$$

Proof. First, we show that a set of $\{\rho^f\}$, λ, and $\{\mu^f\}$ satisfying conditions (4.7)-(4.9) exists. To that end, define the function $V(\mathbf{x})$, where $\mathbf{x} = \left(x^1, \ldots, x^{|\mathcal{F}|}\right)$, as follows: $V(\mathbf{x}) \triangleq \sum_{f \in \mathcal{F}} \int_0^{x^f} g^f(\xi) d\xi$. Consider the following optimization problem:

$$\max_{\mathbf{x}} V(\mathbf{x}) \quad s.t. \quad \sum_{f \in \mathcal{F}} x^f \leq 1 \text{ and } x^f \geq 0, \forall f \in \mathcal{F}$$

Since $V(\mathbf{x})$ is obviously continuously differentiable, the above constrained optimization problem (defined over a compact region) must have a solution, which can be denoted by $\{\rho^f, f \in \mathcal{F}\}$. This solution must satisfy the corresponding Kuhn-Tucker conditions, which are precisely the conditions listed in (4.7)-(4.9).

Next, we show that the strategy profile defined by the above conditions corresponds to an NE, i.e., $\{\rho^f\}$ is the best-response strategy for any node i if all other nodes play the same strategy. Accordingly, consider the corresponding optimization problem from the perspective of node i, with the strategy $\mathbf{r_i} = \left(r_i^1, \ldots, r_i^{|\mathcal{F}|}\right)$:

$$\max_{\mathbf{r_i}} V_i(\mathbf{r_i}, \mathbf{r_{-i}}) \quad s.t. \quad \sum_{f \in \mathcal{F}} r_i^f \leq 1 \text{ and } r_i^f \geq 0. \forall f \in \mathcal{F} \tag{4.10}$$

We note from (4.2) that, for a fixed $\mathbf{r_{-i}}$, the target function $V_i(\mathbf{r_i}, \mathbf{r_{-i}})$ is linear in $\mathbf{r_i}$ (indeed, the coefficient of each r_i^f is constant). This implies that the first-order Kuhn-Tucker conditions corresponding to problem (4.10) are sufficient for optimality. However, since $\left.\frac{\partial V_i}{\partial r_i^f}\right|_{r_i^f = \rho^f, \mathbf{r_{-i}}} = g^f(\rho^f)$ at the symmetrical strategy profile, these Kuhn-Tucker conditions coincide with those stated by (4.7)-(4.9). Hence, $\{\rho^f, f \in \mathcal{F}\}$ is indeed the best-response strategy for any node i, and therefore it is an NE. □

We now proceed to the second major result of this subsection, namely, the uniqueness of the symmetrical equilibrium.

Theorem 4.2. *For any vector of flow prices* $\mathbf{C}$*, the symmetrical equilibrium in the corresponding followers' game is unique.*

Proof. By definition, an equilibrium strategy profile must solve the optimization problem defined in (4.10) for each relay node i. Since V_i is continuously differentiable in r_i^f, it follows that the first-order Kuhn-Tucker conditions are necessary for optimality. Thus, there must exist $\lambda_i \geq 0$ and

$\{\mu_i^f \geq 0, f \in \mathcal{F}\}$ such that the following conditions are satisfied:

$$\frac{\partial V_i}{\partial r_i^f} = \lambda_i - \mu_i^f \quad \forall f \in \mathcal{F} \tag{4.11}$$

$$\lambda_i \left(\sum_{f \in \mathcal{F}} r_i^f - 1 \right) = 0 \tag{4.12}$$

$$\mu_i^f r_i^f = 0 \tag{4.13}$$

We now show by contradiction that there exists at most one symmetrical equilibrium. Suppose that, to the contrary, there exist two different sets $\{\rho_a^f, f \in \mathcal{F}\} \neq \{\rho_b^f, f \in \mathcal{F}\}$ such that the assignments of either $r_i^f = \rho_a^f, \forall i \in \mathcal{R}, \forall f \in \mathcal{F}$ or $r_i^f = \rho_b^f, \forall i \in \mathcal{R}, \forall f \in \mathcal{F}$ both satisfy conditions (4.11)–(4.13). Since the equilibria are symmetrical, the Lagrange multipliers must be identical for all relay nodes, therefore the node index may henceforth be dropped. Accordingly, we denote the Lagrange multipliers corresponding to the two equilibria by $\lambda_a, \lambda_b, \{\mu_a^f\}, \{\mu_b^f\}$, respectively.

Without loss of generality, assume that $\rho_a^{f_1} > \rho_b^{f_1}$ for some $f_1 \in \mathcal{F}$. Then, by (4.13), we have $\mu_a^{f_1} = 0$, and by (4.11),

$$\lambda_a - \left(\lambda_b - \mu_b^{f_1}\right) = \left.\frac{\partial V_i}{\partial r_i^{f_1}}\right|_{r^f = \rho_a^f} - \left.\frac{\partial V_i}{\partial r_i^{f_1}}\right|_{r^f = \rho_b^f} = g^{f_1}\left(\rho_a^{f_1}\right) - g^{f_1}\left(\rho_b^{f_1}\right) < 0,$$

where the last inequality is due to the monotonicity of the function g^{f_1} (Lemma 4.1). Therefore, $\lambda_b > \lambda_a$. Conversely, by the same token, $\rho_a^{f_2} < \rho_b^{f_2}$ for some $f_2 \in \mathcal{F}$ results in $\lambda_a > \lambda_b$. Since both cannot occur simultaneously, we conclude that $\rho_a^{f_1} > \rho_b^{f_1}$ for some $f_1 \in \mathcal{F}$ implies $\rho_a^f \geq \rho_b^f$ for all $f \in \mathcal{F}$. However, $\lambda_b > \lambda_a \geq 0$ implies $\sum_{f \in \mathcal{F}} \rho_b^f = 1$ by (4.12), which leads to the conclusion that $\sum_{f \in \mathcal{F}} \rho_a^f > 1$. Since this is impossible, we conclude that more than one symmetrical equilibrium cannot exist. □

4.3.2 Boundary Equilibria

We now turn our attention to *boundary* strategy profiles, where all strategy components r_i^f are equal to either 0 or 1 for all $i \in \mathcal{R}$, $f \in \mathcal{F}$. Our main result in this subsection concerns the existence of boundary equilibria.

Theorem 4.3. *For any vector of flow prices* $\mathbf{C}$*, there exists a boundary equilibrium in the corresponding followers' game.*

Proof. First, we introduce a "dummy" flow f_0 with $C^{f_0} = 0$ and $e^{f_0} = 0$, such that any node with less than full allocation of cooperation (i.e. $\sum_{f \in \mathcal{F}} r_i^f < 1$ will be indifferent to allocating any part of the remaining slack to the dummy flow, since the utility from cooperation with that flow is always 0. The purpose of introducing the dummy flow is to allow consistent notation in the following proof. Thus, if a node's best strategy is not to cooperate with any flow at all because all flows offer negative expected utilities (i.e. payments that are lower than the energy cost), then the node can instead be said to be fully cooperating with the dummy flow.

We now construct a simple algorithm that finds a boundary equilibrium, as follows. Initially, start with the strategy $r_i^f = 0$ for all $i \in \mathcal{R}$,$f \in \mathcal{F}$. Thereafter, proceed with R iterations to assign the relay nodes to flows, where in each iteration $k = 1, \ldots, R$,

- denote $R^f = \sum_i r_i^f$, $f \in \mathcal{F}$, to be the number of nodes assigned to flow f so far;
- find the flow f^* such that setting $r_k^{f^*} = 1$ maximizes V_k;
- assign $r_k^{f^*} = 1$.

We elaborate on the second step in the above. From (4.2), if node k is assigned to flow f in the iteration where R^f other nodes already allocate a strategy probability of 1 to that flow, then the node's utility will be

$$C^f K^f \sum_{l=0}^{R^f} \frac{1}{l+1} \binom{R^f}{l} (K^f)^l (1-K^f)^{R^f-l} - e^f = C^f \cdot \frac{1-(1-K^f)^{R^f+1}}{R^f+1} - e^f, \tag{4.14}$$

and the flow f^* to which node k should be assigned is thus the one that maximizes (4.14) among all flows (including the dummy flow, if necessary) in the iteration.

We now show by induction that after each iteration k, the assignments so far $\{\mathbf{r_i^f}\}$ constitute an equilibrium among relay nodes $i = 1, \ldots, k$. This is clearly true for $k = 1$. Assume that it is true for $k = n$, and consider iteration $n+1$. Let f_{n+1} be the flow chosen by relay node $n+1$. Then, by construction, relay node $n+1$ has been allocated to the flow offering the maximum expected payment share, and has no incentive to deviate any probability to other flows where the expected payment is smaller. Since the relay nodes are symmetric, the same holds for any other node that is assigned to flow f_{n+1} before iteration $n+1$. Now, consider any node j assigned to a flow $f_j \neq f_{n+1}$. Note that the only change from iteration n to $n+1$ is that $R_{f_{n+1}}$ has increased (i.e. f_{n+1} now offers an even lesser payment share per node than before, as (4.14) is decreasing in R_f), and the iteration made no impact on other flows. Therefore, if j had no incentive to deviate from f_j after iteration n, then j will certainly have no incentive to deviate after iteration $n+1$. Therefore, the strategies after each iteration are in equilibrium among the nodes assigned so far, and eventually result in a boundary equilibrium after all R nodes are assigned. □

We point out that, unlike the symmetrical equilibrium, the boundary equilibrium is not guaranteed to be unique (even after allowing for permutation of the nodes). The reason for this is that the flow f^* maximizing expression (4.14) in a particular iteration need not be unique. For example, consider again the system described in Example 1, except that now $C^1 = 2$ and $C^2 = 1$. Applying the algorithm from the proof of Theorem 4.3, the first node is assigned to flow 1, and thereafter, the second node becomes indifferent between the two flows (it can either cooperate with flow 2 and receive the full payment of $C^2 = 1$, or cooperate with flow 1 and receive half of the payment of $C^1 = 2$, with the other half going to the first node). Consequently, $\mathbf{r_1} = (1, 0)$ and either $\mathbf{r_2} = (1, 0)$ or $\mathbf{r_2} = (0, 1)$ are boundary equilibria (in fact, $\mathbf{r_2} = (r_2^1, r_2^2)$ with any $r_2^1 + r_2^2 = 1$ will bring about an equilibrium, albeit not a boundary one).

4.4 Analysis of the Leaders' Game

In this section, we study the properties of the leaders' game and its equilibrium (corresponding to the Stackelberg-Nash equilibrium of the overall system). Our task is complicated by the findings of section 4.3, namely, that once the leaders' strategies $\mathbf{C}$ are set, the followers' equilibrium is not unique. To get around this complication, we first analyze the leaders' game under the assumption that the followers will always respond by playing their symmetrical equilibrium (which is always

unique), and establish the existence of an equilibrium of the leaders' game for any R, $\{K^f\}$ and $\{e^f\}$, $f \in \mathcal{F}$. We then show that the existence property may no longer hold if the followers may play any other equilibrium rather than the symmetrical one; in particular, we establish that the leaders' game never possesses an equilibrium at all if the followers always respond by playing their boundary equilibrium.

4.4.1 Followers play symmetrical equilibrium

We focus on the followers' symmetrical equilibrium defined in Theorem 4.1, and study its dependence on the payment rate C^f of a specific flow $f \in \mathcal{F}$, with all other rates ($\mathbf{C^{-f}}$) fixed. To streamline the discussion, we view the value of ρ^f in the equilibrium corresponding to a setting of C^f as a function $\rho^f = F(C^f)$ (a scalar function, since we focus only on ρ^f and are not interested in the values of ρ for flows other than f). We shall also be interested in the value of λ that satisfies condition (4.8) in the equilibrium, and denote the respective function as $\lambda = \Lambda(C^f)$.

We begin by exploring these functions for extreme values of C^f. Clearly, with $C^f = 0$, the utility of cooperating with flow f for any relay node is non-positive, implying $\rho^f = F(C^f = 0) = 0$. Denote $\lambda_0 = \Lambda(C^f = 0)$; then, if C^f is gradually increased, the equilibrium remains unchanged as long as $g^f(0) = K^f C^f - e^f \leq \lambda_0$, since condition (4.7) can still be satisfied with some $\mu^f \geq 0$. We conclude that $\rho(C^f) = 0$ and $\Lambda(C^f) = \lambda_0$ for all $C^f \leq C^f_{\min} \triangleq \frac{\lambda_0 + e^f}{K^f}$.

On the other hand, if C^f is very large (more precisely, $C^f \geq C^f_{\max} \triangleq \left[\left(\max_{f' \neq f} C^{f'} K^{f'} - e^{f'}\right) + e^f\right] \frac{R}{K^f}$, which implies that $g^f(1) = \frac{K^f C^f}{R} - e^f \geq g^{f'}(0) = C^{f'} K^{f'} - e^{f'}$ for any $f' \neq f$), then the equilibrium conditions will be satisfied by $\rho^f = F(C^f) = 1$ and $\lambda = \Lambda(C^f) = g^f(1)$, with $\mu^{f'} > 0$ and therefore $\rho^{f'} = 0$ for all $f' \neq f$. Intuitively, if C^f is so large that even a share of $\frac{1}{R}$ of the payment from f is larger than the payment from any other flow, then no node will deviate from cooperating fully with f.

We now proceed to explore the behavior of $F(C^f)$ and $\Lambda(C^f)$ between these extremes, i.e. in the range $C^f_{\min} \leq C^f \leq C^f_{\max}$.

Lemma 4.2. *The function $\Lambda(C^f)$ is continuous and non-decreasing in C^f.*

Proof. Please refer to Section 4.7.2 for the detailed proof. □

Lemma 4.3. *The function $F(C^f)$ is continuous, and, in the range $C^f_{\min} \leq C^f \leq C^f_{\max}$, strictly increasing in C^f.*

Proof. Again, the continuity of ρ^f with respect to C^f is immediate from the continuity of g^f and conditions (4.7)-(4.9). We now prove the monotonicity. For convenience, we denote the function $g^f(\cdot)$ corresponding to C^f_1 and C^f_2 by $g^f_1(\cdot)$ and $g^f_2(\cdot)$, respectively. Now, consider the following alternatives.

- $\Lambda(C^f_2) = 0$. By lemma 4.2, this implies $\Lambda(C^f_1) = 0$ as well. In both equilibria (corresponding to C^f_1 and to C^f_2), since $g^f(0) \geq 0$ (by the definition of $C^f_{\min}$ and the fact that both $C^f_{\min} \leq C^f_1$ and $C^f_{\min} \leq C^f_2$), it follows that condition (4.7) cannot be satisfied with $g(\rho^f) < 0$ (since that would require $\rho^f > 0$ and therefore $\mu^f = 0$). Hence, $g^f(\rho^f) = 0$ in both equilibria. It follows that
$$C^f_1 K^f \frac{1 - (1 - K^f \rho^f_1)^R}{R K^f \rho^f_1} = C^f_2 K^f \frac{1 - (1 - K^f \rho^f_2)^R}{R K^f \rho^f_2},$$
which, if $C^f_1 < C^f_2$, implies $\rho^f_1 < \rho^f_2$ (see proof of lemma 4.1).

- $\Lambda(C_1^f) = \Lambda(C_2^f) > 0$. Thus, in both equilibria, $\sum_{f' \in \mathcal{F}} \rho^{f'} = 1$; moreover, by the definition of $C_{\max}^f$, the set $\mathcal{F}' = \{f' | \rho^{f'} > 0\}$ contains at least one flow $f' \neq f$, and all flows $f' \in \mathcal{F}' \setminus \{f\}$ satisfy $g^{f'}(\rho^{f'}) = \Lambda(C_1^f) = \Lambda(C_2^f)$, i.e. they have identical $\rho^{f'}$ in both equilibria. It follows that ρ^f must be identical in both equilibria as well. Now, since $g_1^f(\rho^f) < g_2^f(\rho^f) \leq \Lambda(C_2^f)$, it follows that the first equilibrium must have $\mu^f > 0$ and therefore $\rho^f = 0$, contradicting the definition of $C_{\min}^f$.
- $\Lambda(C_1^f) < \Lambda(C_2^f)$. Thus, in the second equilibrium, $\sum_{f' \in \mathcal{F}} \rho^{f'} = 1$, and once again, by the definition of $C_{\max}^f$, the set $\mathcal{F}' = \{f' | \rho^{f'} > 0\}$ contains at least one flow $f' \neq f$, and all flows $f' \in \mathcal{F}'$ satisfy $g^{f'}(\rho^{f'}) = \Lambda(C_2^f) > \Lambda(C_1^f)$. Since the functions $g^{f'}$ for all flows $f' \in \mathcal{F}' \setminus \{f\}$ are unchanged between the equilibria and are strictly decreasing in the respective $\rho^{f'}$, it follows that $\rho^{f'}$ in the second equilibrium must be lower than in the first for all $f' \in \mathcal{F}' \setminus \{f\}$. This immediately implies that $\rho^f = 1 - \sum_{f' \neq f} \rho^{f'}$ must be greater in the second equilibrium than in the first.

□

Lemma 4.4. *The function $F(C^f)$ is concave in C^f in the range $C_{\min}^f \leq C^f \leq C_{\max}^f$.*

Proof. Please refer to Section 4.7.3 for the detailed proof. □

We now proceed to study the properties of the *best-response function* of flow f, defined as $B^f(\mathbf{C^{-f}}) = \text{argmax}_{C^f} \quad U_f(C^f, \mathbf{C^{-f}})$.

Consider the derivative of the flow utility function with respect to C^f, assuming that the followers respond with a symmetrical equilibrium as per the above analysis:

$$\frac{\partial U_f}{\partial C^f} = \left[u_f'(P_{suc}^f(\rho^f)) - C^f\right] \frac{\partial P_{suc}^f(\rho^f)}{\partial \rho^f} \frac{\partial \rho^f}{\partial C^f} - P_{suc}^f(\rho^f), \tag{4.15}$$

where $\rho^f = F(C^f)$. Since $u_f(P_{suc}^f)$ is concave by assumption, $P_{suc}(\rho^f) = 1 - (1 - K^f \rho^f)^R$ is concave in ρ^f, and ρ^f is concave in C_f by lemma 4.4, it follows that $\frac{\partial U_f}{\partial C^f}$ is non-increasing in C_f, i.e. the utility function is concave in C^f.

Lemma 4.5. *The best-response function of flow f is bounded by $0 \leq B^f(\mathbf{C^{-f}}) \leq u_f'(0)$.*

Proof. We notice that U_f can be written as

$$U_f = \left[\frac{u_f(P_{suc}^f)}{P_{suc}^f} - C^f\right] P_{suc}^f.$$

Obviously, in the best response, the utility is nonnegative (a utility of 0 can always be obtained by $C^f = 0$). Accordingly, if $C^f = B^f(\mathbf{C^{-f}})$, then $0 \leq C^f \leq \max_{P_{suc}^f} \frac{u(P_{suc}^f)}{P_{suc}^f}$. However, the assumption about the concavity of $u_f(P_{suc}^f)$ and $u_f(0) = 0$ implies that $\frac{u_f(P_{suc}^f)}{P_{suc}^f} \leq u_f'(0)$ for any $0 \leq P_{suc}^f \leq 1$, and the lemma follows. □

From lemma 4.5, we conclude that if $u'(0) \leq C_{\min}^f = \frac{\Lambda(C^f=0)+e^f}{K^f}$, then the flow can never achieve a positive utility. The strategy C^f used in this case is immaterial, since no node will cooperates with f under any $0 \leq C^f \leq u'(0)$, and, therefore, the payment of f to the nodes is 0

in any case. Nevertheless, to maintain the continuity of the best-response function with respect to $\mathbf{C}^{-\mathbf{f}}$ (through $\Lambda(0)$), we set $B^f(\mathbf{C}^{-\mathbf{f}}) = u'(0)$.

Otherwise, if $u'(0) > C^f_{\min}$, the optimal C^f is obtained by solving $\frac{\partial U^f}{\partial C^f} = 0$. Due to the concavity of $U^f(C^f)$ (established above), a unique solution is guaranteed; furthermore, we observe that if u_f is continuously differentiable, then the best response function is continuous as well.

Finally, we state the main result of this subsection.

Theorem 4.4. *If the followers always respond by playing in their (unique) symmetrical equilibrium, then there exists an equilibrium in the leaders' game (which is an SNE for the system as a whole).*

Proof. We define the mapping $\mathbf{B}(\mathbf{C}) = \left\{B^f(\mathbf{C}^{-\mathbf{f}}), f \in \mathcal{F}\right\}$ to be the collection of best-response functions to the respective strategy vectors of other flows. Since each component of $\mathbf{B}(\mathbf{C})$ is continuous and bounded (Lemma 4.5), the entire mapping is continuous and bounded. Therefore, it has a fixed point, which is an equilibrium of the leaders' game. □

4.4.2 Followers play boundary equilibrium

In this subsection, we show that the SNE existence property established in Theorem 4.4 does not extend in general to the case that the followers' response may be any other than the symmetrical equilibrium, and, in particular, if the followers are assumed to always respond in a boundary equilibrium. In fact, a stronger property is stated in the following lemma.

Theorem 4.5. *If relay nodes always respond to flow price settings by playing a boundary equilibrium, then at any SNE:*

1. *if R^f denotes the number of nodes cooperating with flow f, then either the set $\mathcal{F}' = \left\{f' | R^{f'} = 0\right\}$ is nonempty or the utility of every relay node is 0;*
2. *the utility values of all relay nodes are identical and equal to $H_{th} \triangleq \max_{f' \in \mathcal{F}'} \left[u_{f'}(K^{f'}) - e^{f'}\right]$ (or 0 if H_{th} is negative).*

Proof. To show the first property, assume to the contrary that the set $\mathcal{F}'$ is empty (i.e. $R^f > 0$ for all $f \in \mathcal{F}$). The utility of each node cooperating with f is given by

$$H^f(R^f) \triangleq \frac{C^f\left[1 - (1 - K^f)^{R^f}\right]}{R^f} - e^f. \tag{4.16}$$

Consider the flow $f \in \mathcal{F}$ for which $H^f(R^f)$ is the highest, and assume that $H^f(R^f) > 0$. Then, since $H^f(R^f) \geq H^{f'}(R^{f'}) > H^{f'}(R^{f'} + 1)$ for any $f' \in \mathcal{F}$, there exists an $\epsilon > 0$ by which C^f can be reduced such that the new $H^f(R^f)$ is still both positive and higher than $H^{f'}(R^{f'} + 1)$ for any $f' \in \mathcal{F}$, and, therefore, no node will have incentive to deviate from cooperating with f. Therefore, C^f cannot be the best-response strategy of f.

If $\mathcal{F}'$ is nonempty, consider the flow $f \notin \mathcal{F}'$ with the highest $H^f(R^f)$ among all flows with $R^f > 0$. We observe that, if $H^f(R^f) > C^{f'}K^{f'} - e^{f'}$ for all $f' \in \mathcal{F}'$, then, again, C^f is not the best-response strategy for f since it can be reduced by some $\epsilon > 0$ without triggering a deviation of any relay node. On the other hand, if there exists any flow $\hat{f} \notin \mathcal{F}'$ with $H^{\hat{f}}(R^{\hat{f}}) < H_{th}$, then it follows that there exists a $f' \in \mathcal{F}$ which can "pull" one of relay nodes currently cooperating with $\hat{f}$ and obtain a positive utility, by setting $C^{f'} = \frac{u_{f'}(K^{f'})}{K^{f'}} - \epsilon$ for some sufficiently small $\epsilon > 0$.

Combining the above observations, we conclude that, if $H_{th} \geq 0$, then $H(R^f) = H_{th}$ for any $f \notin \mathcal{F}'$, i.e. all relay nodes receive an identical utility of H_{th}. □

Corollary 4.1. *In a system with two symmetrical flows (i.e. with identical $u_f(\cdot)$ and K^f for $f \in \{1,2\}$) and $e^f = 0, f \in \{1,2\}$, an SNE does not exist.*

Proof. Consider the options allowed by theorem 4.5. If the utility of all nodes is 0, then, with $e^f = 0$, this implies $C^f = 0$ for both flows. Clearly, this is not an SNE since each flow has an incentive to increase its C^f to a small positive value so as to encourage the nodes to cooperate with it and thereby obtain a positive utility.

On the other hand, if all nodes receive a positive utility of $H_{th} > 0$, the first property of the theorem implies that one of the flows (say, flow 2) does not have any nodes cooperating with it, and therefore, the other flow (say, flow 1) is bearing the payment for all the nodes, i.e.,

$$C^1 \frac{\left[1-(1-K^f)^R\right]}{R} = H_{th} = u_f(K^f).$$

The utility of flow 1 is therefore

$$U_1 = u_f\left(1-(1-K^f)^R\right) - C^1\left[1-(1-K^f)^R\right] = \\ u_f\left(1-(1-K^f)^R\right) - R\cdot u_f(K^f) < u_f\left(R\cdot K^f\right) - R\cdot u_f(K^f) \leq 0$$

where the inequalities follow from the monotonicity and concavity of u_f and the fact that $R \geq 2$. It follows that the first flow cannot be in a best-response strategy. Therefore, no SNE is possible in this system. □

Remark: The fact that $R \geq 2$ is crucial in the proof of the corollary above. If $R = 1$, i.e. there is only one relay node in the network, then the "followers' equilibrium" degenerates simply to that node cooperating with the flow f that provides the highest $H^f(1) = C^f K^f - e^f$, assuming that it is nonnegative (or not cooperating at all otherwise), resulting in $P^f_{suc} = K^f$ for that flow. It can be seen that a vector $\mathbf{C}$ that satisfies the following conditions is then a system SNE:

- $0 < C^{\hat{f}} \leq u_f(K^{\hat{f}})/K^{\hat{f}}$ and $C^{\hat{f}}K^{\hat{f}} - e^{\hat{f}} \geq 0$ for one particular $\hat{f} \in \mathcal{F}$;
- for all other $f' \neq \hat{f}$, $u_{f'}(K^{f'}) - e^{f'} \leq C^{\hat{f}}K^{\hat{f}} - e^{\hat{f}}$;
- for at least one $f' \neq \hat{f}$, $u_{f'}(K^{f'}) - e^{f'} = C^{\hat{f}}K^{\hat{f}} - e^{\hat{f}}$.

In particular, such a vector always exists for symmetrical flows with $e^f = 0$ for all $f \in \mathcal{F}$, by setting $C^f = \frac{u_f(K^f)}{K^f}$ for all flows. In the corresponding equilibrium, the relay node will then cooperate with one of the flows $\hat{f}$, yet the utility of all flows is 0 and cannot be improved: flow $\hat{f}$ cannot reduce its $C^{\hat{f}}$ by any amount since that will cause the node to switch to a different flow, while any attempt to increase the offered payment by another flow will only result in a negative utility for that flow.

4.5 Numerical Examples

In this section, we demonstrate some of the theoretical results obtained previously and gain further insight on the behavior of the game via a numerical study. More specifically, we show two simple

scenarios, which are nevertheless indicative of the typical interactions among the players in the game. We use these examples in particular to comment on the issue of equilibrium efficiency, which was not explicitly addressed in the analytical part of the chapter.

4.5.1 Competition between heterogeneous flows: Single relay

We start with a degenerate scenario consisting of two flows and single relay node ($\mathcal{F} = \{1, 2\}, \mathcal{R} = \{1\}$). For the flows, we adopt a linear utility function, as follows: $u_f(P^f_{suc}) = m_f P^f_{suc}, f \in \mathcal{F}$. In the following, we fix $m_1 = 1$ and vary m_2 to study how the game results depend on the heterogeneous flow utilities. We set $P^1_{sn} = P^1_{nd} = 0.8$ and $P^2_{sn} = P^2_{nd} = 0.4$ (which translates to $K^1 = 0.64$ and $K^2 = 0.16$), reflecting a difference in channel qualities between the endpoint pairs of the flows and the relay. Finally, we assume $e^f = 0$ for both flows. It is easily verified that the socially optimal operating point (i.e. one that maximizes the total utility of all flows) is achieved if the relay node cooperates entirely with the flow with the higher utility, i.e. $\mathbf{r} = (1, 0)$ if $m_1 K^1 \geq m_2 K^2$, and $\mathbf{r} = (0, 1)$ otherwise; therefore, the total maximum social utility is $U_{\max} = \max(0.64, 0.16 m_2)$.

Figure 4.1 plots the flow strategies C^1, C^2 in the resulting SNE as a function of m_2. Clearly, the relay node serves the more profitable flow with probability 1 at the equilibrium. Figure 4.2 illustrates the utility for the flow side ($U_1 + U_2$) and the relay side (V_1), as well as the maximum social utility U_{max}. It is evident that $U_{max} = V_1 + U_1 + U_2$, i.e., the SNE always coincides with the socially optimal operating point. In other words, the proposed pricing mechanism and the resulting competition between the flows guides the relay node to operate efficiently without any information on the flows' utilities.

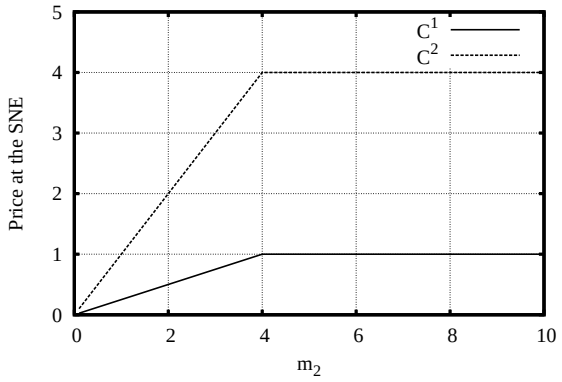

Figure 4.1: Prices C^1, C^2 at the SNE (single relay case)

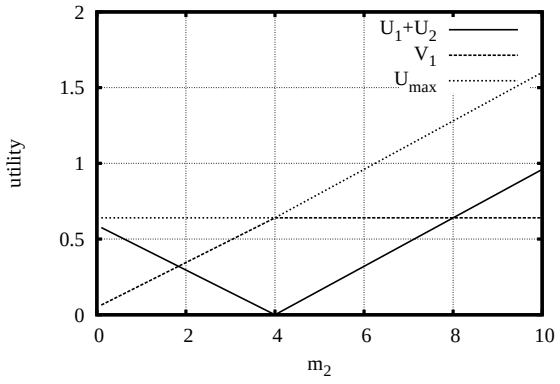

Figure 4.2: Utility partition among flows and relay

It is interesting to observe how the total system utility gets divided between the flows and the relay node. If m_2 is small, flow 1 can obtain the relay service for a very cheap cost, since flow 2 is limited in the price it can offer due to its own low utility. The full utility is thus retained by flow 1. As m_2 increases, flow 1 must increase its price so as to remain just slightly more attractive to the relay than the maximum offer flow 2 is able to make. Thus, the relay node gets paid more for its service, while the utility retained by the flow decreases. At $m_2 = \frac{K_1}{K_2} = 4$, the price war between the flows is at its peak, and the entire system utility of 0.64 is enjoyed by the relay node. For $m_2 > 4$, the first flow can no longer compete with the price able to be offered by flow 2; therefore, flow 2 can secure the service of the relay node by matching (or offering just slightly above) the maximum of flow 1, i.e. $C_2 = 4$. From that point, the utility retained by the relay node is constant,

and all further increases in m_2 are reflected in the utility of flow 2.

4.5.2 Two flows and two relay nodes

We now consider a scenario with two flows and two relay nodes, which is more representative of the interactions among players in a multiple-flow and multiple-relay system. Apart from the second relay, all parameters are set to the same values as before. The results (for the case where the relay nodes play the symmetrical equilibrium) are shown in Figure 4.3 and 4.4. Figure 4.3 shows the prices offered by the flows in the SNE. Figure 4.4 displays the equilibrium efficiency as the "Price of Anarchy" [Pap01], defined as the ratio between the optimal social utility and the system utility achieved at the equilibrium.

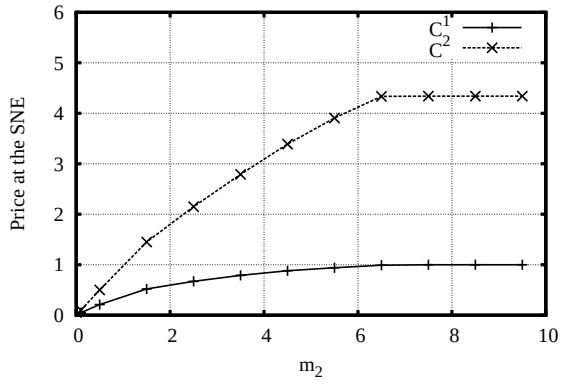

Figure 4.3: Prices C^1, C^2 at SNE (2-relay scenario)

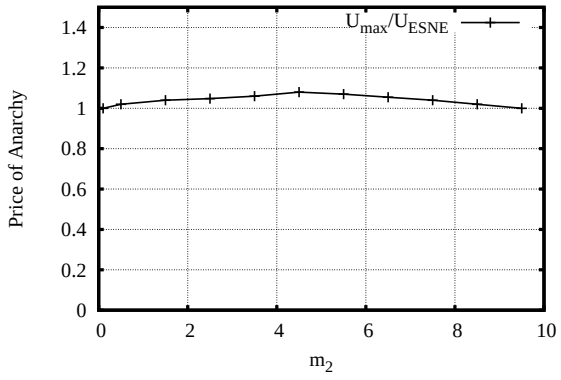

Figure 4.4: Price of Anarchy for 2-relay scenario

From the results, we observe that the price of anarchy tends to 1 when the flows are heterogeneous, i.e. when m_2 is either very small or very large. This is explained by the fact that, in those extremes, both the equilibrium strategy and the global optimum then require the relay nodes to cooperate fully with only one of the flows, respectively. Otherwise, for intermediate ranges of m_2, the SNE is less efficient since the symmetrical followers' equilibria tend to assign a nonzero cooperation probability to each of the flows, as neither flow is in a position to offer a price large enough to attract both relays entirely to itself. Nevertheless, we observe that even the worst price of anarchy is only slightly greater than 1. This suggests that, at least for the scenarios considered, the proposed pricing framework can bring about a reasonably efficient equilibrium, with only a small system utility loss due to players' selfishness.

4.6 Conclusion

We have proposed a market-based pricing framework for wireless networks with autonomous nodes in the context of cooperative relaying. An important difference between our model and other similar studies that feature payment for packet forwarding is that a packet may be relayed by several nodes simultaneously, and, therefore, the payment is shared among several nodes that have participated in its delivery. We have shown that this variation leads to substantially different properties of the resulting game model. In particular, we have established that the game among the relay nodes (followers) possesses several kinds of Nash equilibria (NE), including a unique symmetrical NE and at least one boundary NE. Furthermore, we have established that the game

among the flows (leaders) always possesses a Stackelberg equilibrium if the followers respond in their symmetrical NE, but an equilibrium may not exist if the followers play in a boundary NE. Finally, we demonstrated that the resulting equilibrium is reasonably efficient from a social perspective, particularly when the flows have very heterogeneous utilities.

4.7 Proofs

This section completes the detailed proofs omitted from the main text.

4.7.1 Proof of Lemma 4.1

For convenience, we introduce a variable change of $y \triangleq 1 - K^f x$, and slightly abuse notation by referring to $g^f(y)$ and $h^f(y)$ as functions of y.

We compute the derivatives of $h^f(y)$:

$$\frac{dh^f(y)}{dy} = \frac{K^f}{R(1-y)^2}\left[1 + (R-1)y^R - Ry^{R-1}\right]; \tag{4.17}$$

$$\frac{d^2h^f(y)}{dy^2} = \frac{K^f}{R(1-y)^3}\left[2 - (R-1)(R-2)y^R + 2R(R-2)y^{R-1} - R(R-1)y^{R-2}\right]. \tag{4.18}$$

Denote the expressions in brackets in (4.17) and (4.18) by $A_1(y)$ and $A_2(y)$, respectively. Then:

- Since $A_1(1) = 0$ and $\frac{dA_1(y)}{dy} = -R(R-1)y^{R-2}(1-y) < 0$ for $R > 1$ and $0 < y < 1$, it follows that $A_1(y)$ is strictly positive for all $0 < y < 1$. Hence, $h^f(y)$ is strictly increasing in y, i.e. $h^f(x)$ (and therefore $g^f(x)$ as well) is strictly decreasing in x;
- Since $A_2(1) = 0$ and $\frac{dA_2(y)}{dy} = -R(R-1)(R-2)y^{R-3}(1-y)^2 < 0$ for $R > 1$ and $0 < y < 1$, it follows that $A_2(y)$ is strictly positive for all $0 < y < 1$. Hence, $\frac{dh^f(y)}{dy}$ is strictly increasing in y, which implies that $\frac{dh^f(x)}{dx} = -\frac{dh^f(y)}{dy}$ is strictly increasing in x.

To show that $\frac{h'^f(x)}{[h^f(x)]^2}$ is decreasing in x, or, equivalently, that $\frac{dh^f(y)/dy}{[h^f(y)]^2}$ is decreasing in y, it suffices to show that $h^f(y)\frac{d^2h^f(y)}{dy^2} - 2\left(\frac{dh^f(y)}{dy}\right)^2 < 0$. By a straightforward calculation, this is shown to be equivalent to

$$(R+1)y + (R-1)y^{R+1} - (R+1)y^R - (R-1) < 0. \tag{4.19}$$

Denote $A_3(y)$ to be the expression on the left-hand side of (4.19). Since $A_3(1) = 0$ and $\frac{dA_3(y)}{dy} = (R+1)\left[1 + (R-1)y^R - Ry^{R-1}\right] = (R+1)A_1(y) > 0$ for all $0 < y < 1$, the proof is complete.

4.7.2 Proof of Lemma 4.2

The continuity of λ with respect to C^f is immediate from conditions (4.7)-(4.9) and the continuity of g^f. To establish the monotonicity, suppose to the contrary that $\lambda_1 = \Lambda(C_1^f) > \Lambda(C_2^f) = \lambda_2$ for some $C_1^f < C_2^f$. Then, $\lambda_1 > \lambda_2 \geq 0$ implies that, in the first equilibrium (i.e. corresponding to C_1^f), $\sum_{f' \in \mathcal{F}} \rho^{f'} = 1$. Therefore, there is a non-empty set of flows $\mathcal{F}' = \{f' | \rho^{f'} > 0\}$, and all flows $f' \in \mathcal{F}'$ satisfy $g^{f'}(\rho^{f'}) = \lambda_1$ (since $\rho^{f'} > 0$ implies $\mu^{f'} = 0$). In the second equilibrium (corresponding to C_2^f), since $\lambda_2 < \lambda_1$, it follows that each $g^{f'}(\rho^{f'})$ must be smaller than in the first equilibrium. However, we note that for any $f' \neq f$ the function $g^{f'}$ has not changed, and for f itself the function g^f even increased (since $C_1^f < C_2^f$). Since $g^{f'}(\rho^{f'})$ are strictly decreasing

functions (Lemma 4.1), it follows that $\rho^{f'}$ must have strictly increased in the second equilibrium for all $f' \in \mathcal{F}'$, which is obviously impossible.

4.7.3 Proof of Lemma 4.4

From lemma 4.3, it follows that, for every $0 < \rho^f < 1$, there exist unique $C^f = F^{-1}(\rho^f)$, λ, and $\{\rho^{f'}, f' \neq f\}$ that define a symmetrical equilibrium together with ρ^f. Therefore, we can view these quantities as functions of ρ^f, and consider their derivatives with respect to ρ^f.

We rewrite condition (4.7) as follows:

$$C^f h^f(\rho^f) = \lambda + e^f \tag{4.20}$$

and, for any flow $f' \neq f$ such that $\rho^{f'} > 0$,

$$C^{f'} h^{f'}(\rho^{f'}) = \lambda + e^{f'}. \tag{4.21}$$

Taking the derivative of both sides in (4.20) and (4.21) with respect to ρ^f, we obtain, respectively,

$$\frac{dC^f}{d\rho^f} h^f(\rho^f) + C^f \frac{dh^f(\rho^f)}{d\rho^f} = \frac{d\lambda}{d\rho^f} \tag{4.22}$$

$$C^{f'} \frac{dh^{f'}(\rho^{f'})}{d\rho^{f'}} \frac{d\rho^{f'}}{d\rho^f} = \frac{d\lambda}{d\rho^f} \tag{4.23}$$

or, rearranging (4.23),

$$\frac{d\rho^{f'}}{d\rho^f} = \frac{\frac{d\lambda}{d\rho^f}}{C^{f'} \frac{dh^{f'}}{d\rho^{f'}}}. \tag{4.24}$$

We now distinguish between two sub-regions of λ. If $\rho^f + \sum_{f' \neq f} \rho^{f'} < 1$, then $\lambda = 0$ in some small vicinity of ρ^f. Thus, $\frac{d\lambda}{d\rho^f} = 0$; also, $g^f(\rho^f) = C^f h^f(\rho^f) - e^f = 0$. From (4.22), we thus obtain

$$\frac{dC^f}{d\rho^f} = -\frac{C^f dh^f(\rho^f)/d\rho^f}{h^f(\rho^f)} = -\frac{e^f dh^f(\rho^f)/d\rho^f}{\left[h^f(\rho^f)\right]^2}, \tag{4.25}$$

which, by lemma 4.1, is increasing in ρ^f.

Otherwise, if $\rho^f + \sum_{f' \neq f} \rho^{f'} = 1$, then $\sum_{f'} \frac{d\rho^{f'}}{d\rho^f} = -1$ in the vicinity of ρ^f. Together with (4.24), this implies

$$\frac{d\lambda}{d\rho^f} = -\sum_{f' \neq f} C^{f'} \frac{dh^{f'}(\rho^{f'})}{d\rho^{f'}} \tag{4.26}$$

which can be fed back into (4.22) to yield

$$\frac{dC^f}{d\rho^f} = -\frac{1}{h^f(\rho^f)} \left[C^f \frac{dh^f(\rho^f)}{d\rho^f} + \sum_{f' \neq f} C^{f'} \frac{dh^{f'}(\rho^{f'})}{d\rho^{f'}} \right] = - \frac{(\lambda + e^f) dh^f(\rho^f)/d\rho^f}{\left[h^f(\rho^f)\right]^2} - \frac{1}{h^f(\rho^f)} \sum_{f' \neq f} C^{f'} \frac{dh^{f'}(\rho^{f'})}{d\rho^{f'}}. \tag{4.27}$$

We observe that, since λ is increasing in ρ^f and $g^{f'}(\rho^{f'})$ is decreasing in $\rho^{f'}$, it follows that each $\rho^{f'}$ is decreasing in ρ^f. Therefore, $\frac{dh^{f'}(\rho^{f'}}{d\rho^{f'}}$, which is increasing in $\rho^{f'}$ by lemma 4.1, is decreasing

in ρ^f. It follows that (4.27) is increasing in ρ^f in this case as well.

Combining our findings that both (4.25) and (4.27) are increasing in ρ^f, and noticing that the jump in $\frac{dC^f}{d\rho^f}$ at the boundary between the two sub-regions (namely, the difference between (4.27) at $\lambda = 0$ and (4.25)) is positive, we conclude that the function $C^f = F^{-1}(\rho^f)$ is convex, and, therefore, $F(C^F)$ is concave in the entire range $C^f_{\min} \leq C^f \leq C^f_{\max}$.

Part II

Playing with Enemy

Part II of the thesis is dedicated to the malicious behaviors in wireless networks. In this part, we present a line of research where game theory is used as a tool for analyzing malicious behaviors and developing, implementing, validating new defense mechanisms. The first major contribution we make in this part is the formal quantitative analysis of security under game theoretic framework, based on which we derive the attackers' strategy at the NE, the optimal defending strategies and the maximum possible damage that the attackers can cause. Armed with the analytical results, we make our second contribution by designing effective defense strategies to fight against malicious attackers and exploring the tradeoffs and corresponding optimization problems that the defenders face.

Chapter 5 presents a comprehensive game theoretic model on the intrusion detection problem in the heterogenous networks consisting of nodes with different security assets. The expected behaviors of malicious attackers and the optimal strategy of the defenders are elaborated. Chapter 6 addresses the jamming attack in wireless networks and propose an active defense strategy by draining the jammer's energy. The effectiveness and the limitation of the proposed strategy is evaluated using game theory. In Chapter 7, we address the multi-path routing in wireless multi-hop networks. Specific optimization problems are formulated and game theory is applied to derive their solutions and correspondent routing algorithms. The tradeoff between route security and availability is also investigated.

Chapter 5

On Intrusion Detection in Heterogenous Networks

5.1 Introduction

Today's computer and communication networks especially wireless networks are becoming more and more dynamic, distributed and heterogenous, which, combined with the complexity of underlying computing and communication environments, increases significantly the security risk by making the network control and management much more challenging than ever. Consequently, nowadays networks are much more vulnerable to various attacks such as TCP SYN flooding, SSPing and DoS attack, etc. The last few years have witnessed significant increase of attacks and their damages. In such context, the intrusion detection system (IDS) is widely deployed as a complementary line of defense to the classical security approaches aiming at removing the vulnerabilities which may not be very effective or even fail to function in some cases.

In almost all contemporary networks, network nodes (targets from the attackers's point of view) usually have different sensibility levels or possess different security assets depending on their roles and the data or information they hold. In other words, the networks are usually heterogenous in terms of security. More specifically, some targets are more "attractive" to attackers than others. Examples of such targets include the servers containing sensible secret information, high hierarchy nodes in military networks, etc. These targets are usually also better protected and are thus more difficult or costly to attack. In such heterogenous environments, two natural but crucial questions are: What are the expected behaviors of rational attackers? What is the optimal strategy of the defenders (IDSs)?

In this chapter, we answer the posed questions by developing a non-cooperative game theoretic model of the network intrusion detection problem, analyzing the resulting equilibria and investigating the engineering implications behind the analytical results. We then derive optimal strategy for the defender side and the guidelines for IDS design and deployment. Our study in this chapter is generic such that no specific context of attacks and networks is assumed in the analysis. Nevertheless, as we will show later via case study, the model established in this chapter is particularly suitable in wireless networks where the interaction between the attackers and defenders is much more complicated than in the traditional wired environments and the best strategy for the defenders consists of a tradeoff of various factors.

Our main contributions of this chapter can be summarized as follows:

- We provide a game theoretic framework of intrusion detection in heterogenous networks where targets have different security assets.
- Under the framework, we derive the expected behaviors of rational attackers, the minimum monitor resource requirement of the defenders and the optimal strategy of the defenders.
- We provide two case studies to illustrate how our game theoretic framework can be applied to configure the intrusion detection strategies in realistic scenarios for wireless networks.

This chapter proceeds as follows. Section 5.2 briefly presents related work and compares our work with existing work. In Section 5.3, we formulate the non-cooperative intrusion detection game. In Sections 5.4 and 5.5, we study the NE of the game in the case of single and multiple attacker(s)/defender(s), respectively. Based on our analysis, we derive optimal defender strategy and guidelines for IDS design and deployment. In Section 5.6, we show how our game theoretic framework can be applied to configure the intrusion detection strategies via two case studies. Section 5.7 discusses some variants and extensions of the game. Section 5.8 provides numerical results of the game theoretic framework. Section 5.9 concludes the chapter.

5.2 Related Work

Intrusion detection has been an active research field for a long time. Most research efforts address the problem of how to improve the performance of IDSs: e.g., increase coverage of attack types, boost detection rate and keep false alarm rate low, etc [MP02], [MST98], [LSM00]. In [ZL00], Zhang *et al.* proposed a distributed cooperative IDS, in which a node detecting an intrusion with low confidence can initiate a global intrusion detection procedure through a cooperative detection engine. The local detection engine is built on the rule-based classification algorithm. In a later paper [HFLY03], Yi *et al.* extended the previous work on local anomaly detection and conducted a cross-feature analysis to explore the correlations between each feature and other features using decision-tree based classification algorithm. An intrusion detection method based on the analysis is proposed for detecting ad hoc routing anomalies. In [SSA06], Subhadrabandhu *et al.* took another line of research by applying theories of hypothesis testing and approximation algorithms to develop a statistical framework for intrusion detection in ad hoc networks.

Recently, several game theoretic approaches have been proposed to model the interaction between the attackers and IDSs. Kodialam *et al.* [KL03] proposed a game theoretic framework to model the intrusion detection game between the service provider and the intruder. The objective of intruder is to minimize the probability of being detected by choosing a set of paths to inject malicious packets, and the objective of the service provider is to sample a set of links to maximize the detection probability. The equilibrium strategy of both players is to play the minmax strategy of the game. Alpcan and Basar [AB04] model the intrusion detection as a noncooperative non-zero-sum game with both finite and continuous-kernel versions. In their model a fictitious player is added to the game to represent the output of the IDS sensor network. The authors showed the existence and uniqueness of the NE and studied the dynamics of the game. Liu *et al.* [LCM06] studied the problem using Bayesian game theory in the context of ad hoc networks where both players update their strategies based on their observation of previous results. A Bayesian hybrid detection system is proposed based on the analytical results for the defender to strike a balance between its energy costs and monitoring gains. Agah *et al.* [ADBA04] and Alpcan and Basar

[AB03] reconsidered the problem in sensor networks where each player's optimal strategy depends only on the payoff function of the opponent. A two-player non-cooperative game is thus formulated between the attacker and the defender (network), and the analysis on the resulting NE leads to a defense strategy for the network. Patcha and Park [PP06] modeled the interaction between an attacker and an individual node as a non-cooperative signaling game where the sender is either of type Attacker or Regular. The receiver with IDS detects the attack with a probability depending on its belief which is updated according to the "message" it has received.

Despite the substantial work on the intrusion detection in the literature, none of them addresses the problem in heterogenous environments. Motivated by this observation, our work contributes to the existing literature by providing a game theoretic framework of the network intrusion detection problem in heterogenous environments consisting of targets with different security assets. By characterizing the resulting NE, we further derive the minimum monitor resource requirement and the optimal strategy of the defender side in such environments.

Moreover, existing game theoretic work on the intrusion detection is mainly theoretic work based on highly abstract models. In our work, besides providing the theoretic quantitative framework, we also illustrate the application of the proposed framework in real scenarios via case studies, which is absent in existing work. Our work can thus serve as a building block to guide the design and evaluation of the intrusion detection systems.

5.3 Network Intrusion Detection Game Model

We consider a network $\mathcal{N} = (\mathcal{S}_\mathcal{D}, \mathcal{S}_\mathcal{A}, \mathcal{T})$ where $\mathcal{S}_\mathcal{D}$ is the set of agents equipped with the IDS module which we refer to as *defenders* throughout the chapter, $\mathcal{S}_\mathcal{A}$ is the set of *attackers* and $\mathcal{T} = \{1, 2, \cdots, N\}$ is the set of network nodes which may be attacked by the attackers, referred to as *targets*. We start with the simplest case where there are only one attacker and one defender. We model the interactions between them as a non-cooperative game. The objective of the attacker is to attack the targets without being detected. To this end, it chooses the strategy $\mathbf{p} = \{p_1, p_2, \cdots, p_N\}$ which is the attack probability distribution over the target set $\mathcal{T}$ where p_i is the probability of attacking target i. $\sum_{i\in\mathcal{T}} p_i \leq P \leq 1$ represents the attacker's resource constraint. This constraint can be relaxed if the attacker can attack multiple targets simultaneously, e.g., broadcasting malicious packets to attack many network nodes at the same time. This case will be addressed in later sections. For the defender, in order to detect the attacks, it monitors the targets with the probability distribution $\mathbf{q} = \{q_1, q_2, \cdots, q_N\}$, where q_i is the probability of monitoring target i. Here monitor means that the defender collects audit data and examines them for signs of security problems. Similarly, we have $\sum_{i\in\mathcal{T}} q_i \leq Q \leq 1$ that represents the defender's monitor resource constraint.

We assume that each target $i \in \mathcal{T}$ processes an amount of security asset denoted as W_i, representing the loss of security when the attacks on i are successful, e.g., loss of reputation or data integrity, cost of damage control, etc. The security assets of the targets depend on their roles in the network and the data or information they hold. In practice, the security assets are evaluated in the risk analysis/assessment phase using formal analysis or specific tools before the IDS deployment. If the attack on target i is not detected, then the attacker gets payoff W_i while the defender gets payoff $-W_i$. Otherwise, the payoff for the attacker and defender is $-W_i$ and

W_i, respectively. Other payoff formulations are also possible. In those cases, our analysis in this chapter can be extended by modifying the utility function of the attacker and defender.

Throughout this chapter, we assume that the security assets of different targets are independent. We argue that this assumption holds in many scenarios such as ad hoc networks where no hierarchy or infrastructure is available and each node operates independently of others. A limitation of our work in this study is the static full information game formulation. However, despite these simplification and limitation, the results and its implications are far from trivial. In fact, our model presented here can serve as a theoretic basis for further more sophisticated game models on the intrusion detection problem tailed to specific scenarios.

Table 5.1 illustrates the payoff matrix of the attacker-defender interaction on target i in the strategic form. In the matrix, a denotes the detection rate of the IDS module of the defender, b denotes the false alarm rate (i.e., false positive rate), and $a, b \in [0, 1]$. The cost of attacking and monitoring (e.g., energy cost) target $i \in \mathcal{T}$ are also taken into account in our model and are assumed proportional to the security asset of i, denoted by $C_a W_i$ and $C_m W_i$, respectively. $C_f W_i$ denotes the loss of a false alarm. In our study, we implicitly assume that $C_a < 1$, otherwise the attacker has no incentive to attack, similarly $C_m < 1$.

	Monitor	Not monitor
Attack	$(1-2a)W_i - C_aW_i$, $-(1-2a)W_i - C_mW_i$	$W_i - C_aW_i, -W_i$
Not attack	$0, -bC_fW_i - C_mW_i$	$0, 0$

Table 5.1: Strategic form of the game for target i

The overall payoff of the attack and defender, defined by the utility functions U_A and U_D, is as follows:

$$\begin{aligned}
U_A(\mathbf{p}, \mathbf{q}) &= \sum_{i \in \mathcal{T}} p_i q_i \left[(1-2a)W_i - C_aW_i\right] + p_i(1-q_i)(W_i - C_aW_i) \\
&= \sum_{i \in \mathcal{T}} p_i W_i (1 - 2aq_i - C_a) \\
U_D(\mathbf{p}, \mathbf{q}) &= \sum_{i \in \mathcal{T}} p_i q_i (-(1-2a)W_i - C_mW_i) - p_i(1-q_i)W_i - (1-p_i)q_i(bC_fW_i + C_mW_i) \\
&= \sum_{i \in \mathcal{T}} [q_i W_i \left[p_i(2a + bC_f) - (bC_f + C_m)\right] - p_i W_i]
\end{aligned}$$

We conclude this section with the definition of the network intrusion detection game with one attacker/defender.

Definition 5.1. *The intrusion detection game with one attacker/defender G is defined as follows:*

Players: *Attacker, Defender*

Strategy set: *Attacker:* $A_A = \{\mathbf{p} : \mathbf{p} \in [0, P]^N, \sum_{i \in \mathcal{N}} p_i \leq P\}$

Defender: $A_D = \{\mathbf{q} : \mathbf{q} \in [0, Q]^N, \sum_{i \in \mathcal{N}} q_i \leq Q\}$

Payoff: U_A *for attacker,* U_D *for defender*

Game rule: *The attacker/defender selects its strategy* $\mathbf{p}/\mathbf{q} \in A_A/A_D$ *to maximize* U_A/U_D

5.4 Solving the Intrusion Detection Game with one Attacker/Defender

For non-cooperative games as G, the most important solution concept is the Nash equilibrium (NE), where no player has incentive to deviate from its current strategy. In the case of G, we have the following definition of NE.

Definition 5.2. *A strategy profile* $(\mathbf{p}^*, \mathbf{q}^*)$ *is said to be a NE of* G *if neither the attacker nor the defender can improve its utility by unilaterally deviating its strategy from it.*

5.4.1 Sensible Target Set

In G, since the attacker has limited attack resource, a natural question is whether a rational attacker will focus on some targets or allocate its attack resource to all targets to reduce the probability of being detected. Next we study this question before delving into the analysis of the NE. To facilitate the analysis, we sort the targets based on their security asset W_i as: $W_1 \geq W_2 \geq \cdots \geq W_N$. We then define the sensible target set and the quasi-sensible target set as follows:

Definition 5.3. *The sensible target set* $\mathcal{T}_\mathcal{S}$ *and the quasi-sensible target set* $\mathcal{T}_\mathcal{Q}$ *are defined such that:*

$$\begin{cases} W_i > \dfrac{|\mathcal{T}_\mathcal{S}| \cdot (1-C_a) - 2aQ}{(1-C_a)(\sum_{j\in\mathcal{T}_\mathcal{S}} \frac{1}{W_j})} & \forall i \in \mathcal{T}_\mathcal{S} \\ W_i = \dfrac{|\mathcal{T}_\mathcal{S}| \cdot (1-C_a) - 2aQ}{(1-C_a)(\sum_{j\in\mathcal{T}_\mathcal{S}} \frac{1}{W_j})} & \forall i \in \mathcal{T}_\mathcal{Q} \\ W_i < \dfrac{|\mathcal{T}_\mathcal{S}| \cdot (1-C_a) - 2aQ}{(1-C_a)(\sum_{j\in\mathcal{T}_\mathcal{S}} \frac{1}{W_j})} & \forall i \in \mathcal{T} - \mathcal{T}_\mathcal{S} - \mathcal{T}_\mathcal{Q} \end{cases} . \tag{5.1}$$

where $|\mathcal{T}_\mathcal{S}|$ *is the cardinality of* $\mathcal{T}_\mathcal{S}$, $\mathcal{T} - \mathcal{T}_\mathcal{S} - \mathcal{T}_\mathcal{Q}$ *denotes the set of targets in the target set* $\mathcal{T}$ *but neither in* $\mathcal{T}_\mathcal{S}$ *nor in* $\mathcal{T}_\mathcal{Q}$.

The following lemma further characterizes $\mathcal{T}_\mathcal{S}$ and $\mathcal{T}_\mathcal{Q}$:

Lemma 5.1. *Given a network* $\mathcal{N}$, *both* $\mathcal{T}_\mathcal{S}$ *and* $\mathcal{T}_\mathcal{Q}$ *are uniquely determined.* $\mathcal{T}_\mathcal{S}$ *consists of* N_A *targets with the largest security assets such that:*

1. *If* $W_N > \dfrac{N(1-C_a) - 2aQ}{(1-C_a)\sum_{j=1}^{N} \frac{1}{W_j}}$, *then* $N_A = N$, $\mathcal{T}_\mathcal{Q} = \Phi$.

2. *If* $W_N \leq \dfrac{N(1-C_a) - 2aQ}{(1-C_a)\sum_{j=1}^{N} \frac{1}{W_j}}$, N_A *is determined by the following equations:*

$$\begin{cases} W_{N_A} > \dfrac{N_A \cdot (1-C_a) - 2aQ}{(1-C_a)\sum_{j=1}^{N_A} \frac{1}{W_j}} \\ W_{N_A+1} \leq \dfrac{N_A \cdot (1-C_a) - 2aQ}{(1-C_a)\sum_{j=1}^{N_A} \frac{1}{W_j}} \end{cases} . \tag{5.2}$$

$\mathcal{T}_\mathcal{Q}$ *consists of the target(s)* i *such that* $W_i = \dfrac{N_A \cdot (1-C_a) - 2aQ}{(1-C_a)\sum_{j=1}^{N_A} \frac{1}{W_j}}$.

Proof. Please refer to Section 5.10.1 for detailed proof. □

Remark: It follows straightforwardly from Lemma 5.1 that $N_A \geq 1$. Given the performance parameter of IDS and the attack cost, $\mathcal{T}_\mathcal{S}$ depends on the security assets of targets and the monitor resource of the defender. $|\mathcal{T}_\mathcal{S}|$ is non-decreasing in Q. If $2aQ \geq N(1-C_a)$, $|\mathcal{T}_\mathcal{S}| = N$ or $\mathcal{T}_\mathcal{S} = \mathcal{T}$. We investigate the following three typical scenarios to gain a more in-depth insight on $\mathcal{T}_\mathcal{S}$:

- In the degenerate case where $N = 1$, $N_A = 1$.
- In the homogeneous case where $W_i = W_j, \forall i, j \in \mathcal{T}$, $N_A = N$.
- In an extremely heterogeneous case where $W_1 \simeq \cdots \simeq W_k \gg W_{k+1} \geq \cdots \geq W_N$, $N_A = k$.

$\mathcal{T}_\mathcal{Q}$ can be regarded as the border set between $\mathcal{T}_\mathcal{S}$ and $\mathcal{T} - \mathcal{T}_\mathcal{S}$ and may be empty.

We now study the security implications of $\mathcal{T}_\mathcal{S}$ in the following theorem.

Theorem 5.1. *A rational attacker has no incentive to attack any target $i \in \mathcal{T} - \mathcal{T}_\mathcal{S} - \mathcal{T}_\mathcal{Q}$.*

Proof. Please refer to Section 5.10.2 for the detailed proof. □

Remark: Theorem 5.1 is a powerful result in that it shows that focusing only on the targets in $\mathcal{T}_\mathcal{S}$ and $\mathcal{T}_\mathcal{Q}$ is enough to maximize the attacker's payoff. Other targets are "self-secured" such that they are not "attractive" enough to draw the attacker's attention due to their security assets and the monitor resource constraint of the defender, even these targets are not monitored by the defender.

Noticing the utility function of the defender, if the attacker does not attack the target i, then the defender has no incentive to monitor i, either. The following guideline for the defender is thus immediate:

Guideline 1: A rational defender only needs to monitor the targets in $\mathcal{T}_\mathcal{S} + \mathcal{T}_\mathcal{Q}$.

5.4.2 Nash Equilibrium Analysis

In this subsection, we derive the NE of the intrusion detection game G. We can easily check that G is a two-person game defined in [Ros65] and thus admits at least one NE following Theorem 1 in [Ros65]. Moreover, let $(\mathbf{p}^*, \mathbf{q}^*)$ denote the NE of G, it holds that

$$\begin{aligned} 0 \leq (1 - 2aq_i^* - C_a)W_i = (1 - 2aq_j^* - C_a)W_j \\ \geq (1 - 2aq_k^* - C_a)W_k \quad \forall i, j, k \in \mathcal{T}, p_i^*, p_j^* > 0, p_k^* = 0. \end{aligned} \tag{5.3}$$

(5.3) can be shown noticing the attacker's utility function U_A: if $(1 - 2aq_i^* - C_a)W_i < 0$, then the attacker has incentive to change p_i^* to 0; if $(1 - 2aq_i^* - C_a)W_i < (1 - 2aq_j^* - C_a)W_j$, then the attacker has incentive to decrease p_i^* and increase p_j^*; if $(1 - 2aq_i^* - C_a)W_i < (1 - 2aq_k^* - C_a)W_k$, then the attacker gets more payoff by set $p_k^* = p_i^*$ and $p_i^* = 0$. In the same way, noticing the defender's utility function U_D, it holds that

$$\begin{aligned} 0 \leq W_i[p_i^*(2a + bC_f) - (bC_f + C_m)] = W_j[p_j^*(2a + bC_f) - (bC_f + C_m)] \\ \geq W_k[p_k^*(2a + bC_f) - (bC_f + C_m)] \quad \forall i, j, k \in \mathcal{T}, q_i^*, q_j^* > 0, q_k^* = 0. \end{aligned} \tag{5.4}$$

Note the resource constraint of the players, we consider the following cases

Case 1: $\sum_{i\in\mathcal{T}} q_i^* = Q$ *and* $\sum_{i\in\mathcal{T}} p_i^* = P$. In this case, combining (5.3) and (5.4) leads to

$$p_i^* \begin{cases} = \dfrac{P_A}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}} - \left(\dfrac{N_A}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}} - 1 \right) \dfrac{bC_f + C_m}{2a + bC_f} & i \in \mathcal{T}_\mathcal{S} \\ \in \left[0,\ \dfrac{P_A}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}} - \left(\dfrac{N_A}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}} - 1 \right) \dfrac{bC_f + C_m}{2a + bC_f} \right] & i \in \mathcal{T}_\mathcal{Q} \\ = 0 & i \in \mathcal{T} - \mathcal{T}_\mathcal{S} - \mathcal{T}_\mathcal{Q} \end{cases}$$

$$q_i^* = \begin{cases} \dfrac{1}{2a} \left(1 - C_a - \dfrac{N_A(1 - C_a) - 2aQ}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}} \right) & i \in \mathcal{T}_\mathcal{S} \\ 0 & i \in \mathcal{T} - \mathcal{T}_\mathcal{S} \end{cases}$$

where $P_A > \left(N_A - W_{N_A} \sum_{j=1}^{N_A} \dfrac{1}{W_j} \right) \dfrac{bC_f + C_m}{2a + bC_f}$, and $\sum_{i\in\mathcal{T}} p_i^* = P$. The necessary condition for the solution to be a NE is

$$\begin{cases} W_i[p_i^*(2a + bC_f) - (bC_f + C_m)] \geq 0, P_A \leq P \\ (1 - 2aq_i^* - C_a)W_i \geq 0 \end{cases} \quad i \in \mathcal{T}_\mathcal{S} \quad \Longrightarrow \quad \begin{cases} N_D \geq N_A \\ N_A(1 - C_a) \geq 2aQ \end{cases},$$

where $N_D = \left\lfloor \dfrac{(2a + bC_f)P}{bC_f + C_m} \right\rfloor$, where $\lfloor n \rfloor$ denotes the largest integer not more than n.

Case 2: $\sum_{i\in\mathcal{T}} q_i^* < Q$ *and* $\sum_{i\in\mathcal{T}} p_i^* = P$. In this case, noticing U_D, we have

$$W_i[p_i^*(2a + bC_f) - (bC_f + C_m)] = 0 \geq W_j[p_j^*(2a + bC_f) - (bC_f + C_m)] \quad \forall i, j \in \mathcal{T}, q_i^* > 0, q_j^* = 0$$

Otherwise the defender will increase q_i^* to get more payoff. Combining the above equation with (5.3) and (5.4), we can thus solve $\mathbf{p}^*$, $\mathbf{q}^*$ as

$$p_i^* \begin{cases} = \dfrac{bC_f + C_m}{2a + bC_f} & W_i > W_{N_D+1} \\ \in \left[0, \dfrac{bC_f + C_m}{2a + bC_f} \right] & W_i = W_{N_D+1} \\ = 0 & W_i < W_{N_D+1} \end{cases} \quad q_i^* = \begin{cases} \dfrac{1 - C_a}{2a} \left(1 - \dfrac{W_{N_D+1}}{W_i} \right) & W_i > W_{N_D+1} \\ 0 & W_i \leq W_{N_D+1} \end{cases}$$

where $\sum_{i\in\mathcal{T}} p_i^* = P$. The necessary condition for the derived solution to be a NE is

$$\sum_{W_i > W_{N_D+1}} q_i^* < 1 \Longrightarrow N_D < W_{N_D+1} \sum_{W_i > W_{N_D+1}} \frac{1}{W_i} + \frac{2aQ}{1 - C_a} \Longrightarrow N_D < N_A \quad \text{(From (5.2) in Lemma 5.1)}$$

Particularly, if $N_D = 0$, then $q_i^* = 0, \forall i \in \mathcal{T}$,

$$p_i^* \begin{cases} \in [0, P] & W_i = W_1 \\ = 0 & W_i < W_1 \end{cases}$$

where $\sum_{i\in\mathcal{T}, W_i = W_1} p_i^* = P$.

Case 3: $\sum_{i\in\mathcal{T}} q_i^* < Q$ *and* $\sum_{i\in\mathcal{T}} p_i^* < P$. In this case, we have

$$\begin{cases} (1-2aq_i^*-C_a)W_i = 0 \\ W_i[p_i^*(2a+bC_f)-(bC_f+C_m)] = 0 \end{cases} \quad i\in\mathcal{T} \quad \Longrightarrow \quad \begin{cases} p_i^* = \dfrac{bC_f+C_m}{2a+bC_f} \\ q_i^* = \dfrac{1-C_a}{2a} \end{cases} \quad i\in\mathcal{T}.$$

The necessary condition of $\sum_{i\in\mathcal{T}} q_i^* < Q$ and $\sum_{i\in\mathcal{T}} p_i^* < P$ is $N_D \geq N$ and $N(1-C_a) \geq 2aQ$. Moreover, from Lemma 5.1, in this case, it holds that $N_A = N$.

The following theorem summarizes the above analysis results on the NE of G.

Theorem 5.2. *The strategy profile* $(\mathbf{p}^*, \mathbf{q}^*)$ *is a NE of* G *if and only if it holds that*

1. *If* $N_D < N_A$, *then*

$$p_i^* \begin{cases} = \dfrac{bC_f+C_m}{2a+bC_f} & W_i > W_{N_D+1} \\ \in \left[0, \dfrac{bC_f+C_m}{2a+bC_f}\delta\right] & W_i = W_{N_D+1} \\ = 0 & W_i < W_{N_D+1} \end{cases} \quad q_i^* = \begin{cases} \dfrac{1-C_a}{2a}\left(1-\dfrac{W_{N_D+1}}{W_i}\right) & W_i > W_{N_D+1} \\ 0 & W_i \leq W_{N_D+1} \end{cases}$$

where $\sum_{i\in\mathcal{T}} p_i^* = P$.

2. *If* $N_D \geq N_A$ *and* $N_A(1-C_a) > 2aQ$, *then*

$$p_i^* \begin{cases} = \dfrac{P_A}{W_i\sum_{j=1}^{N_A}\frac{1}{W_j}} - \left(\dfrac{N_A}{W_i\sum_{j=1}^{N_A}\frac{1}{W_j}}-1\right)\dfrac{bC_f+C_m}{2a+bC_f} & i\in\mathcal{T}_{\mathcal{S}} \\ \in \left[0,\ \dfrac{P_A}{W_i\sum_{j=1}^{N_A}\frac{1}{W_j}} - \left(\dfrac{N_A}{W_i\sum_{j=1}^{N_A}\frac{1}{W_j}}-1\right)\dfrac{bC_f+C_m}{2a+bC_f}\right] & i\in\mathcal{T}_{\mathcal{Q}} \\ = 0 & i\in\mathcal{T}-\mathcal{T}_{\mathcal{S}}-\mathcal{T}_{\mathcal{Q}} \end{cases}$$

$$q_i^* = \begin{cases} \dfrac{1}{2a}\left(1-C_a-\dfrac{N_A(1-C_a)-2aQ}{W_i\sum_{j=1}^{N_A}\frac{1}{W_j}}\right) & i\in\mathcal{T}_{\mathcal{S}} \\ 0 & i\in\mathcal{T}-\mathcal{T}_{\mathcal{S}} \end{cases}$$

where $P_A > \left(N_A - W_{N_A}\sum_{j=1}^{N_A}\dfrac{1}{W_j}\right)\dfrac{bC_f+C_m}{2a+bC_f}$, *and* $\sum_{i\in\mathcal{T}} p_i^* = P$.

3. *If* $N_D \geq N_A$ *and* $N_A(1-C_a) \leq 2aQ$, *in this case* $N_D = N_A = N$ *and*

$$p_i^* = \frac{bC_f+C_m}{2a+bC_f}, q_i^* = \frac{1-C_a}{2a} \quad i\in\mathcal{T}.$$

Remark 1: In Case 1 of Theorem 5.2, the attacker disposes limited attack resource such that the defender does not use up all its monitor resource or even does not monitor at all. This may also be due to that the monitor cost is too high or the detection rate a is too low. The valuable information that can be drawn is that in some cases where the attack intensity is low, it is a waste of resource for the defender to monitor all the time. If the monitor cost outweighs the gain, the defender is better off to keep silent.

Remark 2: In Case 2, both the attacker and defender use up all their resource to attack and monitor. In other words, the attacker's resource P and the defender's resource Q are constrained in the sense that at the NE, the payoff U_A/U_D is monotonously increasing in P/Q, i.e., given more resource, both players can increase their payoff, as shown in the following:

$$\begin{cases} U_A(\mathbf{p}^*, \mathbf{q}^*) = P\dfrac{N_A \cdot (1 - C_a) - 2aQ}{\sum_{j=1}^{N_A} \frac{1}{W_j}} \\ U_D(\mathbf{p}^*, \mathbf{q}^*) = Q\left[\dfrac{P(2a + bC_f)}{\sum_{j=1}^{N_A} \frac{1}{W_j}} - \dfrac{N_A(bC_f + C_m)}{\sum_{j=1}^{N_A} \frac{1}{W_j}}\right]. \\ -\dfrac{PN_A}{\sum_{j=1}^{N_A} \frac{1}{W_j}} + \dfrac{N_A^2}{\sum_{j=1}^{N_A} \frac{1}{W_j}} \dfrac{bC_f + C_m}{2a + bC_f} - \dfrac{bC_f + C_m}{2a + bC_f} \sum_{j=1}^{N_A} W_j \end{cases} \tag{5.5}$$

In this case, the game G can be regarded as a resource allocation problem that each player tries to choose the most profitable strategy under the resource constraint. The following corollary further highlights the NE in this case.

Corollary 5.1. *In Case 2 of Theorem 5.2, for* $\forall \mathbf{p}' \neq \mathbf{p}^*$, $\forall \mathbf{q}' \neq \mathbf{q}^*$, *let* $\widehat{\mathbf{p}} = \text{argmax}_{\mathbf{p} \in A_A} U_A(\mathbf{p}, \mathbf{q}')$, $\widehat{\mathbf{q}} = \text{argmax}_{\mathbf{q} \in A_D} U_D(\mathbf{p}', \mathbf{q})$ *it holds that* $U_D(\mathbf{p}^*, \mathbf{q}^*) > U_D(\widehat{\mathbf{p}}, \mathbf{q}')$ *and* $U_A(\mathbf{p}^*, \mathbf{q}^*) > U_A(\mathbf{p}', \widehat{\mathbf{q}})$.

Proof. Please refer to Section 5.10.3 for the sketch of proof. □

Corollary 1 implicates that if the defender does not operate on the NE $\mathbf{q}^*$, since the attacker chooses its strategy $\widehat{\mathbf{p}}$ that maximizes its payoff U_A, as a result, the defender gets less payoff than operating at $\mathbf{q}^*$. This also holds for the attacker. Hence, the NE not only corresponds to an equilibrium which is acceptable for both players such that they have no incentive to deviate, but consists of the optimal choice for both players. From the defender's point of view, operating on $\mathbf{q}$ is the optimal strategy in the worst-case scenario where the attack has sufficient attack resource.

Remark 3: In Case 3, both the attacker's resource P and the defender's resource Q are sufficient to attack and defend. In this case, the sensible target set $\mathcal{T}_\mathcal{S} = \mathcal{T}$, i.e., all targets are attacked/monitored. However, both the attacker and the defender do not use up the total resource to attack/defend, but rather reach an intermediate compromise at the NE which is unique. In such context, the situation can be regarded such that the attack and the defender are playing N atomic intrusion detection games G ($N = 1$) on each of the N target. Moreover, at the NE, we have

$$\begin{cases} U_A(\mathbf{p}^*, \mathbf{q}^*) = 0 \\ U_D(\mathbf{p}^*, \mathbf{q}^*) = -\dfrac{bC_f + C_m}{2a + bC_f} \sum_{j=1}^{N} W_j \end{cases}. \tag{5.6}$$

The implications behind (5.6) are:

1. Disposing more attack or monitor resource does not influence the NE and the payoff of both players at the NE.

2. For the attacker, decreasing the attack cost will not increase its utility at the NE since the defender will increase its monitor probability which will further drag U_A^* to 0.

3. For the defender, protecting more valuable targets represents more risk.

Given the security assets of the targets, improving the performance of the IDS module (increasing a and/or decreasing b) or/and decreasing the monitor cost/false alarm cost can increase its utility and alleviate the attack intensity at the NE.

5.4.3 Further Security Implications Behind NE

Theorem 5.2 quantifies the behavior of a rational attacker and defender at the NE from which no player has incentive to deviate. In some cases, the attacker's strategy at the NE $\mathbf{p}^*$ is not unique, but all $\mathbf{p}^*$ yields the attacker the same payoff. In contrast, the defender's strategy at the NE $\mathbf{q}^*$ is unique in all cases. From Theorem 5.2, we can see that a rational attacker will never choose the extreme strategies such as attacking the target with the largest security asset, or evenly distributing its attack resource. Such strategies can be easily defended by the defender and thus cannot bring the most payoff to the attacker. Hence the attacker focuses its attack on $\mathcal{T}_{\mathcal{S}}$ and $\mathcal{T}_{\mathcal{Q}}$ with the probability distribution $\mathbf{p}^*$. With this information in mind, we provide the following guidelines for the defender:

Guideline 2: The defender should choose the monitor probability distribution $\mathbf{q}^*$ according to Theorem 5.2. Under such context, the attacker gets the same payoff by attacking any monitored targets and gets less payoff by attacking any non-monitored targets.

In fact, to equalize the attacker's payoff of attacking any monitored targets turns to be the best choice since otherwise, the attacker will attack the least protected target i where $(1-C_a-2aq_i)W_i$ is maximized to gain extra payoff and the defender's payoff decreases accordingly.

We then study the impact of the monitor resource constraint on the system to gain a more in-depth insight on the NE. To this end, we compare the defender's payoff at the NE of Case 2 where the monitor resource is constrained and Case 3 where defender disposes sufficient resource.

From (5.5) and (5.6), we can see that the resource constraint has a significant negative impact on the system when P is large: for the attacker, it cannot get any profit if the defender has enough resource to monitor ($U_A = 0$), on the contrary if the monitor resource is not sufficient, the attacker's payoff reaches $O(W_i)$; at the defender side, we can quantify the payoff loss due to the lack of monitor resource as:

$$L = -Q\left[\frac{P(2a+bC_f)}{\sum_{j=1}^{N_A}\frac{1}{W_j}} - \frac{N_A(bC_f+C_m)}{\sum_{j=1}^{N_A}\frac{1}{W_j}}\right] + \frac{PN_A}{\sum_{j=1}^{N_A}\frac{1}{W_j}} - \frac{N_A^2}{\sum_{j=1}^{N_A}\frac{1}{W_j}}\frac{bC_f+C_m}{2a+bC_f} - \frac{bC_f+C_m}{2a+bC_f}\sum_{j=N_A+1}^{N}W_j.$$

We can see that with the increase of P, the loss turns positive and may raise to $O(W_i)$.

Following the above analysis, the necessary conditions to limit the damage caused by the attacker are disposing sufficient monitor resource and operating on $\mathbf{q}^*$ of Case 3 of Theorem 5.2 in that the attacker's payoff drops to 0 at the NE regardless of the attack resource P.

Until now, our analysis was based on the condition that there is one defender, i.e., $Q \leq 1$. In case where $N(1-C_a) > 2a$, one defender is not enough to maintain the favorable NE. Obviously more than one defender is needed. Hence, a natural question we pose is that under such context, how much monitor resource Q, or moreover, how many defenders are needed to achieve system optimality in terms of security? How to configure them to maximize U_D?

5.5 Intrusion Detection Game with Multiple Attackers/Defenders

In this section, we extend our efforts to the intrusion detection game with multiple attackers/defenders to study the posed questions. To this end, we relax the resource constraint $P \leq 1$ and $Q \leq 1$. We base our study on the following assumptions:

1. The attacker side disposes sufficient attack resource P.
2. The attackers can communicate and cooperate among themselves to launch attacks and so do the defenders to arrange their monitoring.
3. The attack gain on the same target is not cumulative, i.e., if attackers A_i and A_j attack the same target m simultaneously with success, the attack gain is $U_A^m = (1 - C_a)W_m$, not $2(1 - C_a)W_m$.

Assumption 3 is a simplified scenario. In fact, the attack gain may range from $(1 - C_a)W_m$ to $\min\{2(1 - C_a)W_m, W_m\}$ depending on the specific scenarios, noticing that target m cannot lose more than the security asset W_m it holds even in the worst case. Here in order to perform a closed-form analysis, we focus on the simplified scenario where the gain of multiple attacks on the same target is not cumulative. We consider it a reasonable assumption when the attackers can communicate among them and multiplying attacks does not increase the chance of success or decrease the attack cost. In other scenarios, the assumption does not hold. However, our analysis in the simplified case can be adapted to investigate these cases by modifying the attackers' utility function to take into account the cumulative effect of the attacks on the attack gain and cost.

At the defender side, having multiple defenders monitor the same target influences the detection and the false alarm rate, thereby may change the final payoff. We thus conduct our analysis for the following two cases. In the first case, each target is monitored by at most one defender at any time. In the second case, we allow one target to be monitored by several defenders simultaneously and their results are combined to further detect possible attacks.

5.5.1 Case 1

Since the attack gain is not cumulative, the attackers will never attack the same target simultaneously. In this subsection, we address the case where any target is monitored by at most one defender at any time. The intuition of adopting this strategy is to use the monitor resource in an economic way, i.e., to cover the most targets possible with the monitor resource Q. In such context, our previous analysis can be applied with slight modification on the notation p_i and q_i: now p_i denotes the total attack resource from the attackers spent to attack the target i; similarly, q_i denotes the total monitor resource from the defenders spent to monitor the target i. Apply Theorem 5.2, the NE $(\mathbf{p}^*, \mathbf{q}^*)$ can be derived as:

1. If $2a \leq 1 - C_a$, then $p_i^* = 1$ and $q_i^* = 1, \forall i \in \mathcal{T}$. In this case, the IDS modules of the defenders are not efficient enough to thwart attacks. The payoff of the players at the NE is

$$\begin{cases} U_A(\mathbf{p}^*, \mathbf{q}^*) = (1 - C_a - 2a) \sum_{i \in \mathcal{T}} W_i \\ U_D(\mathbf{p}^*, \mathbf{q}^*) = -(1 - 2a + C_m) \sum_{i \in \mathcal{T}} W_i \end{cases}$$

2. If $2a > 1 - C_a$, then $p_i^* = \dfrac{bC_f + C_m}{2a + bC_f}$, $q_i^* = \dfrac{1 - C_a}{2a}$, $i \in \mathcal{T}$. The correspondent payoff is: $U_A(\mathbf{p}^*, \mathbf{q}^*) = 0$ and $U_D(\mathbf{p}^*, \mathbf{q}^*) = -\sum_{i \in \mathcal{T}} \dfrac{bC_f + C_m}{2a + bC_f} W_i$.

Here we implicitly assume that $C_m \leq 2a$ in that $C_m > 2a$ leads to $q_i^* = 0$, which is the trivial case where the defender side do not monitor any target due to the high monitor cost.

For Case 1, it is clear that the number of defenders required to maintain the above NE is $N_{min} = N$. For Case 2, at the NE, $\sum_{i \in \mathcal{T}} q_i = \dfrac{N(1 - C_a)}{2a}$. Noticing that each defender disposes at most $q_i = 1$ as monitor resource, we need at least $N_{min} = \left\lceil \dfrac{N(1 - C_a)}{2a} \right\rceil$ defenders to maintain the above NE under the condition that the defenders can cooperate among them to arrange their monitoring, where $\lceil n \rceil$ denotes the smallest integer not less than n. Following the condition $2a > 1 - C_a$, we have $N_{min} \leq N$ and if $C_a \ll 1$, $N_{min} \sim \dfrac{N(1 - C_a)}{2a} \sim \dfrac{N}{2a} > \dfrac{N}{2}$.

The intuition behind the above results is that if the detection rate of the defenders is not high enough to thwart the attacks, then each target should be monitored as much as possible to decrease the damages caused by the attackers as much as possible. On the other hand, if the defenders are efficient enough in terms of the detection rate, then less monitor resource is required because in such context, the attacker side does not attack on the maximum intensity.

Can we improve the results by letting multiple defenders monitor the same target simultaneously and combine the monitor results to make the final decision? We answer this question by performing the following analysis.

5.5.2 Case 2

The intuition of adopting this strategy is to combine the monitor results of multiple defenders to achieve better performance. As price, the monitor cost is higher.

Consider the case where x defenders monitor the same target simultaneously and the attack is said to be detected if it is detected by at least y ($1 \leq y \leq x$, referred to as detection threshold) out of the x defenders. The aggregate detection rate a_x^y and false alarm rate b_x^y can be computed as:

$$\begin{cases} a_x^y = \sum_{i=y}^{x} \binom{x}{i} a^i (1-a)^{x-i} \\ b_x^y = \sum_{i=y}^{x} \binom{x}{i} b^i (1-b)^{x-i} \end{cases}$$

where a and b is the detection and false alarm rate of the individual defender. The following straightforward lemma studies a_x^y and b_x^y.

Lemma 5.2. *$\forall x, y \in \mathbb{Z}^+, y \leq x$ and $0 < a, b < 1$, it holds that:*

- *Both a_x^y and b_x^y is monotonously decreasing w.r.t. y given x and w.r.t. x given y ($y \leq x$).*
- *If $x > 1$, then $a_x^y < xa$, $b_x^y < xb$.*

Extending Theorem 5.2, at the NE $(\mathbf{p}^*, \mathbf{q}^*)$, we have:

1. If $2a_{x_i}^{y_i} \leq 1 - C_a$, then $p_i^* = 1, q_i^* = 1, \forall i \in \mathcal{T}$,

$$\begin{cases} U_A(\mathbf{p}^*, \mathbf{q}^*) = (1 - C_a - 2a_{x_i}^{y_i}) \sum_{i \in \mathcal{T}} W_i \\ U_D(\mathbf{p}^*, \mathbf{q}^*) = -(1 - 2a_{x_i}^{y_i} + x_i C_m) \sum_{i \in \mathcal{T}} W_i \end{cases}$$

2. If $2a_{x_i}^{y_i} > 1 - C_a$, then $p_i^* = \dfrac{b_{x_i}^{y_i} C_f + x_i C_m}{2a_{x_i}^{y_i} + b_{x_i}^{y_i} C_f}$, $q_i^* = \dfrac{1 - C_a}{2a_{x_i}^{y_i}}$, $i \in \mathcal{T}$. The correspondent payoff is $U_A(\mathbf{p}^*, \mathbf{q}^*) = 0$ and $U_D(\mathbf{p}^*, \mathbf{q}^*) = -\sum_{i \in \mathcal{T}} \dfrac{b_{x_i}^{y_i} C_f + x_i C_m}{2a_{x_i}^{y_i} + b_{x_i}^{y_i} C_f} W_i$.

where x_i denotes the number of defenders simultaneously monitoring the target i with the detection threshold y_i, p_i denotes the total attack resource from attackers spent to attack the target i, q_i denotes the monitor resource of each of the x_i defenders spent to monitor the target i.

The previous subsection where each target is monitored by at most one defender at any time can be regarded as the degenerate case $x_i = y_i = 1$. For Case 1, we have $N_{min} = N$ at $x_i = y_i = 1$. For Case 2, if $x_i = 1$, $N_{min} = N$; If $x_i > 1$, it follows from Lemma 5.2 that $N_{min} = \left\lceil \sum_{i \in \mathcal{T}} x_i \dfrac{(1 - C_a)}{2a_{x_i}^{y_i}} \right\rceil > \left\lceil \dfrac{N(1 - C_a)}{2a} \right\rceil$.

Compare the above analysis with the results in Section 5.4.1 where each target is monitored by one defender, if each target is monitored by multiple defenders simultaneously, more defenders are usually needed to maintain the NE although the detection rate may be higher. Hence, to minimize the required number of defenders, the monitor resource should be used in an economic way such that each target is monitored by at most one defender at any time.

However, if the objective of the defender side is not to maintain the NE with minimum number of defenders, but rather to maximize its payoff at the NE, e.g., if there is sufficient monitor resource, then the answer may be different. In such context, the defender side needs to solve the optimization problem $\max_{1 \leq y_i \leq x_i} U_D(\mathbf{p}^*, \mathbf{q}^*)$, as summarized in the following theorem:

Theorem 5.3. *The optimal strategy for the defender side is to let each target be monitored by x^* defenders simultaneously with the detection threshold y^*:*

$$(x^*, y^*) = \begin{cases} \underset{1 \leq y \leq x,\ 2a_x^y \leq 1 - C_a}{\operatorname{argmin}} & 1 - 2a_x^y + xC_m \quad C_1 < C_2 \\ \underset{1 \leq y \leq x,\ 2a_x^y > 1 - C_a}{\operatorname{argmin}} & \dfrac{b_x^y C_f + xC_m}{2a_x^y + b_x^y C_f} \quad C_1 \geq C_2 \end{cases}$$

where

$$\begin{cases} C_1 = \min\limits_{1 \leq y \leq x} 1 - 2a_x^y + xC_m \quad s.t. \quad 2a_x^y \leq 1 - C_a \\ C_2 = \min\limits_{1 \leq y \leq x} \dfrac{b_x^y C_f + xC_m}{2a_x^y + b_x^y C_f} \quad s.t. \quad 2a_x^y > 1 - C_a \end{cases}$$

Remark: The above optimization problem can be solved numerically. The choice of x^* consists of searching a tradeoff between the amount of observation based on which the final decision is made and the monitor cost. The choice of y^* consists of searching a tradeoff between the detection rate and the false alarm rate: with a larger y, the false alarm rate b_x^y decreases, but the detection rate a_x^y also decreases. A bad choice of y may lead to significant sub-optimality at the defender

side even if it disposes sufficient monitor resource. We will show this point via numerical study in Section 5.7.

At the optimal configuration, at least $N_{min} = \left\lceil \frac{Nx^*(1-C_a)}{2\sum_{i=y^*}^{x^*} C_{x^*}^i a^i (1-a)^{x^*-i}} \right\rceil$ defenders are needed to achieve the system optimality in terms of security.

Based on the results in this section, we have the following guidelines for the defenders:

Guideline 3: In any case, at least $\left\lceil \frac{N(1-C_a)}{2a} \right\rceil$ defenders are needed in order to effectively monitor the targets.

Guideline 4: In some cases, having multiple defenders monitoring the targets simultaneously and combining their results helps the defenders achieve optimal protection performance.

5.6 Model Application: Case Study

In this section, we provide two case studies to show how our game theoretic framework can be applied in the IDS configuration and deployment for wireless networks.

5.6.1 Case Study 1

In [RB06], Abderrezak and Abderrahim propose a secure architecture for mobile ad hoc networks. Their approach divides the ad hoc network into clusters and implements a decentralized certification authority. Each cluster has a cluster head (CH). The private key of the certification authority (CA) is distributed over CHs using threshold cryptography where every CH holds a fragment of the whole key. Each cluster is managed by the CH in the cluster which plays the role of certifying public keys of the cluster's member nodes and a set of nodes called Registration Authority (RA), which are nodes with high trust level. The role of RAs is to filter and analyze certificate requests before forwarding them to the CH and monitor the cluster's member nodes by rating each of its neighbor nodes with the reputation rate which reflects the trust level of the monitored node. The cluster's member nodes with sufficiently high reputation rate are elected as RAs if necessary.

In the proposed security architecture, a crucial issue is to determine the monitor strategy of the RAs. To this end, we apply our game theoretic framework. The solution procedure can be summarized in three steps:

1. Determine the security assets of the targets
2. Compute the sensible target set $\mathcal{T}_S$ based on Lemma 5.1
3. Apply Theorem 5.2 to determine the monitor strategy $\mathbf{q}$

In the studied scenario, we consider the reputation rate of a node as its security asset, i.e., $W_i = R_i$ for node i whose reputation rate is R_i. We consider the worst-case scenario where the attacker side disposes sufficient attack resource. In ad hoc networks, it is usually extremely easy to launch attacks. It follows that $C_a \ll 1$. To calculate the sensible target set $\mathcal{T}_S$, we sort the nodes by their security assets as: $W_1 \geq W_2 \geq \cdots \geq W_N$ and apply Lemma 5.1 to compute N_A by the

following inequalities:

$$\begin{cases} W_{N_A} > \dfrac{N_A - 2a}{\sum_{j=1}^{N_A} \frac{1}{W_j}} \\ W_{N_A+1} \leq \dfrac{N_A - 2a}{\sum_{j=1}^{N_A} \frac{1}{W_j}} \end{cases} .$$

In the last step, we apply Theorem 5.2 to compute the monitor strategy $\mathbf{q}$:

$$q_i^* = \begin{cases} \dfrac{1}{2a}\left(1 - \dfrac{N_A - 2a}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}}\right) & i \geq N_A \\ 0 & i < N_A \end{cases} .$$

5.6.2 Case Study 2

In [SSA06], Subhadrabandhu *et al.* postulate that the wireless ad hoc networks in near future will consist of two classes of nodes: (1) inside nodes communicate using the network and at the same time perform system tasks like relaying packets, discovering routes, securing communication, etc; (2) outside nodes only communicate using the network. Examples of inside nodes include pre-deployed terminals, access points and trusted users. Outside nodes are usually common users and visitors. In such architecture, to ensure the security of the network, a subset of inside nodes are equipped with IDS modules. Such inside nodes are called IDS capable inside nodes. Operating in promiscuous mode, the IDS capable inside nodes monitor the outside nodes in their neighborhood in order to isolate any malicious attackers. Due to the coverage redundancy, each outside node is monitored by multiple IDS capable inside nodes, which may decide differently base on their own observations. These different decisions are further combined to make the final decision. In such context, the task for the IDS designer is to determine how many IDS capable inside nodes are needed to monitor efficiently the outside nodes and how to configure them.

Theorem 5.3 can be applied to answer the above question. More specifically, by solving the optimization problem $\max_{1 \leq x \leq y} U_D(\mathbf{p}^*, \mathbf{q}^*)$, we obtain x^* and y^*. The resulting optimal strategy is thus to let x^* IDS capable insides nodes monitor one outside node simultaneously with the detection threshold y^*. The choice of x^* consists of searching a tradeoff between the amount of observation based on which the final decision is made and the monitor cost. The choice of y^* consists of searching a tradeoff between the detection rate and the false alarm rate. Moreover, let N_o be the number of outside nodes to be monitored in the network, $\left\lceil \dfrac{N_o x^*(1-C_a)}{2\sum_{i=y^*}^{x^*} \binom{x^*}{i} a^i (1-a)^{x^*-i}} \right\rceil$ IDS capable inside nodes are needed to efficiently monitor the outside nodes in the network. In other words, each outside node should be monitored by at least $\left\lceil \dfrac{x^*(1-C_a)}{2\sum_{i=y^*}^{x^*} \binom{x^*}{i} a^i (1-a)^{x^*-i}} \right\rceil$ IDS capable inside nodes.

After dimensioning the IDS capable inside nodes, the next step is to select the IDS capable inside nodes among all inside nodes. The goal of this step is to minimize the number of IDS capable nodes under the constraint that each outside nodes is monitored by at least $\left\lceil \dfrac{N_o x^*(1-C_a)}{2\sum_{i=y^*}^{x^*} \binom{x^*}{i} a^i (1-a)^{x^*-i}} \right\rceil$ IDS capable inside nodes. The heuristic algorithm MUNEN proposed in [SSA06] can be applied here to select IDS inside nodes.

It is interesting to compare our work with that in [SSA06] where the authors propose a statistical

framework for intrusion detection for ad hoc networks. They focus on minimizing the monitor resource consumption subject to limiting the security risk under given threshold. Our work, on the other hand, focuses on finding the optimal strategy for the defenders to achieve system optimality in terms of security. These two solutions actually address the intrusion detection problem from two different angles, that in [SSA06] from an optimization angle while ours from a game theoretic angle.

5.7 Network Intrusion Detection as a Stackelberg Game

In the previous sections, we focused on the intrusion detection game where both the attacker and the defender side take the decision locally at the same time. However, in many cases, the attackers may launch attacks based on the strategy of the defenders or conversely, the defenders decide the strategy based on the attackers strategy. In this subsection, we address these cases by modeling the interaction between the attackers and the defenders as a Stackelberg game [OR94], in which a "leader" chooses a strategy and then a "follower", informed of the leader's choice, chooses its strategy accordingly such that both sides try to maximize their payoff. We thus formulate a noncooperative Stackelberg game for the intrusion detection G^S as follows. In the following formulation, the attacker side plays the role of leader, the counterpart case where the defender side plays the role of leader can be formulated in the same way.

Players:	Leader: attacker side; Follower: defender side
Strategy:	$\mathbf{p} \in A_A$ and $\mathbf{q} \in A_D$
Payoff:	U_A for leader and U_D for follower
Game rule:	the leader decides $\mathbf{p}$ first, the follower decides $\mathbf{q}$ after knowing $\mathbf{p}$

Follower's Problem:

The follower is given the leader's chosen strategy. It then chooses its strategy to maximize its payoff. Formally, for any given $\mathbf{p} \in A_A$, the follower solves the following optimization problem:

$$\mathbf{q}(\mathbf{p}) = \underset{\mathbf{q} \in A_D}{\operatorname{argmax}} U_D(\mathbf{p}, \mathbf{q})$$

Leader's Problem:

The leader knows that the follower will choose its strategy to greedily maximize its payoff. Therefore, the leader chooses its strategy which will maximize its payoff, given the follower will subsequently choose its strategy to maximize its payoff. Formally, the leader solves the following optimization problem:

$$\mathbf{p}(\mathbf{q}) = \underset{\mathbf{p} \in A_A}{\operatorname{argmax}} U_D(\mathbf{p}, \mathbf{q}(\mathbf{p}))$$

The Stackelberg game is often solved by backwards induction: First solve the follower's problem for every possible strategy taken by the leader; The solution consists of the best response strategy of the follower as a function of the leader's strategy; Then the leader decides its optimal strategy according to the follower's best response strategy. The obtained solution is often referred to as a Stackelberg equilibrium (SE) or Stackelberg-Nash equilibrium (SNE).

Next we study the SNE of G^S for the case where the attacker side is the leader and the follower, respectively. In the following study, we focus on the scenario where $2a > 1 - C_a$, $C_m, C_a \ll 1$, both the attacker and the defender side process sufficient attack and monitor resource P and Q

respectively, and each target is monitored by at most one defender at any time. However, our study is also applicable in other cases although the result may be different.

5.7.1 Leader: Attacker Side; Follower: Defender Side

In this case, the attacker side is the leader. By performing backwards induction, we can solve the best response of the follower as:

$$q_i(\mathbf{p}) \begin{cases} = 0 & p_i < \dfrac{bC_f + C_m}{2a + bC_f} \\ \in [0,1] & p_i = \dfrac{bC_f + C_m}{2a + bC_f} \\ = 1 & p_i > \dfrac{bC_f + C_m}{2a + bC_f} \end{cases}.$$

Noticing the payoff of the leader is $\sum_{i \in \mathcal{T}} p_i W_i (1 - C_a - 2a q_i(\mathbf{p}))$, we obtain the SNE $(\mathbf{p^S}, \mathbf{q^S})$ as follows

$$\begin{cases} p_i^S = \dfrac{bC_f + C_m}{2a + bC_f} & i \in \mathcal{T} \\ q_i^S = 0 & i \in \mathcal{T} \end{cases}.$$

The corresponding payoff of the leader and follower is as follows

$$\begin{cases} U_A(\mathbf{p^S}, \mathbf{q^S}) = \dfrac{bC_f + C_m}{2a + bC_f}(1 - C_a) \sum_{i \in \mathcal{T}} W_i \\ U_D(\mathbf{p^S}, \mathbf{q^S}) = -\dfrac{bC_f + C_m}{2a + bC_f} \sum_{i \in \mathcal{T}} W_i \end{cases}.$$

However, the above obtained SNE is a weak equilibrium in that $U_D(\mathbf{p^S}, \mathbf{q^S}) = U_D(\mathbf{p^S}, \mathbf{q}'), \forall \mathbf{q}' \in \mathbf{A_D}$, hence the leader is not sure whether the follower will operate on $\mathbf{q^S}$ or not. This may have detrimental effect on the payoff of the leader: e.g., if the follower sets $q_i = 1$ for all target i instead of $q_i = 0$, then $U_A = \dfrac{bC_f + C_m}{2a + bC_f}(1 - C_a - 2a) \sum_{i \in \mathcal{T}} W_i < 0$, as consequence, the leader get negative payoff. This is clearly not desirable for the leader (attacker) in that its payoff is 0 when doing nothing.

To push the follower to choose the desired $\mathbf{q^S}$ from the leader's perspective, the leader has incentive to set $p_i = p_i^S - \epsilon = \dfrac{bC_f + C_m}{2a + bC_f} - \epsilon$ where ϵ is a small positive number. Under such context, the follower will operate on $\mathbf{q^S}$. For the leader, its payoff is $\dfrac{bC_f + C_m}{2a + bC_f}(1 - C_a) - \epsilon(1 - C_a) \sum_{i \in \mathcal{T}} W_i$, only slightly less than its desired payoff at the SNE if ϵ is sufficiently small, which we argue is acceptable for the leader.

	Lead ($\mathbf{p^L}$)	Follow ($\mathbf{p^F}$)
Lead	$U_A = -\frac{bC_f + C_m}{2a + bC_f}\delta \sum_{i\in\mathcal{T}} W_i$	$U_A = 0$
($\mathbf{q^L}$)	$U_D = -\left[\frac{bC_f + C_m}{2a + bC_f} + \frac{1 - C_a}{2a}(2a + bC_f)\epsilon - \epsilon\right] \sum_{i\in\mathcal{T}} W_i$	$U_D = -\left(\frac{1 - C_a}{2a} + \delta\right)(bC_f + C_m) \sum_{i\in\mathcal{T}} W_i$
Follow	$U_A = \left(\frac{bC_f + C_m}{2a + bC_f} - \epsilon\right)(1 - C_a) \sum_{i\in\mathcal{T}} W_i$	$U_A = 0$
($\mathbf{q^F}$)	$U_D = -\left(\frac{bC_f + C_m}{2a + bC_f} - \epsilon\right)(1 - C_a) \sum_{i\in\mathcal{T}} W_i$	$U_D = 0$

Table 5.2: Payoff Matrix of the lead-or-follow game

5.7.2 Leader: Defender Side; Follower: Attacker Side

The above analysis can be applied in this symmetrical case where the leader is the defender side. The SNE $(\mathbf{p^S}, \mathbf{q^S})$ is:

$$\begin{cases} p_i^S = 0 & i \in \mathcal{T} \\ q_i^S = \dfrac{1 - C_a}{2a} & i \in \mathcal{T} \end{cases}.$$

To push the follower to choose the desired $\mathbf{p^S}$ from the leader's point of view, the leader sets $q_i = q_i^S - \delta = \frac{1 - C_a}{2a} + \delta$ where δ is a small positive number. Under such context, the follower will operate on $\mathbf{p^S}$. For the leader, its payoff is $-\frac{1 - C_a}{2a}(C_m + bC_f) \sum_{i\in\mathcal{T}} W_i - \delta(C_m + bC_f) \sum_{i\in\mathcal{T}} W_i$, only slightly less than its desired payoff at the SNE if δ is sufficiently small.

5.7.3 Lead or Follow

We next consider an interesting scenario where the attack/defender side decides whether to be the leader (pick the leader's strategy obtained previously) or the follower (pick the follower's strategy) without the knowledge of its opponent's choice. In such context, does the strategy to be the leader dominate the strategy to be the follower in that according to our analysis, the leader may "control" the behavior of the follower to some extent, but does it hold in the scenario considered in this subsection?

We study the following "lead or follow" intrusion detection game to answer the posed question: the players are the attacker and the defender side; they choose either the leader strategy (denoted by $\mathbf{p^L}$ and $\mathbf{q^L}$, respectively) or the follower strategy (denoted by $\mathbf{p^F}$ and $\mathbf{q^F}$, respectively) to maximize their payoff U_A and U_D defined previously. $\forall i \in \mathcal{T}$, we have

$$\begin{cases} p_i^L = \dfrac{bC_f + C_m}{2a + bC_f} - \epsilon \\ q_i^L = \dfrac{1 - C_a}{2a} + \delta \end{cases} \qquad \begin{cases} p_i^F = 0 \\ q_i^F = 0 \end{cases}.$$

The payoff of the attacker and the defender side is depicted in Table 5.2. Since both ϵ and δ are sufficiently small, the terms containing $\epsilon\delta$ are ignored in the table.

Recall that we consider the scenario where $2a > 1 - C_a$ and $C_m, C_a \ll 1$. From the point of view of the defender side, the first line is strictly dominated by the second line, indicating that the

defender side is always better off choosing to be the follower. Moreover, there exists a unique NE for the lead-or-follow game which is $(\mathbf{p^L}, \mathbf{q^F})$, i.e., the attacker side is the leader and the defender sides follows.

The obtained NE of the "lead or follow" game seems to be more favorable to the attacker side since it can control the strategy of the follower, the defender side, by being the leader and push the follower to keep silent. However, in fact the defender side also "control" the attacker side by being the follower: this can be shown by the fact that the leader's strategy and payoff at the unique NE depend uniquely on the parameters of the defender. That is to say, the follower can exert its influence on the leader via its performance parameters, e.g., if $b, C_m \ll a$, both p_i and U_A are very small at the NE.

According to our model, an efficient defender system can not only achieve high detection rate, but also significantly limit the attack probability and consequently limit the harm that the attacker may do on the system. To let multiple defenders monitor one target simultaneously, as discussed in Section 5.4, is one way to increase the efficiency of the defender system, e.g., the defender side sets x, y such that $U_D = -\left(\frac{b_x^y C_f + C_m}{2a_x^y + b_x^y C_f} - \epsilon\right)(1 - C_a)\sum_{i \in \mathcal{T}} W_i$ is maximized.

One issue we would like to mention is that the above analysis is based on the condition that both the attacker and the defender side have sufficient attack and monitor resource. The defender side being the follower ($q_i^F = 0$) does not mean that no defender is needed to maintain the NE. On the contrary, the NE can be viewed as an optimal "agreement" between the two players such that before reaching the "agreement", the players may try different strategies to choose one that maximize their payoff. If, for example, the defender side does not have enough monitor resource, the attacker will not choose the strategy $\mathbf{p^L}$, instead, it may operate on $p_i = 1$ to maximize its payoff. Thus the sufficiency of resource is the necessary condition of the NE outcome.

5.8 Numerical Study

In this section, we perform numerical study on two typical scenarios to validate our analytical results.

We first consider a network with high requirement on security, e.g., military networks usually require a high level of confidentiality and need to be resistant to various attacks. In such scenario, the security assets of targets W_i ($i \in \mathcal{T}$) are much higher than the related cost: i.e., $C_a, C_m, C_f \ll 1$. We set $C_a = C_m = 0.001$ and $C_f = 0.01$. The defenders are usually equipped with high-performance IDS modules with powerful processing capability. Hence a relatively large value $a = 0.9$ and small value $b = 0.05$ are chosen in our study.

The second scenario we consider is at the other end of the spectrum where the attack/monitor cost is important (we set $C_a = C_m = 0.1$ and $C_f = 0.3$ in this case), e.g., a WLAN at the airport where both attackers and defenders have limited battery and processing capability. The defender in such cases are usually not so efficient. We thus set $a = 0.4$ and $b = 0.2$. In both scenarios, there are 10 targets with normalized security assets: $W_i = (11 - i) * 0.1$ ($i = 1, 2, \cdots, 10$).

5.8.1 One Attacker, One Defender

We start with the network intrusion detection game with one attacker/defender. The attack resource P and the monitor resource Q are both set to 1. Table 5.3 shows the NE $(\mathbf{p}^*, \mathbf{q}^*)$

calculated using our analytical model. As shown in the analytical results, both the attack and defender focus only on the targets in the sensible target set (Target 1-6 for scenario 1 and target 1-4 for scenario 2).

Scenario 1	Scenario 2
$p_1^* = 0.118$, $q_1^* = 0.279$	$p_1^* = 0.239$, $q_1^* = 0.394$
$p_2^* = 0.131$, $q_2^* = 0.249$	$p_2^* = 0.245$, $q_2^* = 0.313$
$p_3^* = 0.147$, $q_3^* = 0.211$	$p_3^* = 0.253$, $q_3^* = 0.212$
$p_4^* = 0.161$, $q_4^* = 0.169$	$p_4^* = 0.262$, $q_4^* = 0.081$
$p_5^* = 0.197$, $q_5^* = 0.096$	$p_5^* = 0$, $q_5^* = 0$
$p_6^* = 0.236$, $q_6^* = 0.004$	$p_6^* = 0$, $q_6^* = 0$
$p_7^* = 0$, $q_7^* = 0$	$p_7^* = 0$, $q_7^* = 0$
$p_8^* = 0$, $q_8^* = 0$	$p_8^* = 0$, $q_8^* = 0$
$p_9^* = 0$, $q_9^* = 0$	$p_9^* = 0$, $q_9^* = 0$
$p_{10}^* = 0$, $q_{10}^* = 0$	$p_{10}^* = 0$, $q_{10}^* = 0$
$U_A^* = 0.459$, $U_D^* = -0.460$	$U_A^* = 0.585$, $U_D^* = -0.800$

Table 5.3: NE

	Scenario 1	Scenario 2
$(U_D)_{max}$	-0.561	-0.965
$\overline{U_D}$	-0.823	-1.265
$(U_D^*)_{min}$	-0.461	-0.801

Table 5.4: Payoff degradation due to deviation from NE

To further evaluate our analytical results and proposed design guidelines, we investigate the cases where the defender does not operate on the NE. We thus simulate 300 random strategies for the defender and we calculate the correspondent payoff U_D under the condition that the attacker chooses its strategy to maximize its payoff. Table 5.4 shows the results: $(U_D)_{max}$ denotes the maximum payoff of the defender with the simulated 300 random strategies, $\overline{U_D}$ denotes the average payoff of the defender, $(U_D^*)_{min}$ denotes the minimum payoff of the defender under the condition that the defender operate on $\mathbf{q}^*$ and the attacker choose its strategy to maximize its payoff. Comparing the above numerical results, we can see that in the simulated scenarios, the NE consists of the optimal choice for the defender under the condition that the attacker is intelligent to choose its strategy maximizing its payoff. The above numerical result confirms the proposed guideline 1 and 2 in the analytical model.

In practice, the detection rate a and the false alarm rate b usually cannot be accurately measured or estimated. To evaluate the impact of the defender's estimation error of a and b on the utility of players, we conduct a sensitivity analysis. More specifically, we vary the error $|\Delta a|/a$ and $|\Delta b|/b$ and let the defender operate on the NE strategy based on the inaccurate estimation. At the attacker side, it chooses its strategy to maximize U_A. Figure 5.1 plots the increase of U_A and the degradation of U_D w.r.t. U_A and U_D without estimation errors as functions of the relative estimation error $\frac{|\Delta a|}{a}$ and $\frac{|\Delta b|}{b}$ in both scenarios. The results show that the impact on the estimation error of b is negligible. In contrast, the impact of the estimation error of a on the players' payoff varies from $5 - 11\%$ when the error reaches 25%. We also observe that over estimating a always leads to more increase (decrease) of U_A (U_D) than under estimating it.

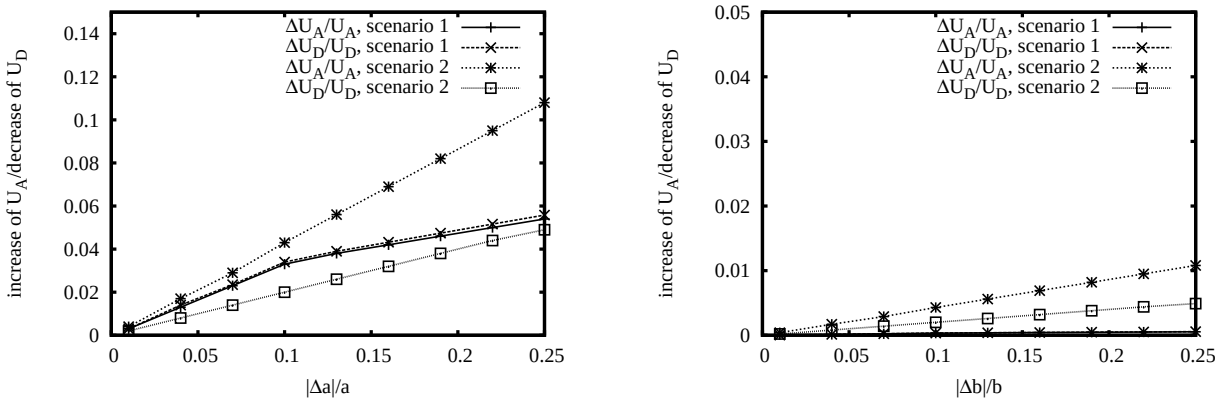

Figure 5.1: Sensitivity analysis on the error of a (left) and b (right)

5.8.2 Multiple Attackers/Defenders

We then study the case of multiple attackers/defenders and investigate the optimal strategy for the defender side. Figure 5.2 plots $-U_D$ at the NE for the studied scenarios with different x, y. Table 5.5 shows the optimal strategy for the defender side according to the analytical model.

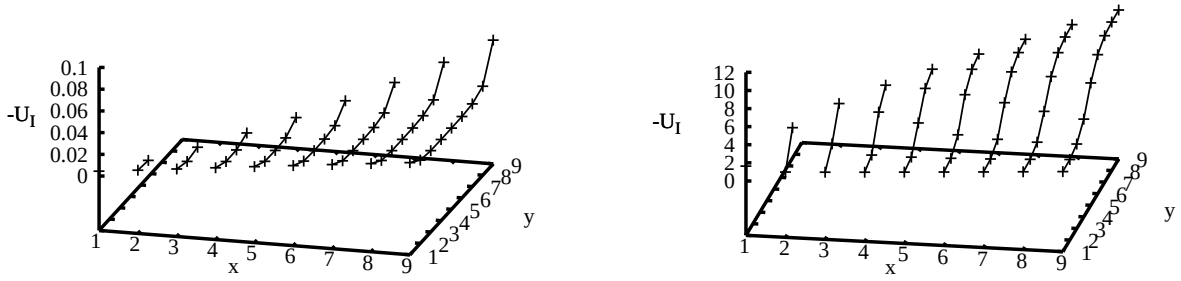

Figure 5.2: $-U_D$ as function of x, y, left: scenario 1; right: scenario 2

Scenario 1	Scenario 2
$x^* = 1$, $y^* = 1$ $p_i^* = 0.00083$, $q_i^* = 0.556$ $N_{min} = 6$	$x^* = 2$, $y^* = 1$ $p_i^* = 0.237$, $q_i^* = 0.703$ $N_{min} = 15$
$U_A^* = 0$, $U_D^* = -0.0046$	$U_A^* = 0$, $U_D^* = -1.22$

Table 5.5: Optimal strategy for defenders

For scenario 1, the optimal strategy for the defender side is to let each target to be monitored by at most one defender simultaneously at the probability 0.556. The minimum number of required defenders is 6. For scenario 2, the optimal strategy for the defender side is to let each target to be monitored by 2 defenders simultaneously at the probability 0.703. In such case, we have $a(x = 2, y = 1) = 0.64$, the minimum number of required defenders is 15 according to Theorem 5.3.

From the above results, we can see that the optimal strategy for the defender side depends very much on the parameters such as a, b etc. The payoff U_D in scenario 1 is much less sensitive w.r.t. y especially when $y \leq x - 2$ then in scenario 2. This can be explained by the fact that $a_x^y(b_x^y$ respectively) is less sensible w.r.t. y given x when $a(b)$ is close to 1 or 0. As a consequence, for scenario 2, deviating from the optimal strategy causes much more severe utility degradation than scenario 1. Another valuable information we can draw from the result is that appropriately configuring the defense system (e.g., setting x, y) is so important that a bad configuration not only is a waste of resource, but causes significant security damage to the system. This result confirms our remark of Theorem 5.3.

We then study the impact of lack of monitor resource on the network security. The following two cases are simulated: 1). There are N_{min} defenders operating at $\mathbf{q}^*$; 2). There are $N_{min} - 1$ defenders choosing random monitor strategies. 300 random strategies are simulated for this case. In case 2, we set $x = y = 1$ for scenario 1 and $x \leq 2$, $y = 1$ for scenario 2: i.e., for scenario 1, each target is monitored by at most 1 defender at a time; for scenario 2, each target may be monitored by 1 or 2 defenders simultaneously with detection threshold set to 1. This is a reasonable setting noticing the resource and the performance parameters of the scenarios. In both cases, the attacker side chooses its strategy that maximizes its payoff and the attack resource P is set to 10. Table 5.6 shows the payoff degradation due to the lack of sufficient monitor resource.

	Scenario 1	Scenario 2
U_D^1	-0.0045	-1.24
$(U_D^2)_{max}$	-0.37	-2.98
$\overline{U_D^2}$	-1.3	-16.85

Table 5.6: Payoff degradation due to resource constraint

In Table 5.6, U_D^1 denotes the payoff of the defender side at the NE, $(U_D^2)_{max}$ and $\overline{U_D^2}$ denote the maximum and average payoff of the defender side choosing the simulated random strategies. The results show that lack of monitor resource degrades significantly the system security. This degradation becomes more severe if the attacker side disposes more attack resource. This can be seen comparing the numerical results in Table 5.6 ($P = 10$) and Table 5.4 ($P = 1$). Therefore, sufficient resource and appropriate configuration at the defender side are two necessary conditions of efficiently protecting the network from being attacked, which confirms the guideline 3 and 4 in the analytical model.

5.9 Conclusion

This chapter addresses the intrusion detection problem in heterogenous networks consisting of nodes with different security assets. We formulated the interaction between the attacks and the defenders as a non-cooperative game and performed an in-depth analysis on the NE and the engineering implications behind. Based on our game theoretic analysis, we derived expected behaviors of rational attackers. We showed that sufficient monitor resource and appropriate configuration at the defender side are two necessary conditions of efficiently protecting the network. We then derived the minimum monitor resource requirement and the optimal strategy of the defender side to achieve system optimality. We also provide two case studies to show how our game theoretic

framework can be applied to configure the intrusion detection strategies in realistic scenarios.

5.10 Proofs

This section completes the detailed proofs omitted from the main text.

5.10.1 Proof of Lemma 5.1

The proof consists of first showing that $\mathcal{T}_\mathcal{S}$ is composed of n targets with largest security assets and then proving $n = N_A$ by showing that neither $n < N_A$ nor $n > N_A$ is possible. It follows obviously that $\mathcal{T}_\mathcal{Q}$ is also uniquely determined.

Here we prove Case 2 of the lemma because Case 1 holds straightforwardly. It is obvious that N_A targets with the largest security assets satisfying (5.2) consists of a sensible target set $\mathcal{T}_\mathcal{S}$ in that (5.1) holds in such case. We then need to prove that $\mathcal{T}_\mathcal{S}$ is unique.

We first show that if $i \in \mathcal{T}_\mathcal{S}$, then $\forall j < i$ $(W_j \geq W_i)$, it holds that $j \in \mathcal{T}_\mathcal{S}$, if not, there exists $j_0 < i$ $(W_{j_0} \geq W_i)$ such that $j_0 \in \mathcal{T} - \mathcal{T}_\mathcal{S}$. It follows that $W_{j_0} \leq \dfrac{|\mathcal{T}_\mathcal{S}| \cdot (1 - C_a) - 2aQ}{(1 - C_a) \sum_{k \in \mathcal{T}_\mathcal{S}} \frac{1}{W_k}}$. On the other hand, from Definition 5.3, we have $W_i > \dfrac{|\mathcal{T}_\mathcal{S}| \cdot (1 - C_a) - 2aQ}{(1 - C_a) \sum_{k \in \mathcal{T}_\mathcal{S}} \frac{1}{W_k}}$. It follows that $W_i > W_{j_0}$, which contradicts with $W_{j_0} \geq W_i$. Hence $\mathcal{T}_\mathcal{S}$ is composed of n targets with largest security assets.

We then prove $n = N_A$ by showing that it is impossible that $n < N_A$ or $n > N_A$. If $n < N_A$, from (5.2), we have

$$
\begin{aligned}
W_{N_A} > \frac{N_A \cdot (1 - C_a) - 2aQ}{(1 - C_a) \sum_{j=1}^{N_A} \frac{1}{W_j}} \quad &\Longrightarrow \quad W_{N_A} (\sum_{j=1}^{N_A} \frac{1}{W_j}) > \frac{N_A \cdot (1 - C_a) - 2aQ}{1 - C_a} = N_A - \frac{2aQ}{1 - C_a} \\
&\Longrightarrow \quad W_{N_A} (\sum_{j=1}^{N_A} \frac{1}{W_j}) - (N_A - n) > n - \frac{2aQ}{1 - C_a}
\end{aligned}
$$

Noticing $W_{N_A} \leq W_i, \forall i \leq N_A$ and $n < N_A$ (i.e. $W_{n+1} \geq W_{N_A}$), we have

$$
\begin{aligned}
W_{n+1} (\sum_{j=1}^{n} \frac{1}{W_j}) \quad &\geq \quad W_{N_A} (\sum_{j=1}^{n} \frac{1}{W_j}) = W_{N_A} (\sum_{j=1}^{N_A} \frac{1}{W_j}) - W_{N_A} (\sum_{j=n+1}^{N_A} \frac{1}{W_j}) \\
&\geq \quad W_{N_A} (\sum_{j=1}^{N_A} \frac{1}{W_j}) - (N_A - n) > n - \frac{2aQ}{1 - C_a}
\end{aligned}
$$

Hence $W_{n+1} > \dfrac{n \cdot (1 - C_a) - 2aQ}{(1 - C_a) \sum_{j=1}^{n} \frac{1}{W_j}}$. On the other hand, from Definition 5.3, we have $W_{n+1} \leq \dfrac{n \cdot (1 - C_a) - 2aQ}{(1 - C_a) \sum_{j=1}^{n} \frac{1}{W_j}}$. This contradiction shows that it is impossible that $n < N_A$. Similarly we can show that it is impossible that $n > N_A$. Hence, $n = N_A$ is uniquely determined, so is $\mathcal{T}_\mathcal{S}$. It follows obviously that $\mathcal{T}_\mathcal{Q}$ is also uniquely determined. This concludes our proof.

5.10.2 Proof of Theorem 5.1

The proof consists of showing that regardless of the defender's strategy $\mathbf{q}$, for any $\mathbf{p} \in A_A$ such that $\exists i \in \mathcal{T} - \mathcal{T}_\mathcal{S} - \mathcal{T}_\mathcal{Q},\ p_i > 0$, we can construct another strategy $\mathbf{p}'$ such that $p'_i = 0,\ \forall i \in \mathcal{T} - \mathcal{T}_\mathcal{S} - \mathcal{T}_\mathcal{Q}$ and $U_A(\mathbf{p}, \mathbf{q}) < U_A(\mathbf{p}', \mathbf{q})$.

If $W_N \geq \dfrac{N_A \cdot (1 - C_a) - 2aQ}{(1 - C_a) \sum_{j=1}^{N_A} \frac{1}{W_j}}$, $\mathcal{T} - \mathcal{T}_\mathcal{S} - \mathcal{T}_\mathcal{Q} = \emptyset$, the theorem holds evidently. We now prove the case where $W_N < \dfrac{N_A \cdot (1 - C_a) - 2aQ}{(1 - C_a) \sum_{j=1}^{N_A} \frac{1}{W_j}}$, in other words, $\mathcal{T} - \mathcal{T}_\mathcal{S} - \mathcal{T}_\mathcal{Q} \neq \emptyset$.

Consider a vector $\mathbf{q^0} = (q_1^0, q_2^0, \cdots, q_N^0)$ where

$$q_i^0 = \begin{cases} \dfrac{1}{2a}\left(1 - C_a - \dfrac{N_A \cdot (1 - C_a) - 2aQ}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}}\right) & i \in \mathcal{T}_\mathcal{S} \\ 0 & i \in \mathcal{T} - \mathcal{T}_\mathcal{S} \end{cases}$$

It holds that $q_i^0 \geq 0$ and $\sum_{i=1}^{N_A} q_i^0 = Q$. Let $\mathbf{q} = (q_1, q_2, \cdots, q_N)$ denote the monitor probability distribution of the defender, by the Pigeon Hole Principle, it holds that $\sum_{i=1}^{N_A} q_i \leq Q$, thus $\exists m \in \mathcal{T}_\mathcal{S}$ such that $q_m \leq q_m^0$.

We now consider any attacker strategy $\mathbf{p} = (p_1, p_2, \cdots, p_N) \in A_A$ satisfying $\sum_{i \in \mathcal{T} - \mathcal{T}_\mathcal{S} - \mathcal{T}_\mathcal{Q}} p_i > 0$, i.e., the attacker attack at least one target outside the sensible target set with non-zero probability. We construct another attacker strategy profile $\mathbf{p}'$ based on $\mathbf{p}$ such that

$$p'_i = \begin{cases} p_i & i \in \mathcal{T}_\mathcal{S} \text{ and } i \neq m \\ p_m + \sum_{j \in \mathcal{T} - \mathcal{T}_\mathcal{S} - \mathcal{T}_\mathcal{Q}} p_j & i = m \\ p_i & i \in \mathcal{T}_\mathcal{Q} \\ 0 & i \in \mathcal{T} - \mathcal{T}_\mathcal{S} - \mathcal{T}_\mathcal{Q} \end{cases}$$

By comparing the attacker's payoff at $\mathbf{p}$ and $\mathbf{p}'$, noticing that $W_i < \dfrac{N_A \cdot (1 - C_a) - 2aQ}{(1 - C_a) \sum_{j=1}^{N_A} \frac{1}{W_j}}, \forall i \in$

$\mathcal{T} - \mathcal{T}_\mathcal{S} - \mathcal{T}_\mathcal{Q}$, we obtain:

$$
\begin{aligned}
& U_A(\mathbf{p}) - U_A(\mathbf{p}') = \sum_{i\in\mathcal{T}} p_i W_i(1-2aq_i - C_a) - \sum_{i\in\mathcal{T}} p_i' W_i(1-2aq_i - C_a) \\
= & \sum_{i\in\mathcal{T}} p_i W_i(1-2aq_i - C_a) - \Big(\sum_{i\in\mathcal{T}_\mathcal{S}+\mathcal{T}_\mathcal{Q}, i\neq m} p_i W_i(1-2aq_i - C_a) + \left(p_m + \sum_{i\in\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}} p_i \right) W_m(1-2aq_m - C_a) \Big) \\
= & \sum_{i\in\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}} p_i W_i(1-2aq_i - C_a) - \sum_{i\in\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}} p_i W_m(1-2aq_m - C_a) \\
\leq & \sum_{i\in\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}} p_i W_i(1-2aq_i - C_a) - \sum_{i\in\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}} p_i W_m(1-2aq_m^0 - C_a) \\
= & \sum_{i\in\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}} p_i W_i(1-2aq_i - C_a) - \sum_{i\in\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}} p_i \frac{N_A\cdot(1-C_a) - 2aQ}{\sum_{j=1}^{N_A}(1-C_a)\frac{1}{W_j}} \\
\leq & \sum_{i\in\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}} p_i W_i - \sum_{i\in\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}} p_i \frac{N_A\cdot(1-C_a) - 2aQ}{\sum_{j=1}^{N_A}(1-C_a)\frac{1}{W_j}} \\
= & \sum_{i\in\mathcal{T}-\mathcal{T}_\mathcal{S}-\mathcal{T}_\mathcal{Q}} p_i \left(W_i - \frac{N_A\cdot(1-C_a) - 2aQ}{\sum_{j=1}^{N_A}(1-C_a)\frac{1}{W_j}} \right) < 0
\end{aligned}
$$

Hence, operating at $\mathbf{p}'$ gives the attacker more payoff than operating at $\mathbf{p}$. As a result, a rational attacker has no incentive to choose $\mathbf{p}$ compared with $\mathbf{p}'$.

5.10.3 Proof Sketch of Corollary 5.1

It follows from $\sum_{i\in\mathcal{T}} q_i^* = Q$ and $\mathbf{q}' \neq \mathbf{q}^*$ that $\exists m \in T_S$ such that $q_m' < q_m^*$. We can solve $\widehat{\mathbf{p}}$ as

$$
\widehat{p}_i \begin{cases} \in [0,P] & i \in \mathcal{T}_\mathcal{M} \\ = 0 & i \in \mathcal{T} - \mathcal{T}_\mathcal{M} \end{cases}
$$

where $\mathcal{T}_\mathcal{M}$ consists of target i such that $(1-2aq_i' - C_a)W_i$ is maximized, $\sum_{i\in\mathcal{T}_\mathcal{M}} \widehat{p}_i = P$. It follows immediately that $q_i' < q_i^*, \forall i \in \mathcal{T}_\mathcal{M}$. Noticing the defender's utility function U_D, we have $U_D(\widehat{\mathbf{p}}, \mathbf{q}^*) > U_D(\widehat{\mathbf{p}}, \mathbf{q}')$.

Moreover, following the definition of NE, we have $U_D(\mathbf{p}^*, \mathbf{q}^*) \geq U_D(\widehat{\mathbf{p}}, \mathbf{q}^*)$. It follows that $U_D(\mathbf{p}^*, \mathbf{q}^*) > U_D(\widehat{\mathbf{p}}, \mathbf{q}')$. Symmetrically, we can prove that $U_A(\mathbf{p}^*, \mathbf{q}^*) > U_A(\mathbf{p}', \widehat{\mathbf{q}})$.

Chapter 6

A Defense Strategy against Jamming Attack in Wireless Networks

6.1 Introduction

It is widely recognized that the broadcast nature of the shared wireless medium makes wireless networks extremely vulnerable to various attacks ranging from the passive eavesdropping to the sophisticated manipulation of routing information, among which an easily mountable one with detrimental effects on the victim network is jamming, alternatively termed Denial-of-Service (DoS). Jamming is a malicious attack whose objective is to disrupt the communication of the victim network by intentionally causing interference or collision at the receiver side. Usually launched at the PHY and MAC layers, jamming requires no special hardware and can virtually paralyze any wireless networks. [XTZW05] provides a taxonomy of different types of jamming in wireless networks.

The defense strategies in existing literature mainly consist of retreating from the jammer after detecting jamming or rerouting traffic around the jammed area. In [XWTZ04], Xu *et al.* propose two strategies to evade jamming. The first strategy, channel surfing, is a form of spectral evasion that involves legitimate wireless devices changing the channel that they are operating on. The second strategy, spatial retreats, is a form of spatial evasion whereby legitimate devices move away from the jammer. In [WSS03], Wood *et al.* present a distributed protocol to map the jammed region so that the network can avoid routing traffic through it. The solution proposed by Cagalj *et al.* [CCH07] uses different wormholes (wired wormholes, frequency-hopping pairs, and uncoordinated channel hopping) that lead out of the jammed region to report the alarm to the network operator. In [WSZ07], Wood *et al.* investigate how to deliberately avoid jamming in IEEE 802.15.4-based wireless networks.

Despite the different techniques used in existing solutions, they usually require frequency hopping capability or sufficient node mobility to avoid confronting the jammer. Such requirements might be too expensive to implement or even impractical in some scenarios, e.g., single-channel WLANs. Moreover, their effectiveness may be significantly reduced if the jammer is strategic, e.g., mapping the jammed area becomes more difficult if the jammer keeps moving in an unpredictable fashion.

In this chapter, we tackle the problem of defeating jamming from a different angle. Our work is motivated by the observation that although a jamming packet of a few bits suffices to disrupt

a transmitted packet, as argued in [LN05], yet continuously transmitting the jamming packets is energy-consuming and may quickly drain the energy of the jammer with limited battery supply. In other words, a jammer with limited energy resource can never succeed jamming the victim network for any extended period of time. This is especially the case where the jammer is restricted to a configuration similar to that of ordinary network nodes with limited energy resource such as laptops. Given the above argument, an alternative defense strategy against jamming besides passively retreating, especially when it is impossible to move away from the jammer, is to actively fight the jammer face-to-face by draining its energy as fast as possible.

Following the above line of defense, we proceed our analysis as follows. Firstly, we formulate jamming as an optimization problem for the jammer whose goal is to block the communication of the victim network as long time as possible under its energy constraint. To this end, it controls the probability of transmitting jamming packets to strike a balance between keeping a high jamming probability and limiting the energy consumption. On the network side, each node adapts its channel access probability to maximize its utility under the jamming attack. We model the interaction between the jammer and the network as a non-cooperative game G. We show that G has two Nash equilibria (NE) and at one of them, the jammer can paralyze the network with little energy consumption. To avoid this inefficient NE for the network, we propose our defense strategy by introducing the anti-jammer, a special node dedicated to draining the jammer's energy. To achieve its goal, the anti-jammer configures the probability of transmitting bait packets to attract the jammer to transmit. We then formulate the new jamming game G' with the anti-jammer and show that G' admits a unique NE where if the anti-jammer chooses its strategy wisely, the network utility remains the same as that in G, but the jammer's energy consumption increases significantly. Next, we extend our efforts to investigate the dynamics of G' by developing the update mechanisms in which the anti-jammer and network nodes adjust their transmission strategies based on only observable channel information.

Recently, applying game theory in different areas of wireless communication has attracted considerable research attention. Concerning jamming, Mallik *et al.* [MSP00] model the problem of a victim node and a jammer transmitting to a common receiver in an on-off mode as a two-person zero-sum noncooperative dynamic game. Structures of steady-state solutions to the game are then investigated. Sagduyu *et al.* [SE07] model DoS attacks as stochastic games among non-cooperative selfish nodes that randomly transmit packets to a common receiver and malicious nodes with the dual objectives of blocking the packet transmissions of the other selfish nodes as well as optimizing their individual performance. The resulting equilibria are analyzed and the network performance is compared with the cooperative equilibrium. In [LKP07], Li *et al.* formulate the jamming attack as optimization problem as well as max-min problem and derive the optimal attacking strategy for the jammer to maximize the duration before being detected and the optimal defense strategy for the defender to alleviate the attack damage.

Compared with existing work, the focus of our work is not only to alleviate the damage caused by the jammer, but also to fight the jammer actively by draining its energy as quickly as possible. The main contributions of our work can be summarized as follows:

- *Game theoretic framework:* We establish a game theoretic model between the victim network and the energy-limited jammer and derive resulting equilibria.

- *Active defense strategy:* We propose an active defense strategy against jamming and demon-

strate its benefits via both mathematical analysis and numerical experiment.

- *Distributed strategy update mechanism:* We derive distributed update mechanisms in which the anti-jammer and network nodes adjust their strategies based on observable channel information.

The rest of this chapter is organized as follows. Section 6.2 introduces the network model and discusses the assumptions made in our work. Section 6.3 formulates the jamming game and derives the resulting NEs. Section 6.4 presents and analyzes our defense strategy. Section 6.5 and 6.6 focus on the distributed update mechanisms and the implementation issues. Section 6.7 presents a numerical study to evaluate the performance of the proposed defense strategy. Finally, the chapter is concluded in Section 6.8.

6.2 Network Model and Problem Formulation

We consider a single-hop wireless network consisting of a set $\mathcal{N} = \{1,\ 2,\ \cdots,\ n\}$ $(n > 1)$ of nodes operating on the following generalized version of the slotted-Aloha protocol to access the shared wireless medium: Time is divided into synchronized slots. Each node can send one packet in a slot. If a node has a packet to send, it transmits during the next slot with probability p called channel access probability. Since the above generalized slotted-Aloha scheme is the root of various medium access control protocols widely used nowadays, basing our analysis on it makes our results a generic framework easily extensible to other protocols.

In our study, we focus on the extreme case where all network nodes are continuously backlogged, i.e., they always have packets to transmit. The transmission is successful if there is no collision with other transmissions.

As discussed in Introduction, jamming is a DoS attack at the PHY/MAC layer whose goal is to disable the communication of the victim network by intentionally causing collisions. To mount such attack, the jammer senses the wireless channel and transmits a jamming packet colliding with legitimately transmitted packets if the channel is not free. In this chapter, we focus on energy-limited strategic jammer aiming at keeping the communication of the victim network blocked as long time as possible under its energy budget. To this end, it configures the probability of transmitting jamming packets to strike a balance between keeping a high jamming probability and limiting the energy consumption. Mathematically, the jammer's strategy is modeled by the following optimization problem $\mathbf{P_J}$

$$\mathbf{P_J}: \qquad \max_{0\leq\theta\leq 1} \quad T_J \quad \text{s.t.} \quad S \leq S_0,$$

where θ denotes the jammer's strategy, i.e., the probability of transmitting jamming packets, T_J denotes the expected time during which the communication of the victim network is blocked by the jammer, S denotes the throughput of the victim network, S_0 denotes the threshold of effective jamming from the jammer's perspective, i.e., to block the communication of the victim network, it has to limit S not to exceed S_0.

Let p denote the channel access probability of the network nodes, the network throughput can be expressed as $S = np(1-p)^{n-1}(1-\theta)$. $\mathbf{P_J}$ can thus be translated to the following optimization

problem $\mathbf{P'_J}$:

$$\begin{aligned} \min_{0\leq\theta\leq 1} \quad & U_J = [1-(1-p)^n]\theta \\ \text{s.t.} \quad & np(1-p)^{n-1}(1-\theta) \leq S_0. \end{aligned}$$

U_J can be seen as the expected energy consumption of the jammer per slot, given that the energy of transmitting one jamming packet is normalized to 1. As mathematically characterized by $\mathbf{P'_J}$, a strategic jammer searches to block the victim network while minimizing its energy consumption.

At the victim network side, it reacts strategically to operate the most efficiently possible under jamming. Specifically, the network nodes adapt their channel access probability p to maximize the utility function U_N that reflects the difference between the throughput reward and the transmission cost, i.e.,

$$U_N = np(1-p)^{n-1}(1-\theta) - npc,$$

where the throughput reward is normalized to 1 and $c \leq 1$ denotes the transmission cost. To simplify our study, we assume that the transmission cost is the same for all packets. Moreover, throughout this chapter, to avoid the trivial case where the jammer has no incentive to launch jamming attack, we impose the following assumption on S_0:

$$S_0 < n\widehat{p}(1-\widehat{p})^{n-1}, \tag{6.1}$$

where $\widehat{p} = \text{argmax}_{0\leq p\leq 1}\, np(1-p)^{n-1} - npc$. Generally, for the jamming to be effective, S_0 should be sufficiently small. The smaller S_0 is, the more effective the jamming is (also the more aggressive the jammer is). In this chapter, we are especially interested in the aggressive case with small S_0.

To concentrate on the essential properties of jamming and the proposed defense strategy, we limit our study to jamming at PHY/MAC layers. The jammer does not interpret the semantics of the packets to determine which packet to jam. Interested readers are referred to [LN05] for such intelligent jamming attacks in IEEE 802.11 DCF, which are out of the scope of this chapter. Despite some simplifications made in our model, the analysis of the jamming attacks and the derived defense strategy are far from trivial and indeed provide valuable insight on the topic, as shown in the reminder of the chapter.

6.3 Jamming Game Analysis

We model the interactions between the jammer and the victim network as a non-cooperative jamming game G, defined as follows

Definition 6.1. *The non-cooperative jamming game G is a 3-tuple $(\mathcal{P}, \mathcal{A}, \mathcal{U})$, where $\mathcal{P} = \{\mathcal{J}, \mathcal{N}\}$ denotes the player set consisting of the jammer $\mathcal{J}$ and the victim network $\mathcal{N}$, $\mathcal{A} = [0,1] \times [0,1]$ denotes the strategy space, $\mathcal{U} = \{U_N, U_J\}$ denotes the utility function set. The player $\mathcal{J}$ ($\mathcal{N}$) selects its strategy θ (p) to minimize (maximize) its utility U_J (U_N).*

The solution of the jamming game G is characterized by one or more Nash equilibrium (NE), a strategy profile from which no player has incentive to deviate unilaterally. Formally, if (p^*, θ^*) is

a NE of G, it holds that

$$\begin{cases} U_N(p^*, \theta^*) \geq U_N(p', \theta^*) & \forall 0 \leq p' \leq 1 \\ U_J(p^*, \theta^*) \leq U_J(p^*, \theta') & \forall 0 \leq \theta' \leq 1 \end{cases}.$$

Our focus in this section is to derive and analyze the resulting NE of G.

Theorem 6.1. *Let* $k \triangleq \frac{S_0}{c}$ *and* $A(k) \triangleq \sqrt{(1+k)^2 - \frac{4}{n}k}$, *the jamming game* G *admits two NEs:* $p_1^* = 0$, $\theta_1^* = 1$ *and* $p_2^* = \frac{1+k-A(k)}{2}$, $\theta_2^* = 1 - \frac{2^n S_0}{n(1+k-A(k))(1-k+A(k))^{n-1}}$.

Proof. Please refer to Section 6.9.1 for the detailed proof. □

As an important implication of Theorem 6.1, the network is paralyzed ($S = 0$) at the border NE where the jammer adopts the most aggressive strategy by setting θ^* to 1 and the network nodes keep silent.

In contrast to the common sense that the jamming attack is usually very energy consuming, Theorem 6.1 shows that the jamming attack is very cost-effective at the border NE. This is due to the fact that any rational node in the victim network, aware of the existence of the jammer, will not attempt to send any packet, which brings no gain but a waste of energy. Take the IEEE 802.11 WLAN as an example, the rationality of nodes leads to doubling the value of the contention window (CW) after each collision. In such context, the jammer makes the network node repeatedly double the CW value until finally the transmission attempt is given up, which corresponds to the border NE in Theorem 6.1. Consequently, the jammer can disrupt the communication of the victim network with little energy consumption.

6.4 Proposed Jamming Defense Strategy

Motivated by the analytical results of previous section, especially the detrimental damage caused by the jammer at the border NE, we propose our jamming defense strategy in this section. Different form existing solutions that retreat from the jammed area or switch to other channels to avoid being jammed, our approach tackles the problem from a new angle, which is inspired from the following philosophy:

The best defense is an offense.

Applying the above philosophy in our context, we propose our jamming defense strategy consisting of actively fighting the jammer face-to-face by draining its energy as fast as possible. The task of fighting against the jammer is designated to a special network entity referred to as *anti-jammer*. Several practical implementations are possible: e.g., the anti-jammer can be a network node disposing a large amount of energy; or, the role of the anti-jammer can be assigned to all network participants in a distributed way, i.e., each node serves as the anti-jammer for a certain period of time for the interests of the whole network. With the goal of draining the jammer's energy, the anti-jammer transmits a bait packet indistinguishable from legitimate packets at probability q at each slot to attract the jammer to emit the jamming packet.

In the sequel, we formulate the new jamming game G' with the anti-jammer and characterize the resulting NE. The central questions we pose in order to study the performance of the proposed defense strategy are: 1). Does there exist NE in G'? 2). If so, is it unique and can players converge

to the equilibrium? 3). How does the NE compare with the NEs in Theorem 6.1? Is it more desirable for the network?

6.4.1 Jamming Game with Anti-jammer

In this subsection, we study the jamming game G' consisting of the victim network of n nodes, a jammer and an anti-jammer. The network model is the same as in G, the only difference is that the anti-jammer is introduced operating on q to fight against the jammer. In this new context, the network throughput becomes $S = np(1-p)^{n-1}(1-q)(1-\theta)$. The utility function of the network can be written as:

$$U_N = np(1-p)^{n-1}(1-q)(1-\theta) - npc.$$

The jammer's optimization problem $\mathbf{P'_J}$ becomes

$$\begin{aligned} \min_{0\le\theta\le 1} \quad & U_J = [1-(1-p)^n(1-q)]\theta \\ \text{s.t.} \quad & np(1-p)^{n-1}(1-q)(1-\theta) \le S_0. \end{aligned}$$

The following theorem establishes the NE of G'.

Theorem 6.2. *If $q > 0$, G' admits a unique NE (p^*, θ^*).*

1. If the following condition holds

$$n(1-q)(1+k-A(k))(1-k+A(k))^{n-1} > 2^n S_0, \tag{6.2}$$

$$\begin{cases} p^* = \dfrac{1+k-A(k)}{2} \\ \theta^* = 1 - \dfrac{2^n S_0}{n(1-q)(1+k-A(k))(1-k+A(k))^{n-1}} \end{cases} \tag{6.3}$$

2. If the condition (6.2) *does not hold,*

$$\begin{cases} p^* = \underset{p}{\operatorname{argmax}} \quad (1-q)p(1-p)^{n-1} - cp \\ \theta^* = 0 \end{cases} \tag{6.4}$$

Proof. Please refer to Section 6.9.2 for the detailed proof. □

Theorem 6.2 establishes the existence and uniqueness of the NE and quantifies the relation between different parameters (S_0, c and q) and the resulting NE. Theorem 6.2 implies that by properly setting q, the border NE in Theorem 6.1 where the jammer can paralyze the network with little energy consumption can be eliminated in G' and the game reaches a more desirable NE (6.3) from the network's perspective. In this regard, the anti-jammer plays the role of refining NE by eliminating the undesirable equilibrium.

In the following corollary, we provide a simplified necessary condition on q to ensure that the unique NE is the non-border NE derived in (6.3).

Corollary 6.1. *G admits a unique non-border NE (p^*, θ^*) given by (6.3) if the following sufficient condition holds:*

$$\frac{(1-q)k}{1+k}\left[1-\frac{k}{n(1+k)}\right]^{n-1} > S_0$$

Proof. Please refer to Section 6.9.3 for the detailed proof. □

Corollary 6.1 provides a guideline for the anti-jammer on how to choose its strategy q to avoid the less desirable NE. In the asymptotic scenario where $n \gg 1$, noticing that $k = S_0/c$, after some mathematical arrangement, the sufficient condition in Corollary 6.1 can be further simplified to $q < 1 - (S_0 + c)e^{\frac{k}{1+k}}$.

6.4.2 NE Analysis: Comparison with G

After solving the NE of G', it is natural and interesting to compare the non-border NE of G' given in (6.3) with the non-border NE of G derived in (6.13). As can be seen from (6.13) and (6.3), the network utility U_N is the same at the two non-border NEs. In the following theorem, we investigate the jammer's utility U_J at the non-border NE of G and G'.

Theorem 6.3. *By wisely choosing q, the anti-jammer can increase the jammer's energy consumption at the non-border NE if and only if the following condition holds:*

$$S_0 < np^*(1-p^*)^{2n-1}, \tag{6.5}$$

where $p^* = \dfrac{1+k-A(k)}{2}$.

Proof. Please refer to Section 6.9.4 for the detailed proof. □

In the following corollary, we provide a simplified sufficient condition under which the result of Theorem 6.3 holds.

Corollary 6.2. *If $S_0 + c < \left(1-\dfrac{1}{n}\right)^{2n-1}$, or when $n \gg 1$, if $S_0 + c < 1/e^2$, then the anti-jammer can increase the jammer's utility at the NE by wisely choosing q.*

Proof. Please refer to Section 6.9.5 for the detailed proof. □

As a summary of previous analysis, we have demonstrated via Theorem 6.2 and 6.3 the following benefits of the proposed defense strategy. Theorem 6.2 states that if q is properly chosen, the jamming game admits a unique non-border NE given in (6.3). Compared with the non-border NE in G without anti-jammer, the network gets the same payoff at the non-border NE in G'. Theorem 6.3 further shows that under the condition (6.5), the jammer consumes more energy. In this perspective, our solution not only can eliminate the undesirable NE (the border NE in G), but also can increase the jammer's energy consumption at the remaining NE. As a result, under the condition of (6.5) which is especially true for aggressive jammer, our solution can force the jammer to spend its energy more quickly without degrading the network performance.

Theorem 6.3 quantifies the condition under which $U_J^G \geq U_J^{G'}$. Next we provide a qualitative explication on the implication behind. The goal of introducing the anti-jammer is to increase the jammer's energy consumption without degrading the network performance. From another angle, the anti-jammer can be regarded as a jammer that jams the traffic of both the network and the

jammer, the latter being our objective while the former the side effect. When the condition (6.5) is met, i.e., $S_0 + c$ is sufficiently small, the cost of jamming the network traffic is less than the gain of jamming the jammer. In contrast, if the condition is not met, the benefit of introducing the anti-jammer is counter-balanced by its side effect, i.e., the anti-jammer actually helps the jammer jam the network. In this sense, introducing the anti-jammer to counter jamming is like using a "double-bladed sword" which brings both benefit and side effect. Therefore, the strategy of the anti-jammer q should be carefully chosen so as to strike a balance between maximizing the benefit and limiting the side effect.

In the following subsection, we seek the optimal value of q that achieves the above balance.

6.4.3 Choosing Optimal Value of q

In this subsection, we solve the optimal value of q that maximizes the jammer's energy consumption at the non-border NE under the condition (6.5).

Theorem 6.4. *Under the condition* (6.5)*, the optimal strategy for the anti-jammer is* $q^* = 1 - \sqrt{\frac{S_0}{np^*(1-p^*)^{2n-1}}}$.

Proof. Please refer to Section 6.9.6 for the detailed proof. □

6.4.4 Further Discussion and Limitation of Proposed Strategy

It is insightful to note that the interactions among the network, the jammer and the anti-jammer can be modeled by a Stackelberg game, in which the anti-jammer is the leader, the network and the jammer are the followers. The followers choose their strategies p and θ to maximize and minimize their utility function U_N and U_J based on the leader's strategy q. The leader chooses its strategy q to maximize its utility function (i.e., the jammer's energy consumption), taking into account that the followers will subsequently choose their strategy to greedily maximize/minimize their own payoff. Apply our analysis in this section, the Stackelberg game admits a unique equilibrium (q^*, p^*, θ^*) under the condition (6.5).

We conclude this section by discussing the limitations of the proposed defense strategy. Firstly, our solution aims at draining the jammer's energy rather than coping with jamming. As a result, although the jammer consumes more energy to mount the jamming attack, yet the communication of the victim network is disrupted as long as the jammer does not use up its battery. Secondly, as discussed in the beginning of Section 6.4, the role of anti-jammer can be designated to the network node disposing a large amount of energy or to all network participants in a distributed way. In this regard, the altruism of the anti-jammer is implicitly assumed. However, this assumption is not always valid, especially in open environments where network participants are selfish and have no incentive to spend their own energy for the interests of the common, including themselves. In such cases, incentive mechanisms are needed to avoid the above common dilemma. Thirdly, as shown in Theorem 6.2 and 6.3 as well as the numerical experiments presented later, the proposed solution is less effective when the jammer acts more mildly by operating on large S_0. It is insightful to note that in such cases, the attack is no more a jamming attack in the strict sense in that the jammer's goal is not to block the network communication as that of pure jamming with S_0 sufficiently small, but rather to limit the network throughput with a mild threshold S_0.

6.5 Game Dynamics and Distributed Strategy Update Mechanism

In the previous section, we have studied some structural properties of the NE in the jamming game with the anti-jammer and demonstrated the benefits of the proposed defense strategy. In this section, we extend our efforts to study the game dynamics. More specifically, we develop distributed strategy update mechanisms for players to adjust their strategies to converge to the equilibrium based on only observable channel information.

We start with the victim network. Noticing that the objective of the network nodes is to maximize the global network utility under jamming, we propose a distributed update mechanism of the channel access probability, as shown in the following:

$$p_i(t+1) = \left[p_i(t) + \lambda\Big((1-q)(1-\theta)(1-np_i(t)) \prod_{j\in\mathcal{N}, j\neq i} (1-p_j(t)) - (1-p_i(t))c \Big) \right]_0^{p_{max}}. \quad (6.6)$$

where $\big[x\big]_a^b$ denotes $\max\{a, \min\{b, x\}\}$, λ is the step size, $p_{max} \in (0,1)$ is the system parameter.

Theorem 6.5. *Under the condition* (6.5)*, if* $\frac{(1-q)(1-\theta)(1-np_{max})}{1-p_{max}} < c < (1-q)(1-\theta)(1-p_{max})^{n-1}$*, the update scheme* (6.6) *has a unique fixed point, which is also the optimal point where the global network utility is maximized.*

Proof. The proof, detailed in appendix, consists of two steps: we first show that any border point cannot be a fixed point of (6.6); we then focus on the non-border fixed point and prove that $\{\widetilde{p}\}$ is the only non-border fixed point of (6.6), where $\widetilde{p}$ is the root of

$$(1-q)(1-\theta)(1-p)^{n-2}(1-np) = c.$$

It is easy to see that $\{\widetilde{p}\}$ is also the optimal point where the global network utility is maximized. □

Remark: (6.6) can be seen as a subgradient strategy update scheme that gradually approaches the fixed point, which corresponds to the global optima.

We then analyze the jammer's strategy. Noticing that the jammer's utility is to minimize its energy consumption while limiting the network throughput $S \leq S_0$, its best strategy at iteration $t+1$ $\theta(t+1)$ can be derived by

$$S_0 = \big[1-\theta(t+1)\big](1-q) \sum_{i\in\mathcal{N}} p_i(t) \prod_{j\in\mathcal{N}, j\neq i} (1-p_j(t)).$$

However, in practice, since the jammer cannot distinguish the traffic of the anti-jammer and that of an ordinary node, it is impossible to compute $\theta(t+1)$ from the above equation. We thus consider in our study a more practical update scheme for the jammer in which it chooses the smallest θ such that the aggregated throughput including the anti-jammer's traffic is no more than αS_0, where $\alpha \geq 1$ is a tolerant factor, i.e.,

$$\Big[1-\theta(t+1)\Big]\Big[(1-q)\sum_{i\in\mathcal{N}} p_i(t) \prod_{j\in\mathcal{N}, j\neq i} (1-p_j(t)) + q\prod_{j\in\mathcal{N}}(1-p_j(t))\Big] \leq \alpha S_0.$$

$\alpha = 1$ corresponds to the scenario in which the jammer is not aware of the existence of the anti-jammer or it wants to limit the network throughput regardless of the anti-jammer's strategy q. This update scheme can be formally expressed as:

$$\theta(t+1) = \left[1 - \frac{\alpha S_0}{(1-q)\sum_{i\in\mathcal{N}} p_i(t)\prod_{j\in\mathcal{N},j\neq i}(1-p_j(t)) + q\prod_{j\in\mathcal{N}}(1-p_j(t))}\right]_0^1. \tag{6.7}$$

In the following theorem, we analyze the equilibrium of G' under the update scheme (6.6) for the network nodes and (6.7) for the jammer.

Theorem 6.6. *The strategy update scheme in which the network nodes follow* (6.6) *and the jammer follows* (6.7) *admits a unique fixed point under the following condition:*

$$\begin{cases} \dfrac{\alpha S_0}{(1-p_{max})^n} < q \leq \dfrac{n}{n+1} \\ \dfrac{(n-1)p_{max}}{1-p_{max}} + \dfrac{q}{1-q} < \dfrac{\alpha S_0}{c} < \dfrac{p_{max}(1-p_{max})}{1-np_{max}} + \dfrac{(1-p_{max})^2}{1-np_{max}}\dfrac{q}{1-q} \end{cases}. \tag{6.8}$$

Specifically, the fixed point coincides with the non-border NE (p^*, θ^*) *derived in* (6.3) *if* $\alpha S_0 = (1-\theta^*)\left[q(1-p^*)^n + n(1-q)p^*(1-p^*)^{n-1}\right]$.

Proof. Please refer to Section 6.9.8 for detailed proof. □

Theorem 6.6 states that G' has a unique equilibrium under the update scheme (6.6) and (6.7). In Section 6.7, the game dynamics of G' (i.e., the convergence to the unique equilibrium) is further studied via simulation under the above update scheme.

We conclude this section by analyzing the anti-jammer's strategy q, which should be carefully tuned in order to achieve a balance between maximizing the benefit and limiting the side effect, as discussed in the end of Section 6.4.2. Noticing that calculating the optimal value of q requires the knowledge of α which is not available to the anti-jammer, we propose the following adaptive recursive search method to find the locally optimal value of q. We will evaluate the proposed method via simulation in Section 6.7.

1. Set $\Delta q, \varepsilon$ to some small values, T a sufficient long time for convergence. Initialize $q(0) = 0$. Set $n = 0$.

2. Set $n = n + 1$, wait time T for the players to converge, then estimate the jammer's utility $U_J(n)$.[1]

   (a) If $U_J(n) > U_J(n-1)$, set $q(n+1) = q(n) + \Delta q$.

   (b) If $U_J(n) < U_J(n-1)$, set $q(n+1) = q(n) - \Delta q$.

3. Stop until $|U_J(n) - U_J(n-1)| < \varepsilon U_J(n)$.

[1] How to estimate U_J is addressed in Section 6.6.

6.6 Implementation Issue

Previously, we have investigated the dynamics of G' and the distributed strategy update scheme for players to converge to the unique operating point. However, for the network nodes and anti-jammer, since they usually do not have access to the access probability of others, they cannot directly implement the discussed update scheme. In this section, we address this implementation issue, more specifically, how to estimate $(1-q)(1-\theta)\prod_{j\in\mathcal{N},j\neq i}(1-p_j)$ for node i to compute $p_i(t)$ based on (6.6) and how to estimate U_J for the anti-jammer to update q.

Our solution is based on the *Idle Sense* approach (see [HRGD05] for a detailed description) allowing a player to estimate the channel condition by observing the average number of consecutive idle slots between two transmission attempts. As a desirable property, our solution is based on only observable information and does not generate any additional message.

We start with the network nodes. Let $P_{idle} = (1-q)(1-\theta)\prod_{j\in\mathcal{N}}(1-p_j)$ be the probability of an idle slot and n_{idle} be the number of average consecutive idle slots between two transmission attempts, it holds that $n_{idle} = \frac{P_{idle}}{1-P_{idle}}$. It follows that

$$(1-q)(1-\theta)\prod_{j\in\mathcal{N},j\neq i}(1-p_j) = \frac{n_{idle}}{n_{idle}+1}\cdot\frac{1}{1-p_i}.$$

Since node i knows its own strategy $p_i(t)$ and can observe $n_{idle}(t)$, it can compute $p(t+1)$ based on (6.6).

We then turn to the anti-jammer who needs to estimate $U_J = [1-(1-p)^n(1-q)]\theta$, where p and θ is the converged value of $p_i(t), \forall i \in \mathcal{N}$ and $\theta(t)$. To this end, it estimates the network throughput as $S = \frac{N_s}{N_t}$, where N_s is the number of successful transmission on the channel within N_t, the measuring period. It then can establish the equation

$$n(1-q)(1-\theta)p(1-p)^{n-1} = \frac{N_s}{N_t}. \tag{6.9}$$

On the other hand, apply the Idle Sense approach, we have

$$(1-q)(1-\theta)(1-p)^n = P_{idle} = \frac{n_{idle}}{n_{idle}+1}, \tag{6.10}$$

which is observable to the anti-jammer. By (6.9) and (6.10), the anti-jammer can solve p and θ to further estimate U_J.

At the end of this section, we take $(1-q)(1-\theta)\prod_{j\in\mathcal{N},j\neq i}(1-p_j)$ as an example to investigate the accuracy of the estimation of our solution. Based on the central limit theory, given m samples of n_{idle}, we have

$$\lim_{m\to\infty} P\left(\left|\frac{\overline{n_{idle}} - \frac{P_{idle}}{1-P_{idle}}}{\sigma/\sqrt{m}}\right| \leq z\right) = \frac{1}{\sqrt{2\pi}}\int_{-z}^{z} e^{-r^2/2}dr,$$

where σ is the variance of n_{idle}.

Hence, $(1-q)(1-\theta)\prod_{j\in\mathcal{N},j\neq i}(1-p_j)$ can be precisely estimated if sufficient samples on n_{idle} is collected. However, this requires long periods of observation and may lead to slower convergence rate. Therefore, there is a tradeoff between the accuracy of the observation and the delay of

convergence. Based on the experiments we conduct, $m = 10 \sim 25$ achieves fairly good estimation with a reasonable convergence delay.

6.7 Numerical Results

In previous study, we establish a game theoretic model on jamming with the proposed defense strategy and perform mathematical analysis on the existence, uniqueness of the NE and the game dynamics. In this section, we conduct numerical study to gain some more in-depth insight on the NE and the performance of the proposed defense strategy, which cannot be derived directly from analytical results.

6.7.1 NE Analysis of G and G'

We start with the numerical analysis of the NE of the jamming game formulated previously, both with and without anti-jammer. We simulate a single-hop wireless network of 10 nodes. The transmission cost c is set to 0.01. Figure 6.1 plots the non-border NE of G derived in Theorem 6.1 as a function of S_0. Figure 6.2 plots the optimal strategy of the anti-jammer q^* and the NE of G' as a function of S_0 when the anti-jammer operates on q^*. As shown in the results for both cases, when the jammer becomes more aggressive, i.e., S_0 becomes smaller, it tends to increase the jamming probability at the NE. Consequently, the victim network reacts by decreasing their transmission probability at the NE. The optimal strategy of the anti-jammer also becomes more aggressive. Moreover, it can be checked that when $q \to 0^+$, the condition (6.2) equals to $S_0 < 0.14$. This is confirmed by the numerical results in Figure 6.2 that $q^* > 0$ when approximately $S_0 < 0.14$. As q^* tends to 0, the NE of G' coincides with the non-border NE of G, as shown in Figure 6.1 and 6.2.

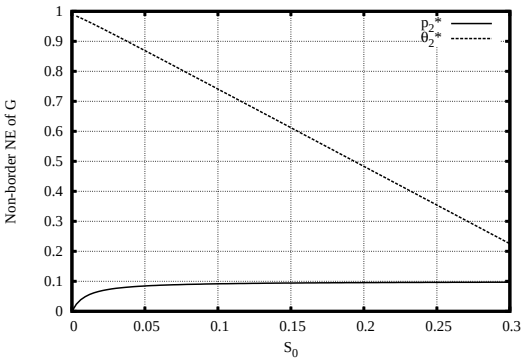

Figure 6.1: Non-border NE of G

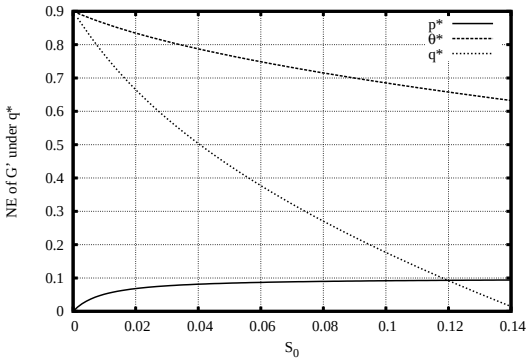

Figure 6.2: NE of G' under q^*

6.7.2 Performance Evaluation of Proposed Defense Strategy

We then evaluate the performance of the proposed defense strategy by comparing the jammer's utility U_J at the non-border NE of G and the unique NE of G', as plotted in Figure 6.3. It is insightful to notice that the jammer's energy consumption at the non-border NE of G first increases sharply w.r.t. S_0 and then decreases mildly when S_0 is large. In fact, with the increase of S_0, p^* increases and θ^* decreases. Noticing that U_J is increasing in p^* and θ^*, the results in Figure 6.3 indicates that U_J is much more sensible to p^* than to θ^* with small S_0 and less sensible to p^* with

large S_0. This observation shows that the more aggressive jamming is also more cost-effective in terms of energy. In this sense, the border NE in G can be regarded as an extreme scenario where the jammer can paralyze the network with little energy consumption, as discussed in Section 6.3.

In contrast, when the proposed defense strategy is implemented, U_J is monotonously decreasing in S_0 at the NE, as shown in Figure 6.3. As observed from Figure 6.2, the anti-jammer acts more aggressively when the jammer is more aggressive, i.e., S_0 is small. Noticing that U_J is increasing in q, the interesting observation in Figure 6.3 indicates that the influence of q on U_J outweighs the that of p on U_J when S_0 is small, thus U_J increases when S_0 decreases in G'. From Figure 6.3, we can also see that the jammer consumes more energy at the NE of G' regardless the value of S_0, which clearly demonstrates the benefits of the proposed defense strategy, especially with the aggressive jammer.

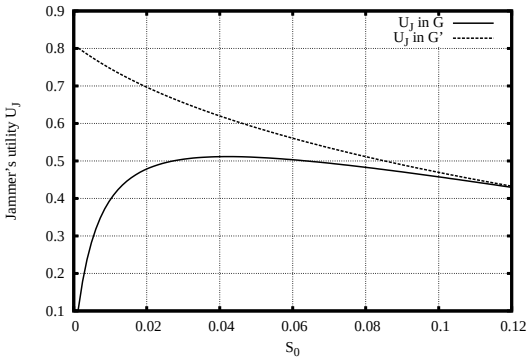

Figure 6.3: Comparison of U_J in G and G'

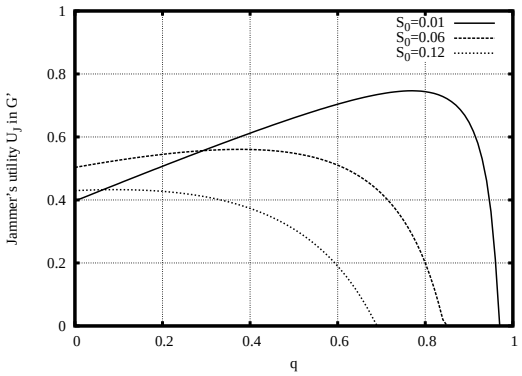

Figure 6.4: U_J in G' as a function of q

We also study the impact of the anti-jammer's strategy on the jammer's utility at the NE by plotting U_J at the NE of G' as a function of q with different value of S_0. As illustrated in Figure 6.4, U_J is almost the same if q is slightly smaller than the optimal strategy q^*, but chutes sharply after q reaches q^*, especially under the aggressive jammer with small S_0. An important guideline that can be drawn from the results is that a conservative strategy at the anti-jammer yields better performance than a too aggressive one.

6.7.3 Game Dynamics

Finally, we study the dynamics of G' by investigating the strategy update mechanisms proposed in Section 6.5. Figure 6.5 and 6.6 plot the trajectory of the players' strategies under the update mechanism (6.6) for the network nodes and (6.7) for the jammer. The step size λ is set to 0.1. S_0 is set to 0.05. p_{max} is set to 0.1. The anti-jammer's strategy is set to the optimal value $q^* = 0.44$, as can be observed in Figure 6.2. α is set to 1.87. With this parameter setting, it can be checked from Theorem 6.6 that the unique fixed point of the strategy update scheme (6.6), (6.7) is the NE where $p^* = 0.084$ and $\theta^* = 0.76$, as can be estimated from Figure 6.2. As shown in Figure 6.5 and 6.6, if the network nodes follow (6.6) and the jammer follows (6.7), the game converges to the unique NE.

We conclude this section by evaluating the performance of the adaptive recursive research method for the anti-jammer to adjust its strategy q. For the parameters: $S_0 = 0.05$, $\Delta q = 0.005$, $\varepsilon = 0.01$. Figure 6.7 plots the converged value of the network throughput S, the jammer's utility U_J and the anti-jammer's strategy q as functions of α. As illustrated in Figure 6.7, if the jammer operates on large α, the network throughput exceeds the threshold S_0. Thus in order to effectively

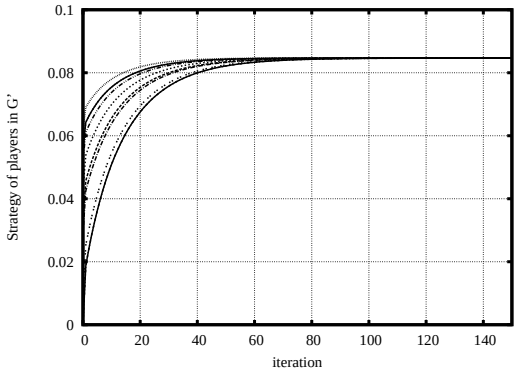

Figure 6.5: Strategy trajectory of network nodes under (6.6)

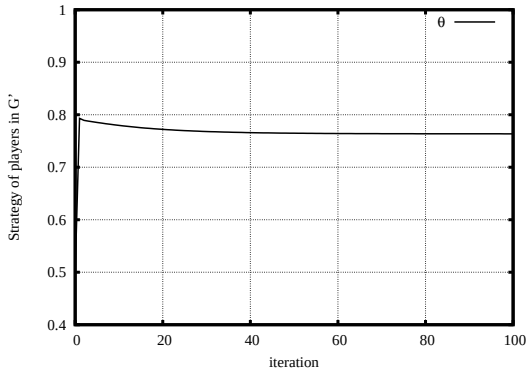

Figure 6.6: Strategy trajectory of jammer under (6.7)

disrupt the network traffic, the jammer has to act aggressively by choosing a small α. As shown in Figure 6.7, this leads to aggressive strategy of the anti-jammer and the increase of the energy consumption for the jammer, where the goal of our proposed defense strategy is achieved.

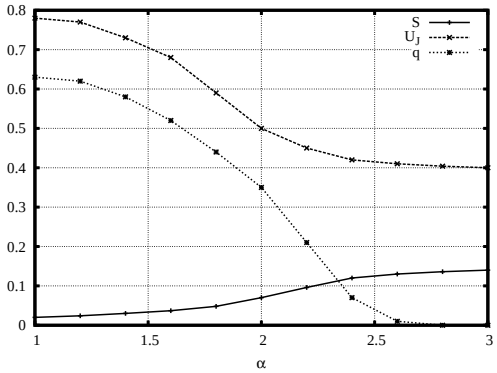

Figure 6.7: Performance evaluation of the adaptive recursive research

6.8 Conclusion

We investigated jamming in wireless networks under a game theoretic framework. Based on the analysis of the jamming game, we propose a defense strategy consisting of actively fighting the jammer face-to-face by draining its energy. We demonstrated that the proposed defense strategy can eliminate the undesirable equilibrium and increase the energy consumption of the jammer at the remaining equilibrium without degrading the network performance. Despite the limitations discussed in Section 6.4.4, we believe that the proposed defense strategy provides an alternative and active line of defense whose effectiveness is well demonstrated both analytically and numerically in the chapter.

6.9 Proofs

This section completes the detailed proofs omitted from the main text.

6.9.1 Proof of Theorem 6.1

We proceed by distinguishing two cases of NE:

Case 1: the NE is on the border of the strategy space. In this case, it is easy to check that only $p^* = 0$, $\theta^* = 1$ satisfies the NE definition.

Case 2: the NE is the non-border point of the strategy space: $0 < p^*, \theta^* < 1$. In this case, for the network, the global maximum of its utility function is achieved at inner point where $\frac{\partial U_N}{\partial p} = 0$, or

$$(1-p^*)^{n-2}(1-np^*)(1-\theta) = c. \tag{6.11}$$

On the other hand, at the NE it holds that

$$S = np^*(1-p^*)^{n-1}(1-\theta^*) = S_0. \tag{6.12}$$

Otherwise, if $S > S_0$, the jammer has incentive to unilaterally decrease θ^*, which contradicts with the definition of NE.

Combining (6.11) and (6.12), we can solve p^* and θ^* as

$$\begin{cases} p^* = \frac{1}{2}\left[1+k-\sqrt{(1+k)^2-\frac{4}{n}k}\right] = \frac{1+k-A(k)}{2} \\ \theta^* = 1 - \frac{2^n S_0}{n(1+k-A(k))(1-k+A(k))^{n-1}} \end{cases}. \tag{6.13}$$

The following two lemmas guarantee that the derived solution (p^*, θ^*) in (6.13) is a NE. Lemma 6.1 proves that it is an inner point of the strategy space. Lemma 6.2 shows that $U_N(p^*, \theta^*) > 0$.

Lemma 6.1. *It holds that* $\frac{k}{n(1+k)} < p^* < \min\left\{\frac{1}{n}, \frac{k}{n}\right\}$ *and* $0 < \theta^* < 1$.

Proof. To prove $\frac{k}{n(1+k)} < p^* < \min\left\{\frac{1}{n}, \frac{k}{n}\right\}$, we rewrite p^* in (6.13) as

$$p^* = \frac{1}{2}\frac{\frac{4k}{n}}{1+k+\sqrt{(1+k)^2-\frac{4}{n}k}}.$$

On the other hand, we have:

$$\begin{cases} \sqrt{(1+k)^2-\frac{4}{n}k} < 1+k \\ \sqrt{(1+k)^2-\frac{4}{n}k} = \sqrt{(1-k)^2+4\left(1-\frac{1}{n}\right)k} > |1-k| \end{cases}.$$

It follows that $\frac{k}{n(1+k)} < p^* < \min\left\{\frac{1}{n}, \frac{k}{n}\right\}$.

We next prove $0 < \theta^* < 1$. It is obvious that $\theta^* < 1$. Suppose, by contradiction, that $\theta^* \leq 0$, it follows from (6.1) and (6.11) that

$$np^*(1-p^*)^{n-1} \geq n\widehat{p}(1-\widehat{p})^{n-1} > S_0 \geq \frac{S_0}{1-\theta^*}$$

which contradicts with (6.12). □

Lemma 6.2. *It holds that* $U_N(p^*, \theta^*) > 0$.

Proof. Noticing (6.12), we have

$$U_N(p^*, \theta^*) = np^*(1-p^*)^{n-1}(1-\theta^*) - np^*c = np^*\frac{S_0}{np^*} - np^*c = np^*c\left(\frac{k}{np^*} - 1\right).$$

It follows from Lemma 6.1 that $U_N(p^*, \theta^*) > 0$. □

Combining the above analysis in Case 1 and Case 2, we conclude our proof of Theorem 6.1.

6.9.2 Proof of Theorem 6.2

We distinguish two cases: 1). the NE is the inner point of the strategy space and 2). the NE is at the border.

We start by examine the inner NE. Let $c' \triangleq \frac{c}{(1-q)}$, $S_0' \triangleq \frac{S_0}{(1-q)}$, the non-border NE (p^*, θ^*) can be derived following exactly the same way as case 2 in the proof of Theorem 6.1. The condition of the derived solution to be the non-border NE is $0 < p^*, \theta^* < 1$, which is satisfied if and only if (6.2) holds. It can be further shown that in this case, there is no border NE.

On the other hand, if (6.2) does not hold, G' does not have non-border NE. In this case, by checking the border of the strategy space, we can show that the only NE is $p^* = \underset{p}{\text{argmax}} \quad (1-q)p(1-p)^{n-1} - cp$ and $\theta^* = 0$.

6.9.3 Proof of Corollary 6.1

Following Lemma 6.1, we have

$$(1-q)np^*(1-p^*)^{n-1} > \frac{(1-q)k}{1+k}\left(1 - \frac{k}{n(1+k)}\right)^{n-1}.$$

Hence, if $\frac{(1-q)k}{1+k}\left(1 - \frac{k}{n(1+k)}\right)^{n-1} > S_0$, it holds that $(1-q)np^*(1-p^*)^{n-1} > S_0$. From Theorem 6.2, G' admits a unique non-border NE (6.3).

6.9.4 Proof of Theorem 6.3

Let U_J^G and $U_J^{G'}$ denote the jammer's utility at the non-border NE of G and G', we have

$$\begin{aligned} U_J^G &= [1-(1-p^*)^n]\left[1 - \frac{S_0}{np^*(1-p^*)^{n-1}}\right] \\ U_J^{G'} &= [1-(1-p^*)^n(1-q)]\left[1 - \frac{S_0}{np^*(1-p^*)^{n-1}(1-q)}\right], \end{aligned}$$

where $p^* = \frac{1+k-A(k)}{2}$. After some straightforward mathematic manipulations, we get

$$U_J^{G'} - U_J^G = (1-p^*)^n q\left[1 - \frac{S_0}{np^*(1-p^*)^{2n-1}(1-q)}\right].$$

Under the condition (6.5), if $0 < q < 1 - \frac{S_0}{np^*(1-p^*)^{2n-1}}$, we have $U_J^{G'} > U_J^G$, i.e., the existence of the anti-jammer actually can increase the jammer's energy consumption at the non-border NE.

On the contrary, if $S_0 \geq np^*(1-p^*)^{2n-1}$, then it follows that

$$1 - \frac{S_0}{np^*(1-p^*)^{2n-1}(1-q)} \leq 1 - \frac{S_0}{np^*(1-p^*)^{2n-1}} \leq 0,$$

i.e., $U_J^2 \leq U_J^1$. In this case, regardless of the value of q, the anti-jammer cannot increase the jammer's energy consumption.

6.9.5 Proof of Corollary 6.2

Recall Lemma 6.1, we have:

$$\begin{aligned} S_0 + c < \left(1 - \frac{1}{n}\right)^{2n-1} &\implies S_0 \frac{1+k}{k} < \left(1 - \frac{1}{n}\right)^{2n-1} \\ &\implies S_0 < np^*(1-p^*)^{2n-1}. \end{aligned}$$

From Theorem 6.2, this indicates that by choosing proper q, the anti-jammer can increase the jammer's utility at the non-border NE. When $n \gg 1$, the above sufficient condition becomes $S_0 + c < 1/e^2$.

6.9.6 Proof of Theorem 6.4

From (6.3), at the non-border NE, we have

$$U_J^{G'} = \left[1 - (1-p^*)^n(1-q)\right]\left[1 - \frac{S_0}{np^*(1-p^*)^{n-1}(1-q)}\right].$$

By imposing $\frac{\partial U_J^{G'}}{\partial q} = 0$, the optimal value of q can be solved as

$$q^* = 1 - \sqrt{\frac{S_0}{np^*(1-p^*)^{2n-1}}}. \tag{6.14}$$

A necessary condition that q^* given by (6.14) is the optimal value is that G' has a unique non-border NE and $0 < q^* < 1$. From Theorem 6.2, this can be translated to check whether the condition (6.2) holds or not. We proceed our analysis as follows

$$\begin{aligned} & n(1-q^*)(1+k-A(k))(1-k+A(k))^{n-1} > 2^n S_0 \\ \Longleftarrow\ & np^*(1-p^*)^{n-1}(1-q^*) > S_0 \quad \text{From (6.14)} \\ \Longleftarrow\ & \sqrt{\frac{nS_0p^*}{(1-p^*)}} > S_0 \quad \text{Noticing } p^* < 1 \\ \Longleftarrow\ & np^*(1-p^*)^{2n-1} > S_0 \quad \text{From (6.5)} \end{aligned}$$

The above shows that (6.2) holds, q^* is the optimal strategy to drain the jammer's energy, which concludes our proof.

6.9.7 Proof of Theorem 6.5

Step 1: We show that any border point cannot be a fixed point of (6.6). Assume, by contradiction, that at the fixed point $\widetilde{\mathbf{p}}$, $\widetilde{p_i} = 0$ or $\widetilde{p_i} = p_{max}$.

- If $\widetilde{p_i} = 0$, then it follows from (6.6) that

$$(1-q)(1-\theta)\prod_{j\in\mathcal{N},j\neq i}(1-\widetilde{p_j}) - c \leq 0,$$

  which, noticing that $\widetilde{p_j} \leq p_{max}$, contradicts with $c < (1-q)(1-\theta)(1-p_{max})^{n-1}$.

- If $\widetilde{p_i} = p_{max}$, we have

$$(1-q)(1-\theta)(1-np_{max})\prod_{j\in\mathcal{N},j\neq i}(1-\widetilde{p_j}) - (1-p_{max})c \geq 0,$$

  which obviously contradicts with $c > \dfrac{(1-q)(1-\theta)(1-np_{max})}{1-p_{max}}$.

Combining the above analysis shows that any border point cannot be a fixed point of (6.6).

Step 2: We show that (6.6) *admits a non-border fixed point which maximizes the network utility.* By imposing $p_i(t) = p_i(t+1) = \widetilde{p_i}$, $\forall i \in \mathcal{N}$, we obtain n equations

$$(1-q)(1-\theta)\left[1 - \frac{(n-1)\widetilde{p_i}}{1-\widetilde{p_i}}\right]\prod_{j\in\mathcal{N},j\neq i}(1-\widetilde{p_j}) = c \quad \forall i \in \mathcal{N}$$

which can be further transformed into

$$(1-q)(1-\theta)\left(\prod_{j\in\mathcal{N}}(1-\widetilde{p_j})\right)\left[\frac{1}{1-\widetilde{p_i}} - \frac{(n-1)\widetilde{p_i}}{(1-\widetilde{p_i})^2}\right] = c \quad \forall i \in \mathcal{N}. \tag{6.15}$$

Hence, $\forall i_1, i_2 \in \mathcal{N}$, we have

$$\frac{1}{1-\widetilde{p}_{i_1}} - \frac{(n-1)\widetilde{p}_{i_1}}{(1-\widetilde{p}_{i_1})^2} = \frac{1}{1-\widetilde{p}_{i_2}} - \frac{(n-1)\widetilde{p}_{i_2}}{(1-\widetilde{p}_{i_2})^2}.$$

Let $g(x) \triangleq \dfrac{1}{1-x} - \dfrac{(n-1)x}{(1-x)^2}$, we have

$$g'(x) = \frac{1}{(1-x)^2}\left[1 - \frac{(n-1)(1+x)}{(1-x)}\right].$$

It holds that $g'(x) < 0, \forall x \in (0,1)$ and $g'(x) = 0$ at 0. It follows immediately from (6.15) that $\widetilde{p}_{i_1} = \widetilde{p}_{i_2}$. Therefore, at the non-border fixed point, we have $\widetilde{p_i} = \widetilde{p}$, $\forall i \in \mathcal{N}$, where $\widetilde{p}$ is the root of

$$(1-q)(1-\theta)(1-p)^{n-2}(1-np) = c.$$

We now show that the above equation admits a unique solution in $(0, p_{max})$. To this end, let $Q(p) \triangleq (1-p)^{n-2}(1-np)(1-q)(1-\theta) - c$. We have

$$Q'(p) = \Big[-n(n-1)(1-p)^{n-2} + (n-1)(n-2)(1-p)^{n-3}\Big](1-q)(1-\theta).$$

It can be checked that $Q(p)$ is monotonously decreasing in p in $\left(0, \frac{2}{n}\right)$ and monotonously increasing in $\left(\frac{2}{n}, 1\right)$. Noticing that $Q(0) = 1 - c > 0$, $Q(1) = -c < 0$ and following the condition in the theorem,

$$Q(p_{max}) = (1-q)(1-\theta)(1-p_{max})^{n-2}(1-np_{max}) - c < 0.$$

We can show that $Q(p) = 0$ admits a unique solution $\widetilde{p} \in (0, p_{max})$. It is further easy to notice that the network utility $n(1-q)(1-\theta)p(1-p)^n - npc$ is maximized at $\widetilde{p}$.

6.9.8 Proof of Theorem 6.6

Step 1: We show that any border point cannot be a fixed point of (6.6) *and* (6.7). Assume, by contradiction, that $(\widetilde{\mathbf{p}}, \widetilde{\theta})$ is a border fixed point. It follows straightforwardly from the condition (6.8) that $0 < \widetilde{\theta} < 1$. Hence there exists i such that $\widetilde{p_i} = 0$ or $\widetilde{p_i} = p_{max}$.

- If $\widetilde{p_i} = 0$, then it follows from (6.6) that

$$(1-q)(1-\widetilde{\theta}) \prod_{j \in \mathcal{N}, j \neq i} (1 - \widetilde{p_j}) \leq c.$$

  Injecting (6.7) into the above inequality leads to

$$\frac{\alpha S_0}{\sum_{j \in \mathcal{N}} \frac{\widetilde{p_j}}{1-\widetilde{p_j}} + \frac{q}{1-q}} \leq c,$$

  which, noticing that $\widetilde{p_j} \leq p_{max}$, contradicts with $\frac{(n-1)p_{max}}{1-p_{max}} + \frac{q}{1-q} < \frac{\alpha S_0}{c}$.

- If $\widetilde{p_i} = p_{max}$, we have

$$(1-q)(1-\theta)(1-np_{max}) \prod_{j \in \mathcal{N}, j \neq i} (1 - \widetilde{p_j}) - (1-p_{max})c \geq 0.$$

  Injecting (6.7) into the above inequality leads to

$$\frac{\alpha S_0}{\sum_{j \in \mathcal{N}} \frac{\widetilde{p_j}}{1-\widetilde{p_j}} + \frac{q}{1-q}} \geq \frac{(1-p_{max})^2}{(1-np_{max})} c,$$

  which contradicts with $\frac{\alpha S_0}{c} < \frac{p_{max}(1-p_{max})}{1-np_{max}} + \frac{(1-p_{max})^2}{1-np_{max}} \frac{q}{1-q}$.

Combining the above analysis shows that any border point cannot be a fixed point.

Step 2: We show that (6.6) *and* (6.7) *admits a unique non-border fixed point.* At the non-border fixed point, combining (6.6) and (6.7), we obtain n equations:

$$\frac{\alpha S_0}{\sum_{j \in \mathcal{N}} \frac{\widetilde{p_j}}{1-\widetilde{p_j}} + \frac{q}{1-q}} = \frac{(1-\widetilde{p_i})^2}{1-n\widetilde{p_i}} c \quad \forall i \in \mathcal{N}.$$

Noticing that under the condition (6.8), $1-n\widetilde{p_i}>0$, $\dfrac{(1-\widetilde{p_i})^2}{1-n\widetilde{p_i}}$ is monotonously increasing in $\widetilde{p_i}$, following the same analysis as that in Step 2 of the proof of Theorem 6.5, we have $\widetilde{p_i}=\widetilde{p}\ \forall i\in\mathcal{N}$, where $\widetilde{p}$ is the root of

$$\frac{\alpha S_0}{\frac{n\widetilde{p}}{1-\widetilde{p}}+\frac{q}{1-q}}=\frac{(1-\widetilde{p})^2}{1-n\widetilde{p}}c, \tag{6.16}$$

which can be further arranged as

$$\frac{\alpha S_0}{c}=\frac{1-\widetilde{p}}{1-n\widetilde{p}}\left[\left(n-\frac{q}{1-q}\right)\widetilde{p}+\frac{q}{1-q}\right].$$

Let $f(\widetilde{p})\triangleq\dfrac{1-\widetilde{p}}{1-n\widetilde{p}}\left[\left(n-\dfrac{q}{1-q}\right)\widetilde{p}+\dfrac{q}{1-q}\right]$, $f(\widetilde{p})$ is monotonously increasing in $\widetilde{p}$ when $q\leq\dfrac{n}{n+1}$. Moreover, noticing (6.8), we have

$$\begin{cases} f(0)=\dfrac{q}{1-q}<\dfrac{\alpha S_0}{c} \\ f(p_{max})=\dfrac{np_{max}(1-p_{max})}{1-np_{max}}+\dfrac{(1-p_{max})^2}{1-np_{max}}\dfrac{q}{1-q}>\dfrac{\alpha S_0}{c} \end{cases}.$$

Therefore, (6.16) has a unique solution $\widetilde{p}$. Noticing that at the non border fixed point, $\widetilde{\theta}$ is uniquely determined by $\widetilde{p}$, it holds that the update scheme (6.6) and (6.7) admits a unique non-border fixed point.

Specifically, if $\theta^*\leq\theta_{max}$ and $\alpha S_0=(1-\theta^*)\left[q(1-p^*)^n+n(1-q)p^*(1-p^*)^{n-1}\right]$, it is easy to see that (p^*,θ^*) satisfies (6.6) and (6.7), thereby is the unique fixed point.

Chapter 7

On Multipath Routing in Multihop Wireless Networks: Security, Availability and Limit

7.1 Introduction

It is widely recognized that the intrinsic nature of wireless networks, such as the broadcast nature of the wireless channel and the limited resources of network nodes, makes them extremely attractive and vulnerable to attackers. Routing amid malicious attackers in such environments is a challenging task. On one hand, the most secure route(s) should be chosen such that the probability of a packet encountering any attackers is as low as possible. On the other hand, given the instability of wireless links, the most reliable route(s) should be selected such that the packet arrival probability at destination is as high as possible.

A natural approach is to use multiple paths to increase the fault tolerance and the resilience to attackers. However, how to choose the secure and reliable paths among exponentially many candidates and how to allocate traffic among them remains a difficult but crucial problem.

7.1.1 Chapter Overview

In this chapter, we address the above fundamental routing problem by focusing on two metrics: route security and availability. We start with the single-attacker case and extend our work to the multiple-attacker case in Section 7.7.

We first study the multipath routing solution minimizing the security risk, i.e., the probability that a packet is captured by the attacker under the condition that the attacker makes all its efforts to maximize this probability. We model such multipath routing problem as an minimaximization problem and formulate it as the maximum flow problem in lossy networks based on which a routing algorithm with polynomial time complexity is derived to solve it.

While the obtained solution provides the most security routes, which is crucial for security sensitive applications, the availability (the probability of a packet arriving at its destination) is another important issue that definitively cannot be ignored, especially in wireless networks with instable links. To this end, we investigate the multipath routing solution maximizing the worst-case route availability under the condition that the attacker makes all its efforts to minimize this

probability. Noticing that solving this problem requires exponential time complexity, we propose an heuristic algorithm computing the optimal path set with polynomial time complexity.

Next, we extend our efforts to study a natural problem: how to achieve a tradeoff between the route security and availability. In this perspective, we derive the routing solution maximizing the route availability while limiting the security risk under given threshold. Furthermore, as a theoretic limit of node-disjoint multipath routing, we establish the relationship between the worst-case route availability a^* and the security risk r^* :

$$a^* \leq r^*(|\mathcal{P}^{nd}| - 1),$$

where $|\mathcal{P}^{nd}|$ is the maximum number of node-disjoint paths in the network.

By simulation, we evaluate the performance of the proposed multipath routing protocols. The results shows that our solutions show the best worst-case security and availability among the simulated multipath routing protocols.

7.1.2 Background and Motivation

Multipath routing, as mentioned above, is a promising way to improve route reliability and security. Past work on multipath routing in wireless networks mainly consists of evaluating the possible paths via reputation metrics based on security or reliability and distributing traffic among the routes with highest reputation ratings.

In [PHS02], Papadimitratos *et al.* proposed an algorithm, called Disjoint Path-set Selection Protocol (DPSP), to find the maximum number of paths between a source and destination with the highest reliability. DPSP tries to find maximum number of node-disjoint paths based on the reliability metric to improve the reliability of communication by increasing the number of used paths.

In [LLF04], Lou *et al.* proposed another solution for calculating the maximum number of the most secure paths called Security Protocol for REliable dAta Delivery (SPREAD). Their solution relies on previous knowledge of security level of each node and calculates the link costs according to them. It also exploits secret sharing to spread data over multiple paths and proposes a security optimized share allocation method.

In [PH06], Papadimitratos *et al.* proposed and analyzed a routing protocol named Secure Message Transmission Protocol (SMT) which improves security and reliability of data transmission through diversity coding of data into multiple symbols and transmitting each symbol over one path by uniform loading. SMT employs a rating mechanism to select the most reliable paths based on end-to-end feedback.

Our work in this chapter differs with existing work in that we base our work on the worst-case scenarios and provide multipath routing solutions with guaranteed security and availability properties. Our motivation is two-fold: first, in most of the proposed solutions, each path is rated according to its past performance and the paths with high rate are selected to carry traffic. In such reputation-based mechanism, the computation of the reputation rates is not trivial at all; furthermore, this mechanism may fail to provide good paths when facing strategic attackers. For example, assume that three paths are available and each time the two paths with highest rates are selected. A strategic attacker can itself do the same rating estimation and attack the two paths with highest rate. The problem is that the rating mechanism implicitly assumes there exists

correlation between the history and future performance. With this correlation, one can predict the attacker's action to some extent. Unfortunately, a strategic attacker will certainly not take predictable actions. Instead, in some cases it can even take the advantage of the rating mechanism to cause more severe damage to the networks. Motivated by the above observation, we believe that it is crucial to study multipath routing solutions with guaranteed worst-case security and availability properties, which is the focus of our work.

In terms of the underlying methodology, our work is also related to the min-max optimization and routing games [BSS02], [HB01], [LMR05], [BHO+02]. In fact, our work can be seen as the application of this tools in hostile wireless networks with unreliable/lossy links absent in classical context which pose significant difficulties in solving the problem, as shown in later sections.

7.2 System Model and Assumptions

In our work, we model a multihop wireless network as a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with n nodes and m edges. Due to the instability of the wireless medium, each edge e operates with probability r_e and fails with probability $1 - r_e$. The failures of the edges are assumed to be statistically independent. We consider a data session between a single source S and destination T. S routes its packets along path $P_i \in \mathcal{P}$ (let $\mathcal{P}$ be the set of paths between S and T) with probability q_i. We assume that there is an attacker M attacking the node $v \in \mathcal{V}$ with probability p_v to cause the most damage to the communication between S and T. The attacker's objective can be to maximize the probability of capturing the packet or to minimize the packet arrival probability at T. Multiple-attacker case is discussed in Section 7.7. If node v is attacked, all the traffic passing by it is captured by M during the attack period. We assume that S and T are not attacked by M during the communication.

In this chapter, we assume that each node knows the link reliability $\{r_e\}$. [WMP05] and [ZLLY07b] address the issue of how to estimate and collect this information. We also assume that each node has the knowledge of network topology. This information can be acquired from any *secure* link-state routing protocol, e.g. [PH03]. These assumptions allow us to concentrate on the essential properties of the multipath routing problem and the resulting solutions. Note that in many cases, the dynamic characteristic of wireless networks makes link reliability and network topology change frequently, which requires that the update of the multipath set should be performed periodically or triggered by the change.

7.3 Multipath Routing with Minimum Security Risk

In this section, we study the multipath routing solution minimizing the security risk. We quantify the security risk by the maximum probability that a packet is captured by the attacker. We start with the case of single attacker M. In such routing problem, the objective of S is to calculate $\mathbf{q} = \{q_i\}$ to minimize the maximum damage caused by M. Mathematically, the multipath routing

problem can be formulated as the following minimaximization problem $\mathbf{MP_1}$:

$$\begin{aligned} r^* = \quad & \min_{\mathbf{q}} \max_{\mathbf{p}} \quad \sum_{v\in\mathcal{V}} \left[\sum_{v\in P, P\in\mathcal{P}} q(P)\tau(P,v)\varphi(P,v) \right] p_v \\ & \text{Subject to} \quad \sum_{v\in\mathcal{V}} p_v \le 1,\ p_v \ge 0, \quad \forall v \in \mathcal{V} \\ & \qquad\qquad \sum_{P\in\mathcal{P}} q(P) = 1,\ q(P) \ge 0, \quad \forall P \in \mathcal{P} \end{aligned}$$

where $\tau(P,v) = \prod_{e\in P, e\succ v} r_e$, $\varphi(P,v) = \prod_{b\in P, b\succ v} (1-p_b)$. $a \succ b$ denotes that packets encounter node/edge a before node/edge b when routed along P. $r = \sum_{v\in\mathcal{V}} \left[\sum_{v\in P, P\in\mathcal{P}} q(P)\tau(P,v)\varphi(P,v) \right] p_v$ is the expected probability that the packet is captured by M. Let $r' = \sum_{v\in\mathcal{V}} \left[\sum_{v\in P, P\in\mathcal{P}} q(P)\tau(P,v) \right] p_v$. If M attacks at most one node per path, then $r = r'$. In general case, it always holds that $r \le r'$. Noticing that $\mathbf{MP_1}$ is a non-linear optimization problem, we focus on solving $\mathbf{MP_1}'$:

$$(r')^* = \min_{\mathbf{q}} \max_{\mathbf{p}} r'$$

which is a linear optimization problem. Later in Section 7.3.2 we will show that $r^* = (r')^*$.

Consider the inner maximization problem of $\mathbf{MP_1'}$ for fixed $\mathbf{q}$:

$$\begin{aligned} & \max_{\mathbf{p}} \quad \sum_{v\in\mathcal{V}} \left[\sum_{v\in P, P\in\mathcal{P}} \tau(P,v)q(P) \right] p_v \\ & \text{Subject to} \quad \sum_{v\in\mathcal{V}} p_v \le 1,\ p_v \ge 0, \quad \forall v \in \mathcal{V} \end{aligned}$$

Associating a dual variable y, we obtain the following dual optimization problem:

$$\begin{aligned} & \min \quad y \\ & \text{Subject to} \quad y \ge \sum_{v\in P, P\in\mathcal{P}} \tau(P,v)q(P), \quad \forall v \in \mathcal{V} \end{aligned}$$

Substituting this minimization problem in $\mathbf{MP_1'}$ leads to the following linear optimization problem $\mathbf{LP_1'}$:

$$\begin{aligned} & \min \quad y \\ & \text{Subject to} \quad \sum_{v\in P, P\in\mathcal{P}} \tau(P,v)q(P) \le y, \quad \forall v \in \mathcal{V} \\ & \qquad\qquad \sum_{P\in\mathcal{P}} q(P) = 1,\ q(P) \ge 0, \quad \forall P \in \mathcal{P} \end{aligned}$$

The size of $\mathbf{LP_1'}$ grows with the number of possible paths between S and T and can be exponentially large. For this reason we reformulate $\mathbf{LP_1'}$ as the maximum flow problem in lossy networks which can be solved in a polynomial number of steps.

In $\mathbf{LP'_1}$, we can interpret $q(P)$ as a flow on P and y as the capacity of node v. Thus the constraint $\sum_{v\in P, P\in\mathcal{P}} \tau(P,v)q(P) \leq y$ restricts the flow on node v. The constraint $\sum_{P\in\mathcal{P}} q(P) = 1$ states that one unit of flow is sent from S to T. Assume that the capacity of each node v in the network is 1. $\mathbf{LP'_1}$ equals to determine the smallest scaling factor y on the network nodes such that one unit of flow can be sent from S to T. In this way $\mathbf{LP'_1}$ can be mapped to the *maximum flow* problem.

Here we would like to emphasize that the maximum flow problem in our context differs from the classical maximum flow problem due to the packet loss factor $\tau(P,v)$. Indeed our problem can be seen as the maximum flow problem in lossy networks [Way]. Each link has unlimited capacity $+\infty$, but has a reliable factor r_e. If $r_e = 1, \forall e \in \mathcal{V}$, our problem degenerates to the standard maximum flow problem with node capacity constraint.

7.3.1 Solving the Multipath Routing Problem

We first give the stretch of the solution:

- Perform *node splitting* to transform the maximum flow problem with node capacity constraint into the maximum flow problem with link capacity constraint.
- Calculate the maximum flow f^* in the transformed network after the node splitting procedure. Decompose the maximum flow into sub-flow on paths P_1, P_2, $\cdots$, P_l from S to T with flow f_i on P_i respectively.
- S should route its packets along path P_i with probability $q_i = f_i/f^*$ to minimize the security risk. The minimum security risk r^* is $1/f^*$.
- Perform the inverse procedure of node splitting. Map the paths and flows in transformed graph into the correspondent paths and flows in the original graph.

In the following, we detail the core part of the solution.

Node Splitting

The objective of *node splitting* is to transform the maximum flow problem with node capacity constraint into the standard maximum flow problem with link capacity constraint. The key idea is to replace a node with capacity c with two virtual nodes with a link of capacity c between them. The detailed transformation procedure is as follows:

- Split each node $v \in \mathcal{V}$ of capacity c_v into two virtual nodes v_1 and v_2. Add a link (v_1, v_2) with the same capacity c_v and the reliable factor 1.
- For each link $(v, v') \in \mathcal{E}$ of reliability p, replace (v, v') by a link (v_2, v') with the same reliability p and the capacity $+\infty$. For each link $(v'', v) \in \mathcal{E}$ of reliability p, replace (v'', v) by a link (v, v_1) with the same reliability p and the capacity $+\infty$.

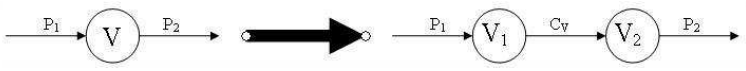

Figure 7.1: Node splitting

Figure 7.1 illustrates the node splitting procedure. After the procedure, node v_1 receives all the input flows of node v; the output flows of node v are sent by the node v_2; the added virtual link (v_1, v_2) carries the flow from input to the output which is restricted by its capacity c_v. Let $\mathcal{G}'$ denote the resulting network after applying the node splitting process on the original network $\mathcal{G}$. It is clear that each flow in $\mathcal{G}$ is one-to-one mapped into a flow with the same quantity in $\mathcal{G}'$. Hence it holds that f^* is the maximum flow in $\mathcal{G}$ if and only if f^* is the maximum flow in $\mathcal{G}'$.

Finding Maximum Flow

Our discussion in this subsection relies on the maximum flow problem in lossy networks. Given a lossy network, the maximum flow problem is to determine the maximum flow that can be sent from a source node S to a sink node T subject to the capacity constraints (i.e., each link has flow bounded by the link capacity) [Way].

Such maximum flow problem in lossy networks is a generalized case of the classical maximum flow problem. To solve this generalized problem, we run the most-improving augmenting path algorithm described in [Way], which generalizes the maximum capacity augmenting path algorithm for the traditional maximum flow problem [RKAO93].

Algorithm 4 Max-flow: Most-Improving Augmenting Path

1: **Input:** transformed network $\mathcal{G}'$
2: **Output:** maximum flow f^*
3: **repeat**
4: $f \leftarrow$ CancelCycles($\mathcal{G}'$)
5: $f^* \leftarrow f^* + f$
6: Find a most-improving augmenting path P in $\mathcal{G}'$
7: Augment flow along P and update f^*
8: **until** f^* is maximum

In Algorithm 4, the augmenting path has a value, defined as the maximum amount of flow that can reach the sink, while respecting the capacity limits, by sending excess from the first node of the path to the sink. A most-improving augmenting path is an augmenting path with the highest value. The algorithm repeatedly sends flow along most-improving augmenting paths. Since these may not be highest gain augmenting paths, this may creates residual flow-generating cycles. After each augmentation, the algorithm cancels all residual flow-generating cycles in CancelCycles(), so that computing the next most-improving path can be done efficiently. Intuitively, canceling flow-generating cycles can be interpreted as rerouting flow from its current paths to highest-gain paths.

An efficient algorithm for computing a most-improving augmenting path based on Dijkstra's shortest path algorithm is proposed in [RKAO93] with time complexity $O(m + nlogn)$ when implemented using Fibonacci heaps. We refer readers to [Way] for detailed algorithm and [Shi04] for a completed survey on the generalized maximum flow problem in lossy networks.

7.3.2 A Game theoretic Interpretation

In this subsection, to gain a more in-depth insight of the internal structure of the obtained multipath routing solution, we study the multipath routing problem from a game theoretic perspective by modelling it as a non-cooperative game between S and M, denoted as G_1. The objective of S is

to determine $\mathbf{q}$ to minimize its utility function $U_s = r$, which is the security risk. The objective of M, on the other hand, is to determine $\mathbf{p}$ to maximize its utility function $U_a = r$.

G_1 is a classical two person zero-sum game with finite strategy set. Following Proposition 33.1 of [OR94], a Nash equilibrium (mixed strategy) is guaranteed to exist. Based on the result on the two person zero-sum game (Proposition 22.2 of [OR94]), we have the following theorem on the NE (Nash equilibrium) of the multipath routing game G_1.

Theorem 7.1. *At the NE of* G_1 $(\mathbf{p}^*, \mathbf{q}^*)$*, it holds that*

$$U_s(\mathbf{p}^*, \mathbf{q}^*) = U_a(\mathbf{p}^*, \mathbf{q}^*) = min_{\mathbf{q}} max_{\mathbf{p}} r = max_{\mathbf{p}} min_{\mathbf{q}} r$$

Theorem 7.1 shows that the solution of $\mathbf{MP_1}$ is the most secure routing strategy minimizing the security risk. The minimized security risk from S's point is, on the other hand, the upper bound of the payoff that M can get. Hence, at the NE, the two players reach a compromise through self-optimization such that neither has incentive to deviate.

We now investigate the attacker's strategy at the NE. We consider the maximum flow f^* on the lossy network $\mathcal{G}'$ which is obtained from $\mathcal{G}$ applying the node splitting. Let f_e^* be the flow of f^* on the edge e. It follows from [MV65] that there exists a cut $\mathcal{C}$ separating S and T such that $\sum_{e \in S} f_e^* = \sum_{e \in S} C_e$. In our case, $\mathcal{C}$ consists of a subset of virtual links added in the node splitting process with capacity 1. This can be shown by the fact that the capacity of all other links is $+\infty$. These virtual links correspond to a set of nodes in the original network, denoted as $\mathcal{V}^{\mathcal{C}}$. As a dual part of the maximum flow problem, at the NE, M attacks every node $v \in \mathcal{V}^{\mathcal{C}}$ with probability $1/|\mathcal{V}^{\mathcal{C}}|$ where $|\mathcal{V}^{\mathcal{C}}|$ denotes the cardinality of $\mathcal{V}^{\mathcal{C}}$. At the NE, the probability that a packet passes the node $v \in \mathcal{V}^{\mathcal{C}}$ is $1/f^*$, thus the probability of the packet being captured can be computed as

$$r^* = \frac{1}{f^*} \times \frac{1}{|\mathcal{V}^{\mathcal{C}}|} \times |\mathcal{V}^{\mathcal{C}}| = \frac{1}{f^*}$$

which confirms the previous analytical results. Furthermore, it follows that at such NE, M attacks at most one node per path. This leads to $r^* = (r')^*$, which justifies our operation of solving $\mathbf{MP'_1}$ instead of $\mathbf{MP_1}$.

7.3.3 Complexity Analysis

In the solution of the previous multipath routing problem, the complexity of the node splitting and the inverse procedure is $O(n)$. We now investigate the complexity of Algorithm 4 in the following theorem.

Theorem 7.2. *Let* ϵ_0 *be the smallest positive number describing all possible values in Algorithm 4, Algorithm 4 terminates within at most* $\left\lfloor log_{\frac{m}{m-1}} \frac{f^*}{\epsilon_0} \right\rfloor + 1$ *iterations, where* $\lfloor n \rfloor$ *denotes the largest integer not larger than* n*.*

Proof. The key idea of the proof is to notice that the maximum flow in lossy networks can be decomposed into at most m augmenting paths. Algorithm 4 selects the path that generates the maximum amount of excess at the sink. Thus, each iteration captures at least a $1/m$ fraction of the remaining flow. Please refer to Section 7.10.1 for the detail of the proof. □

Note that in Algorithm 4, the time complexity of the CancelCycles subroutine is $O\left(mn^2log\frac{1}{\epsilon_0}\right)$ and that of finding the most-augmenting path is $O(m+nlogn)$. Generally, ϵ_0 is sufficiently small. The total time complexity of the algorithm is thus $O\left(mn^2log\frac{1}{\epsilon_0}log\frac{f^*}{\epsilon_0}\right)$.

In reality, it is often more practical for S to find the quasi-optimal solution of $\mathbf{MP_1}$, i.e., the flow $\widetilde{f^*} = (1-\epsilon)f^*$ where ϵ is sufficiently small. In such cases, the time complexity of finding $\widetilde{f^*}$ is $O\left(mn^2log\frac{1}{\epsilon}log\frac{f^*}{\epsilon}\right)$ applying the proof of Theorem 7.2. As a result, the proposed solution offers the flexibility for the source node to balance between the time complexity of the algorithm and the optimality of the result by tuning the parameter ϵ.

7.3.4 Discussion

The multipath routing problem investigated in this section is related to the work of inspection point deployment in [WW95] and intrusion detection via sampling in [KL03] which root from the drug interdiction problem. Our work differs from theirs in that: firstly, in [WW95] and [KL03], the strategy of the police and the service provider is to inspect and sample the edges, while in our problem, the attack is on the nodes, which is more efficient from the attacker's point of view. Secondly, in [WW95], [KL03], the network is lossless, while we work on the lossy network, which is more adapted for wireless networks where packet loss and link instability is one of the major concerns. Thirdly, since finding the maximum flow in lossy networks is by nature much more complex to solve than in classical lossless networks, we choose a solution providing the flexibility for the source node to balance between the time complexity of the algorithm and the optimality of the result by tuning the parameter ϵ.

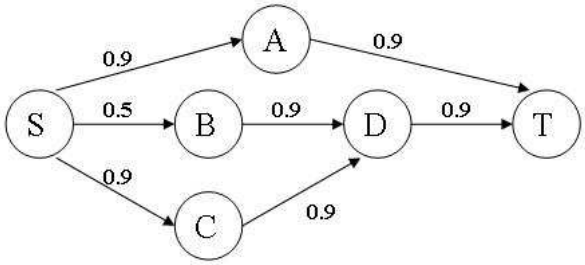

Figure 7.2: Limitation

One limitation of the obtained multipath routing solution is that it minimizes the security risk by choosing appropriate multipaths without taking into account the availability of the selected path set. Figure 7.2 (the number beside the edge is the reliability of the link) provides an illustrative example. Based on the proposed solution, S should select the path SAT and $SBDT$, but it is clear that the path $SCDT$ is more efficient than $SBDT$. The problem is that in previous solution, in some cases, the security is obtained at the price of route availability. This limitation may pose problem for the applications where the availability of the paths is as important as the security or even more, such as ad hoc networks for emergency rescue. In such scenarios, it is more important for S to find the paths with which the packet arriving probability at T (route availability) is maximized at the presence of M. This motivates us to investigate the multipath routing solution maximizing the route availability. In Section 7.6, we extend our work to derive the multipath routing solution to achieve a tradeoff between route security and availability.

7.4 Multipath Routing with Maximum Availability

In this section, we study the multipath routing solution to maximize the availability at the presence of the attacker M. In such context, S solves the following maximinimization problem $\mathbf{MP_2}$:

$$\begin{aligned} a^* = \quad & \max_{\mathbf{q}} \min_{\mathbf{p}} \quad \sum_{P\in\mathcal{P}} q(P)\tau(P,T)\prod_{v\in P}(1-p_v) \\ & \text{Subject to} \quad \sum_{v\in\mathcal{V}} p_v \leq 1,\ p_v \geq 0, \quad \forall v \in \mathcal{V} \\ & \qquad\qquad \sum_{P\in\mathcal{P}} q(P) = 1,\ q(P) \geq 0, \quad \forall P \in \mathcal{P} \end{aligned}$$

where $a = \sum_{P\in\mathcal{P}} q(P)\tau(P,T)\prod_{v\in P}(1-p_v)$ is the expected route availability, i.e., the packet survival probability at T. The engineering implication behind $\mathbf{MP_2}$ is that S maximizes the worst-case route availability under the condition that M arranges its attack to minimize it.

7.4.1 Solving the Maximinimization Problem $\mathbf{MP_2}$

The maximinimization problems such as $\mathbf{MP_2}$ are usually hard to solve directly. In our study, in order to make the problem more tractable, we apply game theory by modelling the multipath routing problem $\mathbf{MP_2}$ as a game G_2 by following the similar way as in Section 7.3.2. What differs here is that the objective of S is to maximize its utility function defined as $U_s = a$ and that the objective of M is to minimize $U_a = a$. Following the same argument, the following theorem is immediate.

Theorem 7.3. *G_2 admits at least one NE $(\mathbf{p}^*, \mathbf{q}^*)$, at which it holds that*

$$U_s(\mathbf{p}^*, \mathbf{q}^*) = U_a(\mathbf{p}^*, \mathbf{q}^*) = \max_{\mathbf{q}} \min_{\mathbf{p}} a = \min_{\mathbf{p}} \max_{\mathbf{q}} a$$

Under the game theoretic formulation, solving $\mathbf{MP_2}$ consists of solving the multipath routing game G_2, more specifically, finding the NE of G_2.

Before delving into the solution, we prove the following useful theorems on the choice of strategy at the NE for the players S and M:

Theorem 7.4. *There exists a NE where the source node S chooses only node-disjoint paths between S and T.*

Proof. The proof consists of showing that if there exists a NE where S routes its traffic on the paths with common nodes, we can always construct a NE where the source node S chooses only node-disjoint paths. Please refer to Section 7.10.2 for the detailed proof. □

In the following, we focus ourself on finding the NE with node-disjoint paths.

Theorem 7.5. *At the NE with only node-disjoint paths, the attacker M attacks at most one node per path.*

Proof. If at such NE, M attacks node $V_1, \cdots, V_n$ on the same path P with probability $p_1, \cdots, p_n$, then the payoff M gets on the path P is

$$U_P = \tau(P,T)(1-p_1)\cdots(1-p_n)$$

If M uses the same resource to attack only one node on P, say V_1, then the payoff it gets on P is

$$U'_P = \tau(P,T)(1 - p_1 - \cdots - p_n) < U_P$$

which implies that the strategy of attacking more than one node on the same path cannot be a NE. □

Now we are ready to solve the NE. We cite the following well known lemma [OR94] to conduct further analysis:

Lemma 7.1. *Every action in the support of any player's mixed strategy NE yields that player the same payoff.*

Let $\mathcal{P}^*$ denote the multipath set chosen by S at the NE, q_i the probability that S chooses path $P_i \in \mathcal{P}^*$ to route its traffic at the NE, p_i the probability that M attacks P_i at the NE, $\tau_i = \tau(P_i, T) = \prod_{e \in P_i} r_e$. Apply Lemma 7.1, we have

$$\begin{cases} \tau_i(1-p_i) = \tau_j(1-p_j) \\ q_i\tau_i = q_j\tau_j \end{cases} \quad \forall P_i, P_j \in P$$

The route availability $a = \sum_{P_i \in \mathcal{P}^*} q_i\tau_i(1-p_i)$. Noticing $\sum_{P_i \in \mathcal{P}^*} p_i = 1$, we have $a = \frac{|\mathcal{P}^*| - 1}{\sum_{P_i \in \mathcal{P}^*} \frac{1}{\tau_i}}$, where $|\mathcal{P}^*|$ is the number of paths in $\mathcal{P}^*$. Noticing that a is the route availability that S wants to maximize, solving the NE consists of finding the multipath set $\mathcal{P}^*$ such that $\frac{|\mathcal{P}^*| - 1}{\sum_{P_i \in \mathcal{P}^*} \frac{1}{\tau_i}}$ is maximized. The maximized value is the solution of $\mathbf{MP_2}$. The strategy of S and M at the NE can be solved as follows:

- S's strategy: route the packet along path P_i with probability $q_i^* = \frac{1}{\tau_i \sum_{P_j \in \mathcal{P}^*} \frac{1}{\tau_j}}$
- A's strategy: attack path P_i with probability $p_i^* = 1 - \frac{|\mathcal{P}^*| - 1}{\tau_i \sum_{P_j \in \mathcal{P}^*} \frac{1}{\tau_j}}$.

It follows from $p_i^* \leq 1, \forall P_i \in \mathcal{P}^*$ that $\tau_i \geq \frac{|\mathcal{P}^*| - 1}{\sum_{P_j \in \mathcal{P}^*} \frac{1}{\tau_j}}$. This implicates that M only focuses on a subset of routes to minimize a. Interestingly, S also has incentive to only route its packets on these paths even though other paths are attack-free due to the fact that the attack-free paths are very poor in terms of performance. In summary, S should solve the following optimization problem $\mathbf{MP'_2}$ to find the NE:

$$\begin{aligned} a^* = \quad & \max_{\mathcal{P}^*} \quad \frac{|\mathcal{P}^*| - 1}{\sum_{P_i \in \mathcal{P}^*} \frac{1}{\tau_i}} \\ & \text{Subject to} \quad \tau_i \geq \frac{|\mathcal{P}^*| - 1}{\sum_{P_j \in \mathcal{P}^*} \frac{1}{\tau_j}} \quad \forall P_i \in \mathcal{P}^* \quad (C_1) \end{aligned}$$

7.4.2 Heuristic Path Set Computation Algorithm

Although solving $\mathbf{MP'_2}$ is more tractable than solving $\mathbf{MP_2}$, yet it requires searching all possible node-disjoint paths between S and T, which leads to exponential time complexity. In the following, we propose an heuristic algorithm computing $\mathcal{P}^*$ with polynomial time complexity.

The goal of the heuristic algorithm is to find the optimal multipath set $\mathcal{P}^*$ such that $a = \frac{|\mathcal{P}^*| - 1}{\sum_{P_i \in \mathcal{P}^*} \frac{1}{\tau_i}}$ is maximized. We first introduce the two intuitions of the algorithm. Firstly, if we define τ_i as the reliability of path P_i, then choosing more reliable paths leads to higher global route availability. Secondly, if we include more paths in $\mathcal{P}^*$, then $|\mathcal{P}^*|$ increases. However, the denominator of a also increases, especially when τ_i is small. Thus, the key point of our heuristic path set computation algorithm is to find as many node-disjoint paths as possible while at the same time as reliable as possible under the condition that the paths in the multipath set satisfy the constraint C_1 such that the global route availability a is maximized.

In order to change the path reliability from a multiplicative to an additive form, each edge $e \in \mathcal{E}$ is assigned a weight $w_e = -\log p_e$. Then the conventional shortest path algorithm such as Dijkstra algorithm can be applied to find the most reliable path.

Algorithm 5 Heuristic Path Set Computation Algorithm

1: **Input:** network $\mathcal{G}$
2: **Output:** multipath set $\mathcal{P}^*$ maximizing $a = \frac{|\mathcal{P}^*| - 1}{\sum_{P_i \in \mathcal{P}^*} \frac{1}{\tau_i}}$
3: Find the most reliable path P_1 by Dijkstra algorithm, select P_1; Set $\mathcal{P}^*(1) = \{P_1\}$, $k = 1$, $a = 0$.
4: **for** each path $P_i \in \mathcal{P}^*(k)$ **do**
5: Inverse the direction of each edge on P_i, and make its length negative of the original link cost.
6: Split each node v on P_i (except S and T) into two nodes v_1 and v_2; Add an edge (v_2, v_1) of cost 0. Replace each edge $(v', v) \in \mathcal{E}$ by the edge (v', v_1) without changing its reliability, replace each edge $(v, v'') \in \mathcal{E}$ by the edge (v_2, v'') without changing its reliability.
7: **end for**
8: Run the Dijkstra algorithm, find the most reliable path P' with reliability τ' in the transformed graph.
9: If $\tau' < \frac{|\mathcal{P}^*(k)|}{\frac{1}{\tau'} + \sum_{P_j \in \mathcal{P}^*(k)} \frac{1}{\tau_j}}$, halt by returning $\mathcal{P}^*$.
10: Transform back to the original graph; erase any interlacing edges; group the remaining edges to form the new path set $\mathcal{P}^*(k+1)$.
11: If $a < \frac{|\mathcal{P}^*(k+1)| - 1}{\sum_{P_i \in \mathcal{P}^*(k+1)} \frac{1}{\tau_i}}$, then $\mathcal{P}^* = \mathcal{P}^*(k+1)$, $a = \frac{|\mathcal{P}^*(k+1)| - 1}{\sum_{P_i \in \mathcal{P}^*(k+1)} \frac{1}{\tau_i}}$.
12: If no more path can be found in the transformed graph, halt by returning $\mathcal{P}^*$, else $k = k + 1$ and go to 2.

The heuristic path set computation algorithm, shown as above, is based on the K-node-disjoint shortest path algorithm [Bha97]. The basic idea of the K-node-disjoint shortest path algorithm is to add a path in each iteration using graph transformation and link interlacing removal such that the total cost is minimized. We refer readers to [Bha97] for a detailed description of the algorithm.

Algorithm 5 is a greedy approach finding the most reliable path at each iteration. The iteration continues as long as: 1) there exist paths in the transformed graph, implying there exist node-disjoint paths in the original graph; 2) the constraint C_1 is satisfied. At the end of the algorithm, the multipath set $\mathcal{P}^*$ maximizing a is returned. Once $\mathcal{P}^*$ is found, S routes its traffic along P_i with probability q_i^*.

One point concerning the correctness of the heuristic algorithm is that if the most reliable path found in the transformed graph satisfies the constraint C_1 (in the transformed graph), then after erasing the interlacing edges, all the paths in the newly formed multipath set $\mathcal{P}^*(k+1)$ satisfy C_1.

This can be shown by recursively applying the following lemma.

Lemma 7.2. *If P_2 is the most reliable path in the transformed graph that satisfies the constraint C_1 (in the transformed graph), then after erasing an interlacing edge with another path $P_1 \in \mathcal{P}^*$, the resulting path P_1' and P_2' satisfy C_1.*

Proof. Please refer to Section 7.10.3 for the detailed proof. □

We conclude this subsection by addressing the complexity of Algorithm 5. The worst-case complexity of the heuristic algorithm is $O(n^3)$ in that there are at most d_s node-disjoint paths between S and T, where d_s is the number of outgoing edges from S. Since $d_s \leq n-1$, the algorithm iterates $n-1$ times in the worst-case (S can reach all nodes in the graph in one hop). In each iteration we run a minimum weight node-disjoint paths algorithm whose complexity is $O(n^2)$. The result is an overall worst-case complexity of $O(n^3)$.

7.5 Achieving Security/Availability Tradeoff

In Section 7.3 and Section 7.4, we focus on the multipath routing solution minimizing the security risk and maximizing the route availability. In fact, security and availability are two important aspects, of which neither should be ignored. Unfortunately, these two aspects sometimes lead to divergent routing solutions. Hence a natural next step is to investigate the multipath routing solution for multihop wireless networks that achieves a good tradeoff between the route security and availability. We formulated the routing problem in such context as the following maximinimization problem $\mathbf{MP_3}$.

$$\begin{aligned}
&\max_{\mathbf{q}} \min_{\mathbf{p}} \quad \sum_{P\in\mathcal{P}} \sum_{v\in P} q(P)\tau(P,T) \prod_{v\in P}(1-p_v) \\
&\text{Subject to} \quad \sum_{v\in\mathcal{V}} \left[\sum_{v\in P, P\in\mathcal{P}} q(P)\tau(P,v)\varphi(P,v) \right] p_v \leq r_0 \\
&\qquad\qquad \sum_{v\in\mathcal{V}} p_v \leq 1,\ p_v \geq 0, \quad \forall v \in \mathcal{V} \\
&\qquad\qquad \sum_{P\in\mathcal{P}} q(P) = 1,\ q(P) \geq 0, \quad \forall P \in \mathcal{P}
\end{aligned}$$

In $\mathbf{MP_3}$, S wants to maximize the route availability in the presence of attacker M, while limiting the security risk at most r_0. Directly solving $\mathbf{MP_3}$ needs an algorithm of exponential time complexity. In this section, we propose an heuristic solution based on Algorithm 5 to solve $\mathbf{MP_3}$. As discussed in Section 7.4, maximizing the worst-case route availability equals to solve $\max_{\mathcal{P}^*} \frac{|\mathbf{P}^*|-1}{\sum_{P_i\in\mathcal{P}^*} \frac{1}{\tau_i}}$ under the constraint C_1. The routing strategy for S is to route the packets along path P_i with probability $q_i^* = \frac{1}{\tau_i \sum_{P_j\in\mathcal{P}^*} \frac{1}{\tau_j}}$. In such context, it is easy to compute the security risk as $r = \max_{P_i\in\mathcal{P}^*} \frac{r_{e_1^i}}{\tau_i \sum_{P_j\in P} \frac{1}{\tau_j}}$ where $r_{e_1^i}$ is the reliability of the first edge of P_i, since $\max_{\mathbf{p}} \min_{\mathbf{q}} r = \min_{\mathbf{q}} \max_{\mathbf{p}} r$, the first constraint of $\mathbf{MP_3}$ on the security risk can be transformed into

$$\tau_i \geq \frac{r_{e_1^i}}{r_0 \sum_{P_j\in\mathcal{P}^*} \frac{1}{\tau_j}}, \forall P_i \in \mathcal{P}^* \qquad (C_2)$$

Our heuristic solution is extended form Algorithm 5. The key idea is to include enough number of reliable paths in $\mathcal{P}^*$ to limit the security risk. The intuition behind is that distributing the traffic among more paths helps limit the security risk. With this in mind, we modify Algorithm 5 such that the iteration stops until the constraints C_1 and C_2 are both satisfied or there is no more node-disjoint path available. In the latter case, the heuristic algorithm fails to find the multipath routing solution to $\mathbf{MP_3}$. This failure may due to the fact that the constraint on the security risk is too stringent such that no possible multipath set can meet the constraint, or alternatively, the heuristic algorithm itself cannot find the solution though it does exist. In such cases, possible solutions include secret sharing and information dispersion in which the key idea is to divide the packet to N parts and the recovery of the packet is possible only with at least T parts. These techniques can further decrease the security risk and improve the performance. We refer readers to [YP01], [PH06] since they are out of the scope of our work.

7.6 theoretic Limit of node-disjoint Multipath Routing

In this section, we establish the relationship between the worst-case route availability a^* and security risk r^* in node-disjoint multipath routing. The relationship gives one important limit of the node-disjoint multipath routing with the presence of an attacker in the sense that we cannot find better routing solutions with node-disjoint paths whose security and availability can go beyond the limit.

Let $\mathcal{P}^{nd}$ be the node-disjoint multipath set selected by S to route traffic, we have shown in Section 7.4 that

$$a^* = \frac{|\mathcal{P}^{nd}| - 1}{\sum_{P_i \in \mathcal{P}^{nd}} \frac{1}{\tau_i}}$$

On the other hand, let $q_k^0 = \dfrac{1}{\tau_k \sum_{P_j \in \mathcal{P}^{nd}} \frac{1}{P_j}}$. We have $\sum_{P_k \in \mathcal{P}^{nd}} q_k^0 = 1 = \sum_{P_k \in \mathcal{P}^{nd}} q_k$, where q_k is the probability of routing packets along P_k. From the Pigeon Hole Principle, there exists at least one path $P_m \in \mathcal{P}^{nd}$ such that $q_m \geq q_m^0$. It follows that

$$r^* = \min_{\mathbf{q}} \max_{\mathbf{p}} = \max_{\mathbf{p}} \min_{\mathbf{q}} \geq q_m r_{e_1^m} = \frac{r_{e_1^m}}{\tau_m \sum_{P_j \in \mathcal{P}^{nd}} \frac{1}{\tau_j}}$$

where $r_{e_1^m}$ is the reliability of the first edge on P_m.

As a result, we get

$$\frac{a^*}{r^*} = \left(|\mathcal{P}^{nd}| - 1\right) \frac{\tau_m}{r_{e_1^m}} \leq |\mathcal{P}^{nd}| - 1 \leq |\mathcal{P}^{nd}|_{max} - 1$$

where $|\mathcal{P}^{nd}|_{max}$ is the maximum number of node-disjoint path between S and T.

As a limit of node-disjoint multipath routing, the above relationship shows the intrinsic constraint of minimizing r and maximizing a at the same time. More specifically, if we want to limit the security risk as low as r, it is impossible to achieve $a > (|\mathcal{P}^{nd}|_{max} - 1)r$; if we want to guarantee the route availability as high as a, then we should expect the security risk of at least $r/(|\mathcal{P}^{nd}|_{max} - 1)$. Moreover, given the requirement on the route security and availability, one can check if it is realizable or too stringent by using the above formula before searching for the routing solution.

7.7 Multipath Routing with Multiple Attackers

In this section, we extend our efforts to investigate the case where there are n ($n > 1$) attackers in the network.

7.7.1 Minimizing Security Risk

There are various formulations of the multipath routing problem under n attackers to minimize the security risk, among which we are interested in two typical formulations. In the first formulation, let r_i be the probability that a packet is captured by attacker i, S wants to minimize $\sum r_i$. This case can be regarded as the case where S plays the multipath routing game G_1 with each of the attackers. Hence, the solution of $\mathbf{MP_1}$ can be applied here. The only difference is that the resulting minimum security risk is nr^*. However, this does not influence routing strategy of S, in other words, no matter how many attackers are there, the routing strategy of $\mathbf{MP_1}$ provides the most secure routing strategy minimizing the security risk in this case.

In the second formulation, the security risk is defined as the probability that a packet is captured by at least one attacker. In this context, the attackers will arrange their attacks such that no more than one attacker will attack the same node simultaneously, i.e., they try to coverage the most nodes possible to maximize the probability of capturing the packet. Similar as in Section 7.3.2, we can show that the attackers attack at most one node per path to maximize the security risk. For S, to minimize the security risk is to solve the following optimization problem $\mathbf{MP_4}$:

$$\begin{aligned} \min_{\mathbf{q}} \max_{\mathbf{p}} \quad & \sum_{v\in\mathcal{V}} \left[\sum_{v\in P, P\in\mathcal{P}} q(P)\tau(P,v) \right] p_v \\ \text{Subject to} \quad & \sum_{v\in\mathcal{V}} p_v \le n,\ 0 \le p_v \le 1, \quad \forall v \in \mathcal{V} \\ & \sum_{P\in\mathcal{P}} q(P) = 1,\ q(P) \ge 0, \quad \forall P \in \mathcal{P} \end{aligned}$$

where p_v is the probability that a node v is attacked by any of the n attackers.

$\mathbf{MP_4}$ is a linear optimization problem and can be solved by classical linear programming techniques. However, due to additional constraints $p_v \le 1$, $\mathbf{MP_4}$ cannot be transformed into maximum flow problem in lossy networks as $\mathbf{MP_1}$ that can be solved in polynomial time. As a result, solving $\mathbf{MP_4}$ may require an algorithm with exponential time complexity.

In the following, we give the upper bound of the security risk under n attackers. To this end, we relax the constraint $p_v \le 1$ and perform variable transformation by letting $p'_v = p_v/n$. $\mathbf{MP_4}$ after the transformation becomes $\mathbf{MP'_4}$:

$$\begin{aligned} \min_{\mathbf{q}} \max_{\mathbf{p}} \quad & n\sum_{v\in\mathcal{V}} \left[\sum_{v\in P, P\in\mathcal{P}} q(P)\tau(P,v) \right] p'_v \\ \text{Subject to} \quad & \sum_{v\in\mathcal{V}} p'_v \le 1, \quad 0 \le p'_v \le 1, \quad \forall v \in \mathcal{V} \\ & \sum_{P\in\mathcal{P}} q(P) = 1,\ q(P) \ge 0, \quad \forall P \in \mathcal{P} \end{aligned}$$

$\mathbf{MP'_4}$ is identical to $\mathbf{MP'_1}$ except for a constant coefficient n. It follows immediately that its

solution is n/f^* where $1/f^*$ is the maximum flow in $\mathbf{MP'_1}$. Let r' be the security risk under n attackers, following the fact that $\mathbf{MP'_4}$ is obtained by relaxing the constraint $p_v \leq 1$ in $\mathbf{MP_4}$, it holds that $r' \leq n/f^*$. In summary, by increasing the number of attackers from 1 to n, the security risk increases at most n times.

7.7.2 Maximizing Route Availability

We consider the multipath routing game between S and the attacker side consisting of n attackers. S tries to maximize the route availability and the attacker side tries to minimize it. It can be shown that at the NE of the game, no more than one attacker attacks the same node at the same time. This is because attacking the same node at the same time gives the attacker side the same payoff as the case where only one attacker attacks the node, which gives the attacker side less payoff than the case where the attacker side arranges the attack to cover the most number of nodes possible. With this in mind, by conducting the similar analysis as in Section 7.4.1, the optimization problem S should solve in multiple-attacker case is $\mathbf{MP_5}$

$$\begin{aligned} \max_{\mathcal{P}^*} \quad & \frac{|\mathcal{P}^*| - n}{\sum_{P_i \in \mathcal{P}^*} \frac{1}{\tau_i}} \\ \text{Subject to} \quad & \tau_i \geq \frac{|\mathcal{P}^*| - n}{\sum_{P_j \in \mathcal{P}^*} \frac{1}{\tau_j}} \quad \forall P_i \in \mathcal{P}^* \quad (C_3) \end{aligned}$$

where $\mathcal{P}^*$ consists of node-disjoint paths. The extension of Algorithm 5 to solve $\mathbf{MP_5}$ is straightforward.

We now investigate the case where S also wants to limit the security risk as low as r_0 at the same time, as in Section 7.5. Recall that $r_{e_1^i}$ denotes the reliability of the first edge of P_i, we sort the path by $\frac{r_{e_1^i}}{\tau_i}$, i.e. $\frac{r_{e_1^i}}{\tau_i} \leq \frac{r_{e_j^1}}{\tau_j} \iff i \leq j$. The security risk in multiple-attacker case is $\sum_{i=1}^{n} \frac{r_{e_i^1}}{\tau_i \sum_{P_j \in P} \frac{1}{\tau_j}}$, which is achieved when the n attackers attack the n most profitable paths. To limit the security risk, the constraint $\sum_{i=1}^{n} \frac{r_{e_i^1}}{\tau_i \sum_{P_j \in P} \frac{1}{\tau_j}} \leq r_0$ should be added to $\mathbf{MP_5}$. Algorithm 5 can be extended in a similar way as in Section 7.5 solve it. In the multiple-attacker case, if $|\mathcal{P}^{nd}|_{max} \leq n$, the communication between S and T is paralyzed by the attackers.

7.8 Performance Evaluation

In this section, we evaluate the performance of proposed multipath routing solutions through simulation using NS 2. Table 7.1 shows the simulation setting. The link reliability of each link is generated from a normal distribution $\sigma(0.7, 0.2)$ trunked in $[0, 1]$ interval.

7.8.1 Single-Attacker Case

We start with single-attacker case. Two scenarios are simulated: the attacker launches its attack to maximize the packet capture probability (scenario 1) or minimize the packet survival probability at the destination (scenario 2). In both scenarios, we assume that the attacker knows the routing strategy of S.

Simulation time	$1000s$
Number of nodes	100, randomly distributed
Network dimension	$1000m \times 1000m$
Transmission range	$200m$
Node speed	$4m/s$, Random waypoint model
Data traffic	CBR $4pkt/s$ 64bytes per pkt

Table 7.1: Simulation Parameters

We compare our solutions with SMT [PH06] and DPSP [PHS02]. To focus on the multipath routing solution itself and perform a fair comparison, we do not implement the message dispersion in SMT. Since SMT and DPSP do not specify how to balance traffic among the paths, we let S chose randomly in the multipath set when having a packet to send.

Let MinSR denote the multipath routing algorithm minimizing the security risk, MaxAV denote the heuristic multipath routing algorithm maximizing the route availability, MaxAV-SR denote the heuristic multipath routing algorithm maximizing the route availability while limiting the security risk under certain threshold (the threshold is set to 16% in out simulation). In MinSR, to balance the complexity of the algorithm and the solution optimality, we set $\epsilon = 0.05$. Table 7.2 shows the simulation results.

	Scenario 1		Scenario 2	
	r	p_s	r	p_s
MinSR	15.2%	54.2%	13.1%	50.3%
MaxAV	19.1%	62.2%	16.8%	59.0%
MaxAV-SR	15.8%	58.2%	15.3%	54.4%
SMT	32.3%	48.5%	39.8%	36.5%
DPSP	24.1%	49.7%	22.8%	45.3%

Table 7.2: Simulation Results: Single-Attacker Case

The simulation results show that SMT performs poorly in both scenarios. This is due to the fact that in our simulation, different from the scenarios simulated in the literatures [PH06], [KRMK06], we simulate the worst-case scenarios where the attacker launches its attack in the unpredictable way which is not correlated with the history rating. In such context, the attacker can actually take the advantage of the path rating mechanism to cause more severe damage. DSDP performs almost the same in two scenarios in that it selects the most reliable multipath set without taking into consideration of attackers. The resilience to attacks of DPSP is purely due to its multipath nature.

For our solution MinSR, it achieves the minimum security risk in scenario 2, which confirms the analytical result in that the upper bound of the security risk r^* is achieved in scenario 1. However, the route availability in MinSR is less than that in MaxAV. This is due to the limitation of MinSR discussed in Section 7.3.4. From the simulation, we can see that the sub-optimality of MinSR in terms of availability can be rather important compared to MaxAV, which achieves the best route availability among all the simulated multipath routing solutions. MaxAV-SR, on the other hand, achieves a tradeoff between the route security and availability, which is shown by the simulation results that its performance in terms of route security and availability lies between MinSR and MaxAV. Furthermore, we observe the fact that the number of maximum node-disjoint

paths in our simulation is around 6. From this observation, we can verify the relation between the route security and availability using the formula derived in Section 7.6 on the theoretic limit of node-disjoint multipath routing.

7.8.2 Multiple-Attacker Case

We then evaluate the performance of MaxAV and MaxAV-SR (the security risk threshold r_0 is set to 0.55) in cooperative multiple-attacker case where the attacker side arranges their attacks on a subset of paths so as to minimize the security risk in scenario 1 and to maximize the route availability in scenario 2. Figure 7.3 and 7.4 plot a and r as a function of the number of attackers. SMT is not plotted here since the route availability of SMT drops below 20% even with 2 attackers. MinSR is not simulated here in that according to our analysis in Section 7.7.1, the first formulation is simply the aggregated case of the single-attacker case, in the second formulation, no polynomial routing algorithm exists minimizing the security risk.

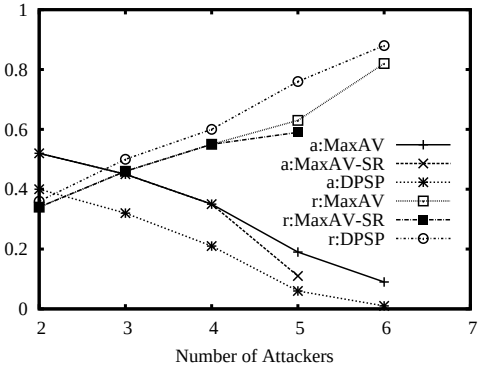

Figure 7.3: Multiple-attacker case: scenario 1

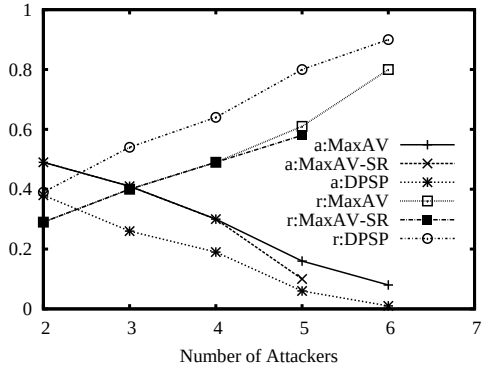

Figure 7.4: Multiple-attacker case: scenario 2

The results show that the performance degrades significantly with the increase of the number of attackers. The communication is almost paralyzed with 5 attackers. At the presence of 6 attackers, MaxAV-SR cannot find routing solution whose security risk is not more than 0.55. Once again, our results seem very different from those obtained from the literatures. This is because we focus on the worst-case scenarios throughout this chapter. Unlike the traditional simulation where a percentage of nodes is assumed to be compromised, we implement much more powerful attackers with perfect knowledge of the network and the routing strategies. These attackers are able to launch the most severe attacks which are not predictable nor correlated in time or space. In such context, our results reflect the lower bound of performance of the simulated routing solutions. We argue that maximizing this lower bound, as discussed in our work, is of great importance since the attackers cannot be underestimated in any case. Meanwhile, we can see from the results that our solutions perform substantially better than DPSP in terms of both route security and availability.

In summary, the simulations show that the proposed multipath routing solutions achieve the design objective of providing the best performance in terms of security and/or route availability in the worst-case scenarios.

7.9 Conclusion

In this chapter, we address the fundamental problem of how to choose secure and reliable paths in multihop wireless networks. We formulate the multipath routing problem as optimization problems

and propose algorithms with polynomial complexity to solve them. Three multipath routing solutions are proposed: MinSR minimizes the security risk, MaxAV maximizes the route availability and MaxAV-SR achieves a tradeoff between them by maximizing the route availability while limiting the security risk under given threshold. We also establish the relationship between the security risk and route availability, which gives the theoretic limit of node-disjoint multipath routing.

The analytical and simulation results in the chapter lead us to the following conclusion:

- Solutions based on path rating which work well in the presence of time or location correlated attacks may fail to provide secure and reliable paths facing strategic attackers with unpredictable attack patterns.
- Two issues are crucial in multipath routing. Firstly, both the security and availability should be taken into account when choosing the optimal paths, as in [LLF04] and our work. Secondly, the traffic should be balanced among paths such that they are equally "attractive" to attackers.
- Among the proposed multipath solutions, MaxAV-SR achieves good security/availability tradeoff by choosing sufficient number of mutually disjoint paths with high reliability and balancing the traffic in the optimal way.

7.10 Proofs

This section completes the detailed proofs omitted from the main text.

7.10.1 Proof of Theorem 7.2

By Corollary 2.3.4 of [Way], the maximum flow in lossy networks can be decomposed into at most m augmenting paths. Algorithm 4 selects the path that generates the maximum amount of excess at the sink. Thus, each iteration captures at least a $1/m$ fraction of the remaining flow. Let f_k be the flow after iteration k, we have:

$$\begin{aligned} f_1 &\geq \frac{1}{m} f^* \\ f_2 &\geq f_1 + \frac{1}{m}(f^* - f_1) \\ &\cdots \\ f_k &\geq f_{k-1} + \frac{1}{m}(f^* - f_{k-1}) \end{aligned}$$

Injecting $f_{k-1}, \cdots, f_2, f_1$ into f_k, we have

$$\begin{aligned}
& f_k \geq f_{k-1} + \frac{1}{m}(f^* - f_{k-1}) = \frac{1}{m}f^* + \frac{m-1}{m}f_{k-1} \\
\geq & \frac{1}{m}f^* + \frac{m-1}{m}\left(\frac{1}{m}f^* + \frac{m-1}{m}f_{k-2}\right) \\
= & \frac{1}{m}\left(1 + \frac{m-1}{m}\right)f^* + \left(\frac{m-1}{m}\right)^2 f_{k-2} \\
\geq & \frac{1}{m}\left(1 + \frac{m-1}{m}\right)f^* + \left(\frac{m-1}{m}\right)^2\left(\frac{f^*}{m} + \frac{m-1}{m}f_{k-3}\right) \\
= & \frac{1}{m}\left(1 + \frac{m-1}{m} + \left(\frac{m-1}{m}\right)^2\right)f^* + \left(\frac{m-1}{m}\right)^3 f_{k-3} \\
\geq & \cdots \\
\geq & \frac{1}{m}\left[\sum_{i=0}^{k-2}\left(\frac{m-1}{m}\right)^i\right]f^* + \left(\frac{m-1}{m}\right)^{k-1} f_1 \\
\geq & \left[1 - \left(\frac{m-1}{m}\right)^{k-1}\right]f^* + \left(\frac{m-1}{m}\right)^{k-1}\frac{1}{m}f^* \\
= & \left[1 - \left(\frac{m-1}{m}\right)^k\right]f^*
\end{aligned}$$

Algorithm 4 terminates if $f^* - \left[1 - \left(\frac{m-1}{m}\right)^k\right]f^* < \epsilon_o$, i.e., $k > log_{\frac{m}{m-1}}\frac{f^*}{\epsilon_0}$.

7.10.2 Proof of Theorem 7.4

We have shown that there exists at least one NE in G_2. We now show that if the NE consists of overlapped paths with common nodes, we can construct another NE with node-disjoint paths.

We first give some definitions. For two paths sharing nodes A, B with $(A, B) \neq (S, T)$, let Q_1 and Q_2 be the node sequence of the two paths between A and B. Q_1, Q_2 can be empty, but they cannot both be empty. Let $l(Q)$ denote the number of nodes in the sequence Q, we call the node sequence AQ_1BQ_2A a *cycle* and define the *diameter* of the cycle AQ_1BQ_2A as $\min\{l(Q_1), l(Q_2)\}$.

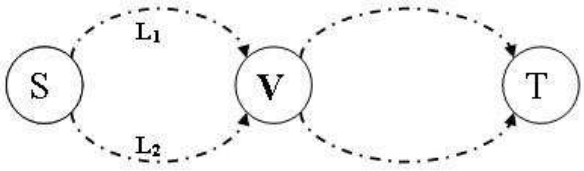

Figure 7.5: Two paths forms a cycle

Assume that at the NE, there exists paths with common nodes. We now study the cycle containing S with the common nodes S and V with the smallest diameter. Suppose this cycle is formed by path P_1 and P_2 with the node sequence $L_1 \in P_1$ and $L_2 \in P_2$ between S and V, as shown in Figure 7.10.2. Without loss of generality, we assume $l(L_1) \leq l(L_2)$. It follows that at the NE, any node $V_n \in L_1$ does not belong to the multipath set chosen by the source except P_1, otherwise we find a cycle with smaller diameter, which contradicts our assumption. It then holds

that at the NE, the attacker has no incentive to attack any nodes on L_1 because if it attacks any node on L_1 with probability p, it gets less payoff if it use the same resource attacking V. From the definition of NE, routing the packets on L_1 gives S the same payoff as routing them on L_2. Hence, we can switch all the traffic from L_1 to L_2 without changing the payoff of S. Moreover, since the attacker does not attack any node on L_1 at the NE, this operation does not change the payoff of the attacker, either. Therefore, it is easy to verify that the multipath set after the above operation is also a NE of G_2. However, the number of cycles decreases by one. As a result, by recursively repeating the above process, we can transfer any NE to a NE where the number of cycles is 0. Such NE consists of only node-disjoint paths between S and T.

7.10.3 Proof of Lemma 7.2

The lemma holds evidently if P_2 does not intercross P_1. In the following we prove the case where P_2 intercrosses with P_1. As illustrated in Figure 7.10.3, P_1 is composed of L_1^1, e, L_1^2, P_2 is composed

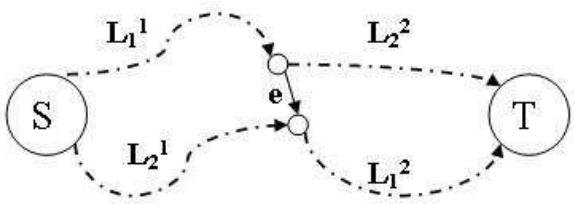

Figure 7.6: P_1, P_2 shares the edge e

of L_2^1, e, L_2^2 before erasing the interlacing edge e. Here L_i^j $(i, j = 1, 2)$ denotes a sequence of edges. Since P_2 satisfies the constraint C_1, we have

$$r_2^1 \frac{1}{r_e} r_2^2 \geq \frac{|\mathcal{P}^*(k)|}{\frac{1}{r_1^1 r_e r_1^2} + \frac{r_e}{r_2^1 r_2^2} + \Gamma}$$

where $\Gamma = \sum_{P_j \in \mathcal{P}^*(k), P_j \neq P_1} \frac{1}{\tau_j}$ and $r_i^j = \prod_{e \in L_i^j} r_e$ $(i, j = 1, 2)$. At this moment, P_2 has not been added into $\mathcal{P}^*(k)$ yet, so the numerator of the above inequality and that in step 7 in Algorithm 5 is $|\mathcal{P}^*(k)|$, not $|\mathcal{P}^*(k)| - 1$. Note the cost of e is $-log(r_e)$ in P_1 and $log(r_e)$ in P_2 in the transformed graph.

Since the Dijkstra algorithm is applied on the graph with link cost $w_e = -\log r_e$, we have: $r_1^1 r_e \geq r_2^1$ and $r_e r_1^2 \geq r_2^2$. Hence, we have:

$$\begin{aligned}
& \frac{1}{r_2^1 r_1^2} \geq \frac{1}{r_1^1 r_e r_1^2},\ r_1^1 r_2^2 \geq \frac{r_2^1 r_2^2}{r_e} \\
\Longrightarrow\ & 1 + \frac{r_1^1 r_2^2}{r_2^1 r_1^2} + r_1^1 r_2^2 \Gamma \geq 1 + \frac{r_2^1 r_2^2}{r_1^1 (r_e)^2 r_1^2} + \frac{r_2^1 r_2^2}{r_e} \Gamma \\
\Longrightarrow\ & r_1^1 r_2^2 \left(\frac{1}{r_1^1 r_2^2} + \frac{1}{r_2^1 r_1^2} + \Gamma \right) \geq \frac{r_2^1 r_2^2}{r_e} \left(\frac{1}{r_1^1 r_e r_1^2} + \frac{r_e}{r_2^1 r_2^2} + \Gamma \right) \\
\Longrightarrow\ & r_1^1 r_2^2 \left(\frac{1}{r_1^1 r_2^2} + \frac{1}{r_2^1 r_1^2} + \Gamma \right) \geq |\mathcal{P}^*(k)| \\
\Longrightarrow\ & \tau_1' = r_1^1 r_2^2 \geq \frac{|\mathcal{P}^*(k)|}{\frac{1}{r_1^1 r_2^2} + \frac{1}{r_2^1 r_1^2} + \Gamma}
\end{aligned}$$

In the same way, we can show $\tau_2' = r_2^1 r_1^2 \geq \frac{|\mathcal{P}^*(k)|}{\frac{1}{r_1^1 r_2^2} + \frac{1}{r_2^1 r_1^2} + \Gamma}$. Noticing that P_1', P_2' consists of $r_1^1 r_2^2$ and $r_2^1 r_1^2$ respectively, it follows that both P_1' and P_2' satisfy C_1, which concludes our proof.

Chapter 8

Conclusion

8.1 Thesis Summary

This thesis has presented a systematic study on selfish and malicious behaviors in wireless networks under the non-cooperative game theoretic framework in different context.

- Part I is dedicated to selfish behaviors, with Chapter 2 addressing the selfish MAC layer behaviors in IEEE 802.11 wireless networks, Chapter 3 focusing on the selfish power/rate control in the same context, and Chapter 4 proposing a pricing framework for cooperative relaying to stimulate cooperation among selfish players in non-cooperative wireless networks. In these wireless resource management problems, we studied the impact of selfishness on the system performance and in case where the resulting NE is inefficient, we developed and analyzed specific incentive-compatible protocols and pricing mechanisms to fill the gap between inefficient NE and the global optimal or quasi-optimal point.

- Part II tackles the malicious behaviors in wireless networks, with Chapter 5 establishing a generic game theoretic framework on the intrusion detection in heterogeneous networks, Chapter 6 analyzing the jamming attacks in wireless networks and proposing an active defense strategy, Chapter 7 addressing the problem of choosing secure and reliable paths in multihop wireless networks. In such security problems, we applied game theory as a basis for analyzing malicious attackers' behaviors, developing and validating new defense strategies to limit the damage caused by attackers.

By employing non-cooperative game theory as a line of research, in each chapter, we formulated the corresponding non-cooperative game in the specific context of that chapter. The resulting NE(s) is then derived, followed by an analysis on the key properties of the game solution, i.e., the existence, uniqueness of the NE, the convergence to the NE and the efficiency of the system at the NE. In Part I, this analysis served as foundations for the further design methodologies that approach the NE to the social optima in case where the NE is shown inefficient. In Part II, this insight leads to the development and validation of new defense mechanisms seeking to eliminate the unfavorable NE from the defender's perspective if multiple NEs exist and limit the damage caused by malicious attackers at the remaining NE.

In the following, we proceed this conclusion chapter by discussing some key open issues and outlining some potential directions for further research. Different from the open problems and possible extensions addressed distributedly in each chapter, which is usually limited to the specific

context of that chapter, we now take a higher-level view on the extension and generalization our work in this thesis.

8.2 Open Issues and Directions for Future Research

8.2.1 Non-cooperative Joint MAC/Power/Rate Control

Chapter 2 and 3 focused on the selfish behaviors where players could configure their contention window and transmission power/rate, respectively. As a natural extension, considering the non-cooperative joint MAC/power/rate control in IEEE 802.11 networks opens a new dimension to the problem. In particular, it is interesting to examine whether the results in Chapter 2 and 3 hold in this new context, and if the game leads to an inefficient NE, how to design pricing functions that incorporate the MAC protocol parameters (access probabilities), the transmission power and data rate to increase the efficiency is also worth exploring.

More profoundly, analyzing this new non-cooperative game can provide valuable insight on the fundamental problem of how to design efficient MAC protocols coupled with power/rate control for non-cooperative random access wireless networks. We believe that an efficient MAC protocol should satisfy the following properties:

- *Convergence and stability*: the protocol should converge to a stable equilibrium.
- *Social optimality and fairness*: the converged equilibrium should be network-wide optimal or at least quasi-optimal and each participant should get a fair share of payoff at this point.
- *Survivability*: the protocol should guide the individual nodes to operate on the designed equilibrium point even if they are purely self-interested and non-cooperative. In other words, it consists of a strategy that no selfish node has incentive to deviate.

How the non-cooperative theory and our results can be applied in developing new methodologies of designing efficient MAC protocols remains an open research problem.

The analysis in Chapter 2 and 3 is based on the saturated traffic model in which all players are back logged. Although this simplified scenario reflects the extreme case where the impact of the selfishness on the network performance is maximized and the saturation assumption is reasonable for a generic study of the corresponding non-cooperative games, we do believe that a thorough investigation of the same game under more realistic traffic models such as voice, TCP file transfers and video is of great practical importance. By introducing more sophisticated queue models and adapting utility functions (e.g., imposing the delay as a hard constraint for delay sensitive traffic such as VoIP), practical MAC protocols and power/rate control schemes can be developed to accommodate diverse applications with different Quality-of-Service (QoS) requirements.

8.2.2 Towards a Hybrid Game Theoretic Model

In Part I, we conduct our analysis under a non-cooperative paradigm where all participants in a wireless network are selfish by aiming at maximizing their own payoff regardless of others. In a more general context, a more challenging question is how the network performs if some players are selfish, others are "socially responsible" to different extent. This situation can be modeled as a hybrid (cooperative and non-cooperative) game where the players' behaviors range from total

cooperation, for those that are entirely altruistic and willing to cooperate for an overall optimum, to pure non-cooperation, for those that are selfish and seek only to maximize its own payoff even at the price of the sub-optimality of the whole network. Studying such hybrid game involves both non-cooperative and cooperative game theory. The characterization of the resulting equilibria and the investigation of the structural properties of the game can provide more insight on the efficiency and survivability of wireless networks in open, dynamic environments.

- At the first level, a mapping can be established between the degree of altruism/selfish for each player and its optimal strategy. This may further help us understand and evaluate the worthwhileness of cooperation as well as the impact of selfishness in a general context.
- At second level, it could suggest new incentive mechanisms to guide the network to a socially efficient point, e.g., to form a favorable coalition where each player benefits a share of profit corresponding to its contribution.

Furthermore, incorporating malicious players into the hybrid game by modeling them as "non-cooperative" players with the goal of paralyzing the network will add a new flavor to the problem.

8.2.3 Limitations of Classical Game Theory

As this thesis uses game theory, mostly classical game theory, as a line of research, we believe that it is pertinent in this conclusion section to address the limitations of classical game theory when applied in the engineering fields such as wireless networking in our case and how these limitations influence our modeling.

A central assumption in classical game theory is the *perfect rationality*, alternatively termed *intelligence*, under which players act as supercomputers with infinite computational capacity and can always find their best strategy, no matter how complex the game is. This utopian assumption clearly does not hold in practical games, where players are people or computer agents with limited computation capacities and where computing the best strategy is extremely costly in terms of time and resource. To bridge the gap between the "perfect rational man" paradigm and the more realistic scenario, the concept of *bounded rationality* is introduced.[1] An effective way to bound rationality is to put constraints or add costs to the information that is used to make the rational decision, typically in terms of acquisition, memory and communicating.

In our context, two learning mechanisms, best response update and subgradient update (better response update), are investigated in detail in different problems to study the game dynamics and the convergence to the equilibrium points. These two update mechanisms can be regarded as "limited memory" modeling of bounded rationality, where players only remember situations in the previous iteration. They are also among the simplest learning mechanisms for the players in a game theoretic environment, and consequently lead to simple network protocols converging to designed equilibrium points. Another example of bounded rationality can be found in Chapter 7, where computing the NE strategy (multipath set) is sometimes NP hard. In such cases, it is more reasonable to assume that the players can content themselves by choosing their strategy based on the heuristic algorithms, though the strategy may not be optimal in the absolute sense.

In our work of applying non-cooperative game theory in wireless networking problems, we usually follow the following procedure. First, we formulate the problem to be tackled as a non-

[1] More detail on this subject can be found in the textbook [Rub98].

cooperative game where each player have knowledge of the actions of other players based on which his decision is made and study the corresponding tradeoffs at the NE. This assumption is clearly not always valid in wireless networks. Hence, we then investigate how the characteristics of wireless networks influence or affect the decision making process of players and the resulting equilibria. Some typical ways of analysis are as follows:

- In Chapter 2, the GTFT strategy is introduced as a more robust version of the TFT strategy in the wireless environments where accurate observation is impossible due to the error-prone nature of the radio channel. With this more tolerant strategy, the game is actually more likely to reach a stable equilibrium where the payoff is acceptably optimal for any player.
- In Chapter 3 and 6, specific mechanisms are designed for players to update their strategy based on only observable information without the knowledge of the actions of other players. The asynchronous version of the strategy update scheme is also investigated as it is sometime impractical for players in wireless networks to remain synchronized with each other.
- In Chapter 5, the detection rate a and the false alarm rate b are two crucial parameters that cannot be exactly estimated in practice. To address this, we conducted a sensitivity analysis study the impact of inaccurate information of the parameters on the players' payoff at the NE.

Despite the efforts in this thesis and elsewhere devoted to adapting the game theory in the wireless networking field and accessing the impact of its limitations on the final results, we argue that it remains an open and challenging task to study games with incomplete and imperfect information in the field of wireless networking with its unique characteristics and constraints.

8.3 Concluding Remark

The key contribution of this thesis is to investigate the selfish and malicious behaviors in wireless networks, or more generally, to study the interactions among network participants or entities with conflicting objectives. Although the analysis is conducted for several specific problems ranging from non-cooperative resource allocation to network intrusion detection, we believe that the methodology employed in this thesis and its results can have much wider applications in emerging fields of modern networks and distributed systems beyond the scope of this thesis. Studying cooperation and security issues arising there is an important development of this thesis, as well as a promising avenue for further research.

Appendix A

Toward Secure and Scalable Time Synchronization in MANET

A.1 Introduction

Ad hoc networks are autonomous collections of mobile nodes communicating with each other over wireless links and cooperating in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure. In such environments, time synchronization is crucial. It is a key function to perform power management and to support the medium access control protocol in the Frequency Hoping Spread Spectrum version of the physical layer [80299]. It also plays an important role in the support of QoS in ad hoc networks, particularly for real-time applications. Furthermore, a common view of local clock time is a basic requirement in some ad hoc routing protocols and cryptography and authentication schemes for detecting out-of-date or duplicated messages.

The high dynamic nature of ad hoc networks, the nondeterminism of the wireless channel and the lack of reference nodes make time synchronization a challenging task in ad hoc networks in that traditional time synchronization techniques for wired networks (e.g., [NTP]) are no more applicable to ad hoc environment due to their centralized nature and the heavy traffic and computation overhead they involve. A good synchronization mechanism for ad hoc networks should be robust to mobility and topology changes, efficient in terms of traffic and processing cost, scalable and secure.

Here we pay a special emphasis on the security aspect because recently many mechanisms have been proposed to address the time synchronization problem in ad hoc networks [EGE02], [GKS03], but most of them do not take into account security, although security is a major challenge in ad hoc networks. As a result, they are very vulnerable to various attacks ranging from modifying and replaying a time synchronization message to sending forged time values to desynchronize the network or disturb the receiver's clock. [KMR05] shows through simulations that the attacks against IEEE 802.11 Timing Synchronization Function (TSF) can cause significant damage to a large number of nodes. Such insecure time synchronization protocols may further cause serious problems on the applications and protocols based on synchronized time. Nodes may fail to be activated because of the incorrect time estimation, which may cause serious problems such as failing to respond to important events and packet loss. Out-of-date and replayed messages cannot be detected in ad hoc routing protocols or some cryptography and authentication schemes, which

may lead to many new opportunities for DoS (Deny-of-Service) and replay attacks.

Given the insecurity of existing time synchronization protocols in ad hoc networks and their detrimental effect on the applications, we propose a novel suite of time synchronization mechanisms for ad hoc networks taking into consideration security, scalability and other challenges. The proposed mechanisms are based on symmetric cryptography, avoiding the costly digital signature schemes which may be undesirable for resource constrained environments such as ad hoc networks.

We start by performing an in-depth analysis on the core problems of existing synchronization mechanisms for ad hoc networks based on which we propose our secure single-hop time synchronization procedure (SSTSP). We show by simulation and analytical studies that SSTSP significantly outperforms existing approaches in terms of scalability, accuracy and security. We then extend our efforts to the secure time synchronization for multi-hop ad hoc networks. We propose the multi-hop secure time synchronization procedure (MSTSP), an extended and adapted version of SSTSP for multi-hop ad hoc networks, and evaluate its performance via simulation. The results show that the performance of MSTSP is significantly superior to TSF and is among the best of currently proposed solutions in terms of accuracy and scalability. Besides, MSTSP can maintain the network synchronized even under malicious attacks.

A.2 Related Work

Time synchronization is the process to ensure that physically distributed processors have a common notion of time. There are two commonly known approaches for time synchronization [RK04], centralized and distributed. The centralized approach is also known as master-slave synchronization where there is one or more accurate clocks (the master(s)) to which all other nodes listen and adjust their local clocks accordingly. The time synchronization mechanism proposed in [GKS03] for ad hoc networks belongs to this catalog. The distributed approach is also known as mutual synchronization where there is no master clock, but instead all clocks cooperate to achieve synchronization in a distributed manner. IEEE 802.11 TSF in ad hoc mode belongs to this catalog.

For mobile ad hoc networks we argue that the distributed approach is more suitable due to its robustness, flexibility and adaptability. This motivates us to focus our efforts on the secure distributed time synchronization mechanism for ad hoc networks. IEEE 802.11 TSF is specified by IEEE 802.11 standards as an efficient distributed synchronization mechanism for single-hop ad hoc networks. Other distributed synchronization approaches [SCS04], [RK04] mainly base themselves on IEEE 802.11 TSF and improve it to achieve better performance or extend it to multi-hop ad hoc networks.

A.2.1 IEEE 802.11 TSF In Ad Hoc Mode

IEEE 802.11 standards specify the ad-hoc-mode Timing Synchronization Function (TSF) for IEEE 802.11 ad hoc networks (IBSS) [80299] in which time synchronization is achieved by periodical time information exchange through beacons containing timestamps and other parameters. Each node maintains a local clock counting in increments of microseconds. All nodes in the IBSS compete for beacon transmission every Beacon Period (BP). At the beginning of each BP, there is a beacon generation window consisting of $w + 1$ slots each of length $aSlotTime$, where w is a parameter defined by system. Each node calculates a random delay uniformly distributed in $[0, w] \times aSlotTime$ and schedules to transmit a beacon when the delay timer expires. If a beacon is received before

the random delay timer has expired, the node cancels the pending beacon transmission. Upon receiving a beacon, the node sets its local clock to the timestamp of the beacon if the value of the timestamp is later than its local clock.

In spite of its distributed nature and its efficiency in terms of communication cost, IEEE 802.11 TSF has the following problems when applied to large scale or multi-hop ad hoc networks:

- *Fastest node asynchronization:* As identified in [LZ03], the clock of the fastest node may drift away, because it may not get a chance to transmit its beacon. Since the fastest node does not synchronize itself to other nodes, its clock will keep drifting away from others. The problem becomes more severe when the number of nodes of the network increases.

- *Beacon collision:* As the number of nodes in the network increases, the synchronization beacon transmission contentions uprise accordingly. As a result, in a large network, due to repeated collisions, synchronization beacons can hardly be successfully transmitted and some nodes may fail to synchronize with others.

- *Time partitioning:* As identified in [SV04], this problem occurs when TSF is applied to multi-hop ad hoc networks, where nodes fall into clusters which may be desynchronized during a long period of time. When the number of nodes increases, the problem has a more negative impact on the synchronization accuracy. Giving faster nodes higher chance in beacon transmission will also increases the impact of the time partitioning problem.

A.2.2 Scalable Time Synchronization for Ad Hoc Networks

ATSP was proposed in [LZ03] to solve the *fastest node asynchronization* problem in IEEE 802.11 TSF. The basic idea is to let the fastest node compete for beacon transmission every BP and let other nodes compete only every I_{max} BPs. The parameter I_{max} should be carefully chosen to reach a tradeoff between scalability and stability. As an improved version of ATSP, the authors propose TATSP in which the nodes are dynamically classified into three tiers according to the clock speed. The nodes in tier 1 compete for beacon transmission in every BP and the nodes in tier 2 compete once in a while and the nodes in tier 3 rarely compete. SATSF is another synchronization protocol proposed in [ZL05] compatible with IEEE 802.11 TSF. In SATSF, node i competes for beacon transmission every $FFT(i)$ BPs. $FFT(i)$ is adjusted at the end of each BP in the way that fast nodes will gradually decrease their FFT value, thus competing more frequently than slow nodes.

ASP is proposed in [SCS04] to synchronize multi-hop ad hoc networks. The basic idea is to synchronize the whole network by fulfilling two tasks: to increase the successful transmission probability for faster nodes and to spread the faster time information throughout the whole network. The first task is achieved by increasing the beacon transmission priority of a node who has faster time and by cutting down the priorities of the others. When some slower nodes get enough information to accomplish synchronization by themselves, their beacon transmission priorities are increased to carry out the second task.

[RK04] proposes a mechanism which differs from the idea of giving faster nodes higher priorities. In the mechanism all nodes participate equally in the synchronization of the network. The authors define a controlled clock, which is an adjusted clock of the real clock, and a parameter $s = \frac{\text{controlled clock}}{\text{real clock}}$. Each node participate the contention with probability p every T_DELAY BPs

if no beacons are received within last T_DELAY beacons. When receiving a beacon, the node updates s and p to synchronize to the sender of the beacon.

A.2.3 Secure and Fault Tolerant Time Synchronization

In spite of the numerous time synchronization protocols proposed for ad hoc networks, most of them have not been built with security in mind. To our knowledge, there exist very few propositions on the secure time synchronization protocols in the literature among which [SZC05] mainly focus on a specific type of attack called delay attack. The authors propose two approaches to detect and accommodate the delay attack. One approach uses the generalized extreme studentized deviate (GESD) algorithm to detect multiple outliers (malicious time offset). The other uses a threshold based on a time transformation technique to filter out the outliers. [GvHS05] proposes several protocols for sensor networks to secure pairwise time synchronization over single hop and multiple hops. The authors further extend their efforts to secure group time synchronization. They propose the lightweight secure group synchronization protocol to counter external attacks and the secure group synchronization protocol to counter both external and internal attacks but at the price of the heavy traffic overhead and the lack of scalability. [SNW06] proposes a fault-tolerant cluster synchronization protocol for sensor networks in which the hash chain scheme is applied to achieve local broadcast authentication. All sensors should be initially synchronized to bootstrap the protocol.

Our proposed time synchronization mechanisms differ from existing schemes in the following ways

- We take into account the scalability issue in our time synchronization protocols. Our synchronization mechanisms do not operate on synchronization message flooding or exchanging between each pair of nodes which may pose scalability problem.
- Our synchronization protocols are totally distributed and do not rely on any synchronization sources or hierarchy. This feature makes our approach robust to topology changes and network dynamics in ad hoc environments.

A.3 System Model

A.3.1 Clock Model

Each mobile node is equipped with a clock, a time measurement device normally composed of a hardware oscillator and an accumulator. Mathematically, the measured time $T(t)$ is a function of real time t:

$$T(t) = \int_{t0}^{t} \rho(\tau) d\tau + T(t_0)$$

where ρ is the nominal frequency of the oscillator, $T(t_0)$ is the initial clock offset.

In an ideally synchronized network, for each node i it holds that $\rho_i(\tau) = 1$ and $T(t_0) = t_0$ for all time long. However, since all hardware clocks are imperfect, the above equations in the ideal case do not hold. As a result, different clocks may drift away from each other. In our work, we use the bounded-drift model in which the difference between $\rho_i(\tau)$ and 1 is bounded by $\Delta\rho_{max} \sim 10^{-6}$,

meaning that the clock drifts away for several seconds in 10 days (10^6 seconds). Therefore, the synchronization process is indispensable and should be executed periodically. We also assume that during a period of time that is not very long, $\rho_i(\tau)$ does not vary with time. Thus the clock can be regarded as linear with respect to real time during that period of time.

A.3.2 Time Synchronization Model

Although time synchronization is essential to many applications in ad hoc networks, the requirement ranges from extreme strict synchronization to loose coordination. Therefore, there are actually many different types of synchronization mechanisms based on different criteria such as the scope and the lifetime of the synchronization [RBM05]. Our mechanism falls into the catalogue of network-wide, server-less, proactive synchronization, as explained as following:

- Network-wide: The proposed synchronization mechanisms provide network-wide synchronization where all nodes within the network achieve approximately the same clock reading. The other end of the spectrum is the synchronization among only a subset of nodes in the network. A typical example is pair-wise synchronization that aims to provide synchronization between a pair of neighbor nodes.
- Server-less: Our proposed synchronization mechanisms are fully distributed without any server or external time sources as in NTP [NTP]. Each node is synchronized with every other node with a time which might be different from the real time. Our approach can meet the need of most applications in ad hoc networks that requires synchronized clock.
- Proactive: The proposed approaches proactive such that the network is maintained synchronized by the repeated execution of the synchronization procedure. In contrast to the proactive synchronization is the on-demand synchronization in which the synchronization procedure is triggered by demand or certain events.

A.3.3 Attacker Model

Possible attacks to time synchronization protocols
Synchronization message forgery
Synchronization message alteration
Synchronization message replay
Synchronization message relay (delay)
DoS attack

Table A.1: Synchronization attacks

Attackers may disrupt the operation of the time synchronization protocols by exhibiting malicious behavior: e.g., replay, forge, corrupt synchronization messages to influence the time view of benign nodes, as shown in Table A.1. The attacks to the synchronization protocols can be classified as external attacks and internal attacks based on the information the attackers have. External attacks are launched by external attackers who do not have the cryptographic credentials (e.g. public/private key pairs, authenticated hash chains) that are necessary to participate in the synchronization procedure. Internal attacks are launched by internal attackers who have compromised legitimate nodes, and therefore have access to the cryptographic credentials of those nodes.

Obviously internal attacks are far more difficult to detect and sometimes cannot be countered by pure cryptographic primitives.

A.4 Single-hop Secure Time Synchronization Procedure

A.4.1 Design Philosophy

Although TSF provides an efficient distributed synchronization mechanism in terms of traffic overhead, it suffers from the scalability problem due to its beacon contention scheme. Besides, it is vulnerable to various malicious attacks. In this section we address the above two problems which are vital to build a scalable and secure synchronization protocol.

First we argue that the root of the scalability problem in TSF lies in the fact that the increase in the number of nodes in the network decreases the synchronization beacon emission opportunity of the fastest node or a subset of the fastest nodes. Some protocols improving TSF increase the successful emission probability of the fastest nodes by attributing them priority with respect to other nodes in the network. These mechanisms are significantly more scalable than TSF, but since they follow the same contention mechanism as TSF, the scalability problem is not totally solved. Furthermore, they usually depend on the observation of the beacons to find and locate the fast nodes, which may increase the latency of synchronization.

SSTSP, however, addresses the scalability problem from another angle. In SSTSP, all nodes content to emit the synchronization beacon at the beginning following the contention mechanism of TSF. The winner becomes the reference node and emits a beacon in the beginning of every BP without random delay. Other nodes synchronize their local clocks to the reference node until the reference node leaves the network, when another round of contention begins. To synchronize to the reference node, a node adjusts its clock parameters to gradually catch up with the pace of the reference clock in order to avoid backward and uncontinuous leaps in time. All nodes have the equal chance to become the reference node, but the contention takes place only when the formal reference node leaves and once the reference node is established, other nodes disable their beacon emission and synchronize their local clocks to the reference node each BP. The proposed mechanism maintains the distributed nature of the synchronization process while removes the scalability problem from its root. By making the full use of every received synchronization beacon and adopting a fine adjustment mechanism, we achieve significantly better synchronization accuracy than TSF and avoid all the backward or other uncontinuous leaps in local adjusted clock. Furthermore, by carefully choosing parameters, our mechanism is robust to the change of the reference node and the loss of synchronization beacons.

Furthermore, our approach can detect malicious synchronization attacks and prevent networks from being desynchronized by malicious nodes using erroneous time values. To this end, we use μTESLA [PST+02], a lightweight technique base on one-way hash chain, to protect synchronization beacons against external attackers. We would like to mention that traditional security mechanisms based on asymmetric cryptographic operations cannot be applied in our context in that it usually takes up to hundreds of milliseconds depending on the CPU capacity of the nodes, which may increase significantly the synchronization error. Furthermore, due to its nature, nodes in ad hoc networks may be resource constrained. It is sometimes expensive or even prohibited for such nodes to perform heavy asymmetric cryptographic operations. In contrast, hash functions are three to four orders of magnitude faster than asymmetric operations and can be performed in an on-the-fly

way such that it causes almost no additional delay.

Moreover, in our approach, we propose the "clock drift check" to counter the internal attacks and other attacks such as delay attacks and replay. This mechanism is based on the fact that the difference between any two clocks cannot drift unboundedly within a certain period of time.

Notations

s_i: Hash chain seed of node i
n: Hash chain length
T_0: Start time of the Hash chain
$h^j(s_i)$: The j^{th} element of node i's Hash chain
BP: Beacon period, typical value is 0.1s
t_i: Local unadjusted time of node i
$c_i(t)$: Local adjusted time of node i at local time t. Our goal is to synchronize $c_i(t)$
t_i^j: Local unadjusted time of node i when receiving the beacon in the j^{th} BP
t_{ref}^j: Local adjusted time of the reference node when emitting the beacon in the j^{th} BP
k_i^j, b_i^j: Coefficient and offset parameter to be adjusted when receiving the beacon in the j^{th} BP
ρ_i: Nominal frequency of node i's clock, can be regarded as constant during a short period of time.
ρ_i': Nominal frequency of node i's adjusted clock, $\rho_i' = \rho_i * k_i^j$ in the j^{th} BP
t_p: Transmission and propagation delay
T^m: Local expected emission time of the synchronization beacon in the m^{th} BP, $T^m = T_0 + m * BP$ if $m > 1$
ts_{ref}^j: Adjusted timestamp value obtained from the beacon emitted by the reference node in the j^{th} BP. $ts_{ref}^j = t_{ref}^j + t_p$. ts_{ref}^j is estimated at the receiver side.
$(t_i^j)^*$, $(t_{ref}^j)^*$, $(ts_{ref}^j)^*$: Expected values of t_i^j, t_{ref}^j, ts_{ref}^j.
ϵ: Maximum error when estimating t_{ref} by ts_{ref}, normally $\epsilon < 5\mu s$
σ: Maximum synchronization error in SSTSP
δ: Threshold in the "clock drift check"

A.4.2 Assumptions and Requirements

We assume that each pair of nodes shares a pair-wise key which is used to bootstrap the synchronization when a node enters the network. Once the new arriver acquires the initial synchronization, the pair-wise keys are no more needed for the following phase.

To use one-way hash chains, we need some mechanism for a node to distribute an authenticated element $h^n(s_i)$ in its hash chain. A traditional approach is to let each node use its public key sign the hash chain element. Alternatively, a node can securely distribute an authenticated hash chain element using pair-wise keys [HPJ02] or non-cryptographic approaches [SA02].

We also assume that the synchronization beacons are timestamped below MAC layer. Thus, we remove the most significant non-deterministic factor of the end-to-end delay of the beacons, medium access waiting time.

A.4.3 Synchronization Procedure

Node initiation

Each node i picks a random seed s_i and generates its hash chain based on s_i: $h(s_i)$, $h^2(s_i)$, ..., $h^n(s_i)$. The last element $h^n(s_i)$ is authenticated and published within the network. The start time of the hash chain T_0 is also published (e.g. T_0 can be configured and published by the first node arriving in the network or be integrated into the synchronization beacons). Suppose the beacons are expected to be emitted at time $T_0 + j * BP$ $(j = 1, 2, ..., n)$. Each element of the hash chain $h^{n-j}(s_i)$ is used as the key to secure the synchronization beacon sent by node i in the time interval $[T_0 + j * BP - BP/2,\ T_0 + j * BP + BP/2]$ if node i is the reference node. Node i, in its synchronization beacon sent in the above time interval, discloses the element $h^{n-j+1}(s_i)$ $(j > 1)$, allowing other nodes to authenticate previously received beacons sent by itself in last time interval $[T_0 + (j-1) * BP - BP/2,\ T_0 + (j-1) * BP + BP/2]$.

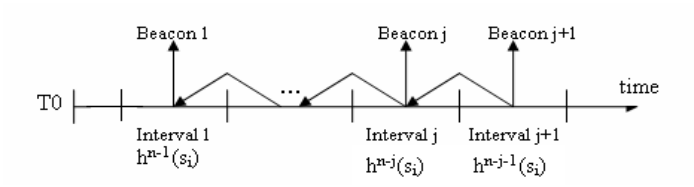

Figure A.1: Hash chain scheme

Our single-hop secure time synchronization procedure (SSTSP) consists of two phases: the bootstrapping phase and the synchronization phase.

Bootstrapping phase

When joining the network, the node first enters the bootstrapping phase during the first BP to acquire the initial synchronization with the rest of the network. This initial synchronization further enables the application of one-way hash chains to secure the time synchronization procedure in the synchronization phase that follows the bootstrapping phase.

We adopt the following simple pair-wise synchronization protocol [GvHS05] in this phase:

1. $i(t_i^s) \rightarrow j(c_j^r)$: $i, j, N_i, SynInit$
2. $j(c_j^s) \rightarrow j(t_i^r)$: $c_j^r, c_j^s, N_i, SynAck, MAC_{K_{ij}}\{j(t_i^r)$: $c_j^r, c_j^s, N_i, SynAck\}$
3. If $d = (t_i^r - t_i^s) - (c_j^s - c_j^r) < \beta(T_{init} + T_{ack})$, i sets $t_i = t_i + (c_j^r - t_i^s) - (t_i^r - c_j^s)$

In the above protocol, i is the new arriver that synchronizes to its neighbor j. i sends a SynInit message at local time t_i^s. j receives the message at its local adjusted time c_j^r and send back a SynAck message at c_j^s containing the correspondent timestamps protected by the attached MAC. i then computes the end-to-end delay d and compares d with $\beta(T_{init} + T_{ack})$ to check if any packet is delayed or replayed by attacks, where β is a coefficient sightly greater than 1, T_{init} and T_{ack} is the transmission time of the SynInit and SynAck including packet header and preamble. In normal cases, we have $d \sim T_{init} + T_{ack}$ since the propagation time is negligible and the calculation of keyed MAC can be processed in the on-the-fly as the packet is being transmitted. If the SynInit or SynAck packet is replayed or delayed by an attacker, then since the attacker cannot receive and

emit at the same time, we have $d \geq 2(T_{init} + T_{ack})$. Next i computes the offset between its local clock and j's clock and uses the offset to adjust its clock.

i thus synchronizes itself with a trusted neighbor j or repeats the above protocol with several neighbors if it does not have any trusted neighbors and further eliminates biased offsets and uses the averaged of the rest unbiased offset to adjust its local clock. In the bootstrapping phase, $c_i(t_i)$ is set to t_i. At the end of the bootstrapping phase, i is synchronized with the network and then enters the following synchronization phase.

Synchronization phase

In this phase, each node competes to be the reference node if it has not heard the synchronization beacon in the last l BPs. A larger value of l makes the mechanism more robust since the failure to receive a beacon may be due to collision or temporary wireless channel instability other than the leave of the reference node. As price, a larger l increases the synchronization error when the reference node changes. In case of collision, the contention may last several BPs. The contention mechanism is the same as in IEEE 802.11 TSF. The winner becomes the reference node and emits a beacon in the beginning of every BP without random delay. Other nodes synchronize their local clocks to the reference node until the reference node leaves the network, when another round of contention begins. A node joining the network does not participate in the contention until it is synchronized with the network. We use μTESLA scheme to protect the beacons. The synchronization beacon sent by the reference node ref in time interval j is:

$$< B,\ j,\ h_{ref}^{n-j}(B,\ j),\ h^{n-j+1}(s_{ref}) >$$

where B is the original unsecured synchronization beacon, $h_{ref}^{n-j}(B,\ j)$ denotes the HMAC output using $h^{n-j}(s_{ref})$ as the key applied to $(B,\ j)$, $h^{n-j+1}(s_{ref})$ is the disclosed key corresponding to the last interval (interval $(j-1)$).

Each node i temporarily stores the recently received beacons. Upon receiving a new beacon from the reference node ref, node i performs the following checks:

- Node i checks whether interval j corresponds to the current time interval.
- If the above check passes, node i further checks the validity of the disclosed key $h^{n-j+1}(s_{ref})$ in the beacon by verifying whether $h^{j-1}(h^{n-j+1}(s_{ref}))$ equals to the published element $h^n(s_{ref})$. In case of success, i checks the authenticity and the integrity of the beacon received in last interval using disclosed key $h^{n-j+1}(s_{ref})$. Node i can store previously authenticated disclosed key $h^{n-j+2}(s_{ref})$ to reduce processing overhead. In this case only one hash operation is needed instead of $j-1$.
- If the above two checks pass, i performs the "clock drift check" whether $|ts_{ref}^j - c_i(t_i^j)| < \delta$, where the threshold δ is the bound of the clock drift between $c_i(t_i^j)$ and ts_{ref}^j. In case where i has not received beacons during last l BPs because the reference node changes, $\delta = (l+2)\sigma$.[1] If i has just entered the synchronization phase, $\delta = \sigma + 4\Delta\rho_{max}BP$.[2] In other cases, $\delta = \sigma$.

[1] See Lemma A.2 for the proof that after the reference node changes, the synchronization error after the change is (l+2) times as much as the synchronization error before the change.

[2] It is easy to show that the maximum clock drift during one BP is bounded by $2\Delta\rho_{max}BP$. When entering the synchronization phase, the difference between the clock of i and the reference node increases in the beginning $2BP$s before i can adjust its clock using authenticated beacons.

If the check fails, the beacon may be replayed or delayed or the timestamp is forged by an internal attacker.

If all the above tests pass, node i then adjusts its local clock using the authenticated beacon $(j-1)$ and $(j-2)$. Note that beacon j cannot be used for clock adjustment until its integrity is verified. In SSTSP each node i has two clocks: an original clock and an adjusted clock. The original clock is the hardware clock of the node, e.g. a 64-bit counter with the resolution of $1\mu s$ in the IEEE 802.11 standard. The adjusted clock takes t_i, the time of the original clock as input and adjusts its value $c_i(t_i)$ according to the following relation:

$$c_i(t_i) = k_i^j * t_i + b_i^j \quad j = 1, 2, \cdots \tag{A.1}$$

Our objective is to synchronize the adjusted clocks of all the nodes in the network by repeatedly adjusting k_i^j and b_i^j ($k_i^j = 1$, $b_i^j = 0$ if $j \leq 2$) at each node when receiving the beacon in the j^{th} BP from the reference node. Compared with IEEE 802.11 TSF, SSTSP has the following desirable features:

- SSTSP achieves better accuracy than IEEE 802.11 TSF via a more sophisticated adjustment scheme in which both the offset and the coefficient parameters are adjusted.
- There is no backwards or other uncontinuous leaps in local clock. This feature is important in some applications. IEEE 802.11 TSF only guarantees that no backwards leaps exist.

The following equations illustrate the clock adjustment of SSTSP:

$$k_i^{j-1} * t_i^j + b_i^{j-1} = k_i^j * t_i^j + b_i^j \tag{A.2}$$

$$c_i((t_i^{j+m})^*) = k_i^j * (t_i^{j+m})^* + b_i^j = (ts_{ref}^{j+m})^* \tag{A.3}$$

$$\frac{t_i^{j-1} - t_i^{j-2}}{ts_{ref}^{j-1} - ts_{ref}^{j-2}} = \frac{(t_i^{j+m})^* - t_i^{j-1}}{(ts_{ref}^{j+m})^* - ts_{ref}^{j-1}} \tag{A.4}$$

$$(ts_{ref}^{j+m})^* = T^{j+m} \tag{A.5}$$

(A.3) follows the argument that the adjusted clock $c_i(t_i)$ is continuous at t_i^j. (A.4) indicates that the adjusted clock of node i is expected to converge to the reference clock at the expected receiving time of the beacon $(j+m)$. Before the convergence, the synchronization error is expected to decrease monotonously. m ($m > 1$) is the parameter of aggressiveness. A larger value of m increases the synchronization latency since the local clock converges slower to the reference node, while it avoids the synchronization error to be increased significantly when the reference node changes. (A.5) establishes the relation of the local clock and the adjusted clock of the reference node based on the linearity of the clocks. As discussed in Section A.3.1, the original clock is regarded as a linear function of real time within a short period of time. The adjusted clock is regarded as linear as long as no adjustment occurs during that period of time. (A.5) follows that the expected emission time of the $(j+m)^{th}$ beacon is T^{j+m}. By solving the equations (A.3)–(A.5)

containing 4 variables k_i^j, b_i^j, $(ts_{ref}^{j+m})^*$ and $(t_i^{j+m})^*$, we get:

$$k_i^j = \frac{(T^{j+m} - (k_i^{j-1} * t_i^j + b_i^{j-1})) * (ts_{ref}^{j-1} - ts_{ref}^{j-2})}{(t_i^{j-1} - t_i^{j-2}) * (T^{j+m} - ts_{ref}^{j-1}) + (t_i^{j-1} - t_i^j) * (ts_{ref}^{j-1} - ts_{ref}^{j-2})}$$

$$b_i^j = k_i^{j-1} * t_i^j + b_i^{j-1} - \frac{(T^{j+m} - (k_i^{j-1} * t_i^j + b_i^{j-1})) * (ts_{ref}^{j-1} - ts_{ref}^{j-2}) * t_i^j}{(t_i^{j-1} - t_i^{j-2}) * (T^{j+m} - ts_{ref}^{j-1}) + (t_i^{j-1} - t_i^j) * (ts_{ref}^{j-1} - ts_{ref}^{j-2})}$$

By repeatedly updating k_i^j and b_i^j using received beacons from the reference node, the local adjusted clock of each node i gradually catches up with the pace of the reference clock and the network is hence synchronized.

A.4.4 Effectiveness of SSTSP

In this section, we provide analytical analysis on the effectiveness of SSTSP by studying the synchronization error bound of SSTSP. Lemma A.1 shows that regardless of the initial value, the adjusted clock of i, c_i, converges to the adjusted timestamp of the reference node ts_{ref}, where $ts_{ref} = t_{ref} + t_p$.

Lemma A.1. *For any node i, its local adjusted clock, c_i, converges to ts_{ref}.*

Proof. Please refer to Section A.8.1 for the detailed proof. □

Apply lemma A.1 and $|ts_{ref} - t_{ref}| < \epsilon$, it is easy to prove that the maximum synchronization error is bounded by 2ϵ, typically $10\mu s$.

Lemma A.2 studies the difference between c_i and ts_{ref} when the reference node changes.

Lemma A.2. *For any node i, let D_i^- and D_i^+ be the difference between c_i and ts_{ref} (ref is the old reference node) before and after the reference node changes, then $D_i^+ < (l+2) * D_i^-$.*

Proof. Please refer to Section A.8.2 for the detailed proof. □

It is further easy to prove that the synchronization error after the change of the reference node is bounded by $\left|\frac{m-l-3}{m}\right| * syn\_err + 2\epsilon$ where syn_err is the synchronization error before the reference node changes. Combining Lemma A.1 and Lemma A.2, we have the following theorem on the synchronization error of SSTSP:

Theorem A.1. *The synchronization error of SSTSP σ can be bounded by $\left|\frac{m-l-3}{m}\right| \cdot 2\epsilon + 2\epsilon$.*

From the above theorem, we can see that by carefully configuring the parameters, the synchronization of SSTSP can be controlled under $10\mu s$.

A.4.5 Traffic and Storage Overhead

In terms of traffic overhead, the number of synchronization beacons emitted in SSTSP is the same as in TSF, while the size of each beacon increases from 56 bytes (24 bytes of preamble and 32 bytes of data) in TSF to 92 bytes (assume 128-bit hash values are used) in SSTSP due to the hash values and the interval index included to secure the beacons.

Besides, each node is required to store its own hash chain. It can either create the hash chain all at once and store all the elements or only store the last element and compute the new element

on demand. [7] proposes a hybrid storage efficient mechanism to reduce storage with a small recomputation penalty: a one-way hash chain with n elements only requires $log_2(n)$ storage and $log_2(n)$ computation to access an element. Each node is also required to buffer temporarily the synchronization beacons received during last 2 BPs. In most cases $300 - 500$ bytes of memory can meet the requirement. We argue that the storage requirement as well as the increase in the beacon size is reasonable considering the gain in performance and security that SSTSP achieves.

A.4.6 Security Analysis

Synchronization beacon forgery and alteration: Attackers may attack the synchronization protocols by forging or modifying synchronization beacons. SSTSP uses the μTESLA scheme to ensure the integrity and authenticity of the synchronization beacons. This prevents the external attackers from modifying or forging the synchronization beacons or impersonating the reference node. A more serious case is when an internal attacker becomes the reference node. In this case, the guard time check serves as a defense line to decrease the effectiveness of the attacks such that the attacker can only forge timestamps whose difference with the receiver's local time is within the guard time, otherwise the beacons containing incorrect timestamps are rejected. We argue that the impact of this attack is limited in that all nodes are synchronized to a virtual clock that may be slightly different to the real clock of the reference node. However, the internal attacker cannot desynchronize the network.

Synchronization beacon replay and relay: Attackers may replay the out-of-date synchronization beacons to deliberately magnify the offset of the time declared in the replayed message and actual time. As a more delicate version of replay attacks, an attacker may firstly jam the channel between the reference node and the victim node A, then delay the synchronization beacons from the reference node and relay it to A later to make A incorrectly estimate the time of the reference node (This attack is referred to as pulse-delay attack in [GvHS05]). The "clock drift check" can thwart these attacks. The argument is that in most cases ($l < 4$), if the beacon is replayed or relayed, since the attacker cannot receive and emit at the same time, we have $|ts^j_{ref} - c_i(t^j_i)| > T_{beacon} > \delta$, where T_{becon} is the transmission time of a beacon including the header and preamble (note that transmitting only the short preamble requires $96\mu s$ in IEEE 802.11b, even in IEEE 802.11g ERP-OFDM, we have $T_{beacon} = 50.7\mu s > \delta$). Even in extreme cases where $l \geq 4$, we can add a number of bits as padding in the beacons (the padding is also included as the HMAC input) to counter the replay or relay attacks such that after padding, we have $T_{beacon} > \delta$.

Deny of Service: Besides the efforts to violate the proper behavior of the synchronization procedure, attackers can disturb the transmission of synchronization beacons at the beginning of each BP or simply generate a massive amount of messages to jam the wireless channel, impeding the traffic including the transmission of time synchronization beacons. Jamming attacks are beyond the scope of our discussion. Actually under jamming attacks all communications in the network are disabled.

A.4.7 Performance Analysis

In this section, we analyze the influence of the following factors on the synchronization protocols.

- Medium access delay: the waiting time at MAC layer before accessing the channel. This delay is non-deterministic in nature ranging from a few microseconds to a few minutes. In SSTSP, timestamping the beacons below MAC layer removes this delay, the most significant factor in the synchronization process.
- Beacon transmission delay: time taken in transmitting the beacon bit-by-bit at the radio of the sender node. This delay is hundreds of microseconds and deterministic in nature depending on the beacon size and the radio speed. [SV04] shows that the beacon transmission delay only adds a few nanoseconds to the synchronization error. Its influence can be annulled by taking into account the delay when adjusting the local clock.
- Beacon propagation delay: time over the wireless link between the sender and receiver node. This delay is typically less than $1\mu s$.

A.4.8 Simulation Study

We further evaluate the performance of SSTSP by simulation. We set the relative clock frequency with respect to real time uniformly distributed in the range of $[1-0.01\%, 1+0.01\%]$, which is the worst clock accuracy allowed by the 802.11 standards. We run the simulation for 1000s for OFDM system with bit-rate of 54Mbps: $w = 30$, $BP = 0.1s$, $l = 1$, the number of nodes $N = 100 - 500$ and the beacon length is 4 slot time. We also set the packet error rate to be 0.01%. We let 5% of the stations leave at BP $k * 200$s ($k > 1$). They return after 50s. In order to simulate the impact of changing the reference node, we let the reference node leave at 300s, 500s and 800s.

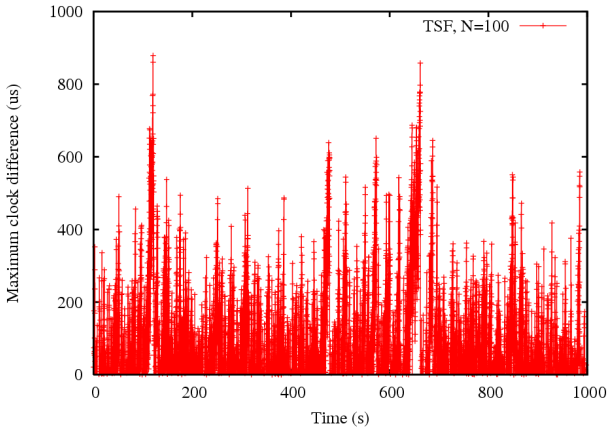

Figure A.2: Maximum clock difference: IEEE 802.11 TSF, 100 nodes

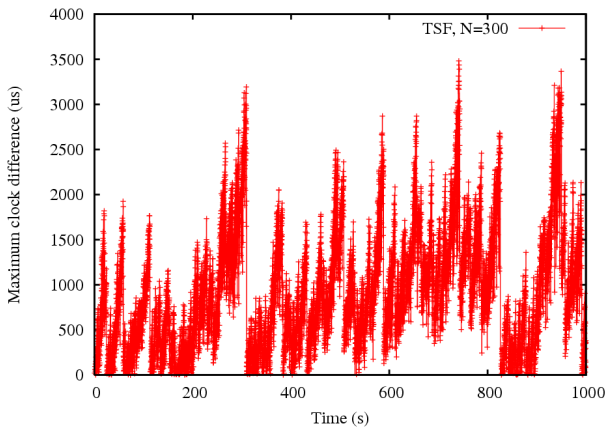

Figure A.3: Maximum clock difference: IEEE 802.11 TSF, 300 nodes

IEEE 802.11 TSF: Figure A.2 and Figure A.3 show the maximum clock drift of IEEE 802.11 TSF in the network of 100 and 300 nodes. We can see the scalability problem due to the *fastest node asynchronization* and the *beacon collision* problem discussed in Section A.2.

SSTSP: Figure A.4 and Figure A.5 show the maximum clock drift of SSTSP in the network of 500 nodes with m=4 and m=1. We can see that SSTSP significantly outperforms IEEE 802.11 TSF by achieving a very precise synchronization with the maximum clock difference below $15\mu s$ after the protocol stabilizes, which is among the best results of currently proposed solutions (see

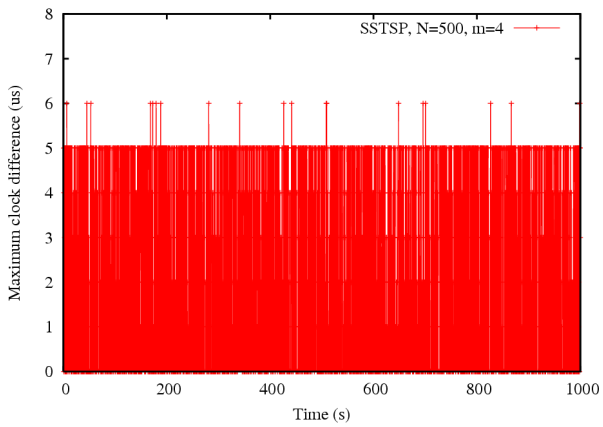

Figure A.4: Maximum clock difference: SSTSP, 500 nodes, m = 4

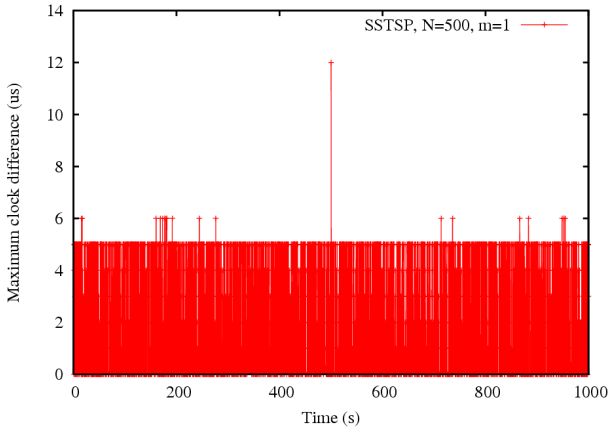

Figure A.5: Maximum clock difference: SSTSP, 500 nodes, m = 1

[ZL05], [SCS04] for their detailed results). Comparing the two figures, we can see that a larger m achieves better performance when the reference node changes. Table A.2 studies the maximum clock difference of different m. We suggest to choose $m = 2$ or 3 to reach a better tradeoff between synchronization accuracy and synchronization latency.

m	Maximum clock difference
1	$12\mu s$
2	$7\mu s$
3	$6\mu s$
4	$6\mu s$
5	$6\mu s$

Table A.2: Maximum clock difference Vs m

Performance under attacks: We also simulate IEEE 802.11 TSF and SSTSP in a hostile environment where an attacker attacks the synchronization protocols during $400s$ to $600s$. The attacker attacks by deliberately sending the synchronization beacons at each BP without delay with an erroneous time value slower than its local clock. We carefully configure the erroneous time values such that they can pass the guard time check in SSTSP. Figure A.6 and Figure A.7 show the synchronization error of IEEE 802.11 TSF and SSTSP under the above attack. The synchronization error of IEEE 802.11 TSF uprises to $20000\mu s$ during the attack. The attacker always wins the contentions thus disabling the fast nodes from emitting beacons. Other protocols improving IEEE 802.11 TSF are also vulnerable to the attack because they depend on the fast nodes to spread the timing information. However, in SSTSP the attacker cannot desynchronize the network even though it manages to become the reference.

A.5 Multi-hop Secure Time Synchronization Procedure

In the rest of the chapter we consider a more challenging task, secure and scalable time synchronization in multi-hop ad hoc networks. Compared with many existing synchronization protocols that form a synchronization tree in the network, our secure multi-hop time synchronization procedure (MSTSP) is fully distributed and server-less. The synchronization is done only locally, without

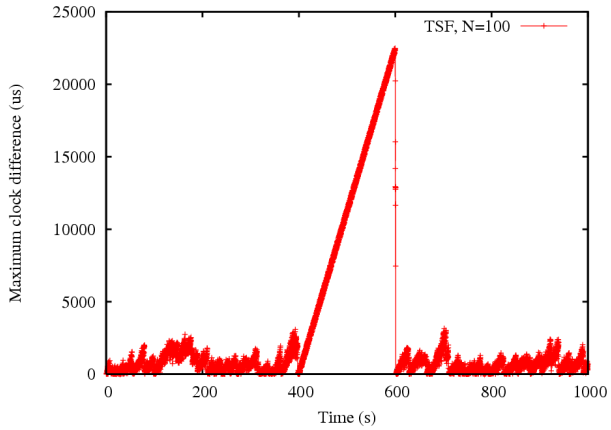

Figure A.6: Maximum clock difference: IEEE 802.11 TSF, 100 nodes, an attacker

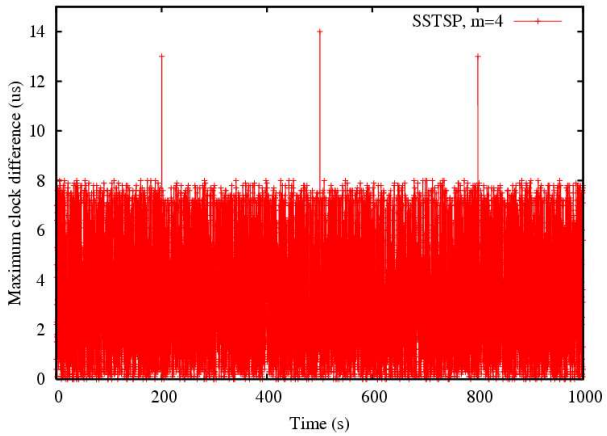

Figure A.7: Maximum clock difference: SSTSP, 500 nodes, an attacker

a global synchronization leader. This feature makes MSTSP robust to topology change and link failure, which happen frequently in multi-hop mobile ad hoc networks.

A.5.1 Overview

In MSTSP, we extend SSTSP, our secure synchronization mechanism for single-hop networks presented in Section A.4, to multi-hop networks by fulfilling the following two tasks:

First, we divide the multi-hop network into single-hop clusters by running SSTSP. The clusters are thus automatically formed and are overlapped by nature. A random delay is added before each synchronization beacon emission to avoid the collision with the beacon emission of neighbor clusters. The intra-cluster synchronization is achieved by SSTSP and each node in the overlapping area randomly chooses the cluster reference node as its reference node and synchronizes to it before it moves out of the transmission range.

We then synchronize all cluster reference nodes to achieve network-wide synchronization. We base our design on the topology redundancy, an intrinsic nature of ad hoc networks that can provide certain level of tolerance to potential attacks. More specifically, we make use of nodes in the overlapping area that belong to more than one clusters (we refer to them as bridge nodes) to relay timestamps among the cluster reference nodes. After collecting the timestamps of the neighbor cluster reference nodes, each cluster reference node synchronizes itself to the fastest neighbor cluster reference node. We take the advantage of the redundancy of ad hoc networks to secure the inter-cluster or network-wide synchronization. In MSTSP, the *time partitioning* problem is avoided by the periodical exchange of time information among neighbor clusters. As a result, the network synchronizes to the fastest cluster reference node.

We give a simple motivating example to illustrate the time synchronization between 2 neighbor cluster reference nodes in MSTSP. Consider Figure A.5.1 where node r_1 and r_2 are two neighbor cluster reference nodes with 3 bridge nodes A, B and C in the overlapping area. Assume r_1 needs to synchronize to r_2 because its clock is slower than that of r_2. Suppose A receives the synchronization beacons from r_1, r_2 at original time t_1, t_2 containing timestamps T_1, T_2. r_1 can estimate the time difference between its adjusted clock and that of r_2 using the original time of A as reference: $\Delta t_{12} = (T_2 - t_2) - (T_1 - t_1)$.

Two points worth further explanation: (1) the adjusted clock of A cannot be used as reference

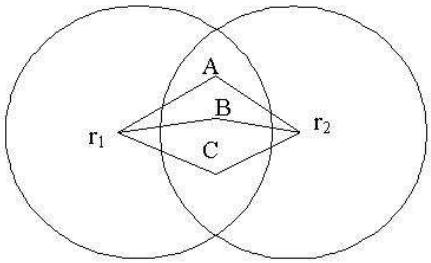

Figure A.8: Inter-cluster synchronization

because it may be adjusted between t_1 and t_2. (2) actually Δt_{12} is measured in local original clock of A, the real time difference measured in the adjusted clock of r_1 is $\Delta t'_{12} = k_1^j \frac{\rho_1}{\rho_A} \Delta t_{12}$. We have $|\Delta t'_{12} - \Delta t_{12}| = |(k_1^j \frac{\rho_1}{\rho_A} - 1)\Delta t_{12}|$. Given that $k_1^j \sim 1$, $\frac{\rho_1}{\rho_A} \sim 1$ and Δt_{12} is in order of $10^1 - 10^2 \mu s$, we can ignore the difference between $\Delta t'_{12}$ and Δt_{12} and use Δt_{12} as the estimation of time difference since $\Delta t'_{12}$ cannot be calculated without the knowledge of ρ_A and ρ_1.

To ensure the integrity of the time values t_1, t_2, T_1, T_2, A puts them in the t_ex (time exchange) message: $< SB_1, t_1, SB_2, t_2, h_A^{n-j}(t\_ex), h_A^{n-j+1}(s_A) >$, where SB_1, SB_2 are received synchronization beacons from r_1, r_2 containing T_1, T_2, $h_A^{n-j}(t\_ex)$ is the HMAC outputs applied to the message with the Hash chain element of A corresponding to current time interval as key, $h_A^{n-j+1}(s_A)$ is the disclosed key for last time interval.

It is possible that A is compromised and thus may forge t_1 and t_2. To counter this attack, r_1 estimates Δt_{12} via different bridge nodes A, B, C. r_1 then eliminates the biased values and sets Δt_{12} to the mean of the rest unbiased values. As a result, if only one of the three nodes is compromised, its impact on the synchronization can be removed. To avoid the collision of t_ex message transmission, each bridge node should desynchronize its t_ex emission (e.g., at time $T_0 + n * BP + BP/2 + d$, where d is randomly chosen in $[0, d_{max}]$). To make MSTSP adaptive to ad hoc networks of different density, each bridge node emits t_ex messages with a pre-configured probability P_s.

A.5.2 MSTSP

Based on the above analysis, we add the following mechanisms to extend SSTSP to multi-hop networks and build our multi-hop secure time synchronization procedure (MSTSP).

- The reference nodes wait a random delay in the range $[0, w] \times aSlotTime$ before emitting the synchronization beacon at each BP to avoid the collision with the reference nodes in neighbor clusters. If a synchronization beacon is heard during the waiting time, the node stop the pending beacon transmission and synchronizes itself to the sender of the beacon.

- We define a parameter P_s for the bridge nodes as the probability of transmitting the t_ex message in each BP. P_s depends on the density of the network and a larger value of P_s increases the robustness of MSTSP to internal attacks at the price of higher traffic overhead. Each bridge node b picks a random number $rand$ from $[0, 1]$ in each BP and compares $rand$ with P_s. If $rand < P_s$, it transmits t_ex containing all the synchronization beacons received from the cluster reference nodes during the last BP as well as the timestamps of the local

original time when it receives them.

$$t\_ex :< SB_1, t_1, SB_2, t_2, ..., SB_n, t_n, h_b^{n-j}(t\_ex), h_b^{n-j+1}(s_b) >$$

Where SB_i is the synchronization beacon emitted by the cluster reference node i, t_i is the local original time when receiving SB_i containing timestamp T_i, $h_b^{n-j}(t\_ex)$ is the HMAC applied to the whole message with the Hash chain element of b corresponding to current time interval as key, $h_b^{n-j+1}(s_b)$ is the disclosed key used in last interval. The transmission is scheduled at $T_0 + n * BP + BP/2 + d$ to asynchronize the transmission of other bridge nodes, where d is randomly chosen in $[0, d_{max}]$.

If a bridge node detects that the difference between any two reference nodes i and j is beyond certain threshold by checking $|(T_i - t_i) - (T_j - t_j)| > 2\beta\Delta\rho_{max}BP$ (β is the tolerant coefficient slightly greater than 1), it notifies other nodes by flooding an signed alert with received beacons as proof. If multiple bridge nodes detect the abnormal difference, the synchronization process is re-initiated.

- Each cluster reference node A collects the synchronization beacons of the neighbor cluster reference nodes via bridge nodes and synchronizes itself to the fastest neighbor reference node by performing the following operations:

  1. For the bridge nodes that send t_ex message in both current BP and last BP, A uses the disclosed keys in t_ex messages received in current BP to verify the authenticity and integrity of the t_ex messages received in last BP. Moreover, since the received t_ex messages contain the beacons of neighbor cluster reference nodes, A can use the disclosed keys in the beacons contained in t_ex messages received in current BP to verify the beacons contained in t_ex messages received in last BP. Note that A cannot directly get the disclosed keys of its neighbor cluster reference nodes since A cannot hear them. However, A can obtain them via bridge nodes in that the synchronization beacons are included in the t_ex messages. By doing so, A thus collect a number of verified t_ex message containing verified beacons sent by neighbor cluster reference nodes.
  2. A then uses the timestamps in these verified messages to synchronize its local adjusted clock to the adjusted clock of the fastest cluster reference node as illustrated in the example. To this end, A collects all the timestamps in the verified t_ex messages containing verified synchronization beacons among which T_r, t_b^r, T_A, t_b^A are respectively the timestamp in the beacon of the cluster reference r, the original time when the bridge node b receives the beacon from r, the timestamp in the beacon of A, the original time when b receives the beacon from A. A then computes $\Delta t_b^r = (T_r - t_b^r) - (T_A - t_b^A)$ which indicates the approximate time difference between A and r in last BP estimated via b. By collecting the time difference Δt_r^b from different bridge nodes b and eliminating the outliers, A thus obtains the estimated time difference with r, Δt_r by averaging them. A then picks $\Delta t^* = max(\Delta t_r)$, the largest value from the time differences with all neighbor cluster reference node r and adds Δt^* to its original clock t_A and adjusted clock c_A if $\Delta t^* > 0$.

In the following lemma, we show that in the stablized case, SSTSP is applicable in MSTSP to achieve intra-cluster synchronization.

Lemma A.3. *SSTSP is applicable in MSTSP to achieve intra-cluster synchronization in the stablized case.*

Proof. Please refer to Section A.8.3 for the detailed proof. □

Based on lemma A.3, we have the following result on the effectiveness of MSTSP

Theorem A.2. *In stablized cases, the time synchronization error of MSTSP can be bounded by* $2NBP\Delta\rho'_{max} + 2\epsilon$*, where* N *is the upper bound of the synchronization route (in number of hops) mentioned in Lemma A.3,* $\Delta\rho'_{max} = max(\rho'_i - \rho'_j) \sim 10^{-6}$.

Proof. Please refer to Section A.8.4 for the detailed proof. □

A.5.3 Security Analysis

In section A.4.6, we have performed the security analysis of SSTSP, showing that SSTSP is powerful enough to prevent single-hop networks or clusters from being desynchronized by both malicious external and internal attackers. In this section we focus on the attack resistance of inter-cluster synchronization in MSTSP to internal attacks. As attack examples, an internal attacker may forge t_ex messages with incorrect receiving time values of the synchronization beacons from correspondent cluster reference nodes to desynchronize them. Two attackers may collaborate to wormwhole a cluster reference synchronization beacon to another cluster reference node far away. As another example, when becoming cluster reference node, an internal attacker may refuse to synchronize to its neighbor cluster reference node even the latter is fastest. MSTSP provides two defense lines to ensure the inter-cluster synchronization against these malicious attacks:

- MSTSP takes the advantage of the topology redundancy of ad hoc networks to provide multiple synchronization paths via different bridge nodes to thwart the attacks to inter-cluster synchronization.
- The compromised or desynchronized cluster reference nodes can be detected by the bridge nodes by emitting alert messages when they detect that the clock difference is beyond the threshold. The synchronization procedure is then re-initiated.

In our approach, a collision of Hash chain elements may cause a security flaw that two or more nodes share their keys to secure their synchronization beacons. If one of them are malicious, it can impersonate others without being detected. Hereby we perform an analysis on the collision probability P_c: let A be the number of Hash chain elements in the element space, for m-bit Hash chains, $A = 2^m$; let N be the number of nodes in the network; let n be the length of the hash chains; let M be the total number of Hash chain elements, $M = N * n$. We thus have

$$\begin{aligned} P_c &= 1 - Prob\ (\text{no collision}) = 1 - \frac{C_A^M * M!}{A^M} = 1 - \frac{A!}{(A-M)!A^M} \\ &= 1 - \frac{A-1}{A}\frac{A-2}{A}\cdots\frac{A-(M-1)}{A} = 1 - \left(1-\frac{1}{A}\right)\left(1-\frac{2}{A}\right)\cdots\left(1-\frac{M-1}{A}\right) \\ &< 1 - \left(1-\frac{M-1}{A}\right)^{(M-1)} \sim 1 - \left(1-\frac{(M-1)^2}{A}\right) \sim \frac{M^2}{A}(M \ll A) \end{aligned}$$

Using 128-bit Hash chains in an ad hoc network of 1000 nodes using Hash chain containing 10^6 elements, we have $P_c < 10^{-28}$, which can be regarded as negligible.

A.5.4 Performance Evaluation

We evaluate MSTSP by NS-2. The clock parameters and the SSTSP parameters are the same as those in Section A.4.8. The number of mobile nodes is 200 unless specifically stated. Each of them is randomly located in a $1000m \times 1000m$ field with a transmission range of 250m. All nodes move according to the random way-point model with maximum speed 5m/s with the pause time 50s. P_s is set to 0.6 unless specifically stated. We measure 3 metrics to evaluate the performance of MSTSP: maximum synchronization error, traffic overhead and synchronization latency.

Maximum synchronization error: IEEE 802.11 TSF is not scalable for multi-hop ad hoc networks. In the network of 200 nodes, the maximum synchronization error is already nearly $600\mu s$ (Figure A.9). In contrast, MSTSP shows much better performance. As shown in Figure A.10 and Table 3, the maximum synchronization error of MSTSP is about $61\mu s$ in the same scenario. We further vary the network size and simulate MSTSP in these configurations. The result is shown in Table 3. The average synchronization error of MSTSP is $30\mu s$-$50\mu s$. ASP is reported to achieve $100\mu s$-$200\mu s$ in terms of synchronization error. The average synchronization error of the mechanism proposed in [RK04] ranges from $50\mu s$ to $200\mu s$ depending on the network size and other parameters. To our knowledge, the accuracy of MSTSP is among the best of currently proposed solutions.

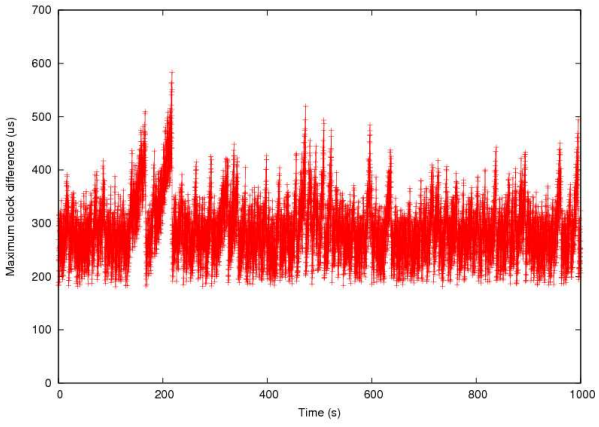

Figure A.9: Maximum clock difference, IEEE

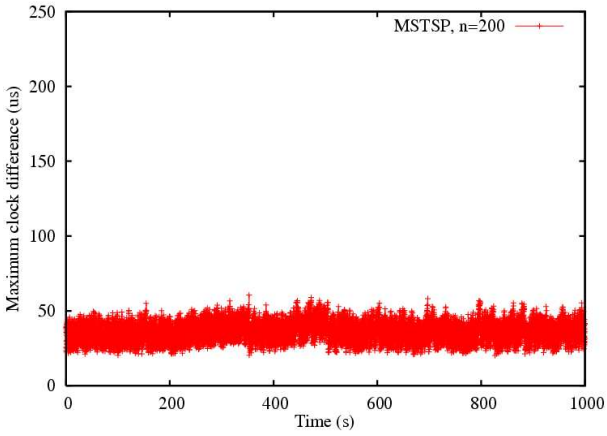

Figure A.10: Maximum clock difference, MSTSP

802.11 TSF

Number of nodes	Maximum synchronization error	Average synchronization error
100	$55\mu s$	$31\mu s$
200	$61\mu s$	$36\mu s$
500	$83\mu s$	$49\mu s$

Table A.3: Synchronization error: MSTSP

Traffic overhead: Traffic overhead is a crucial issue for time synchronization protocols in resource constrained environments. Some traditional synchronization mechanisms require each node to diffuse its local time values each synchronization period, resulting $o(n^2)$ traffic overhead. IEEE 802.11 TSF is very efficient in traffic cost, but its synchronization error in multi-hop ad hoc networks may uprise unboundedly. Figure A.11 shows the traffic overhead (number of synchronization

beacons plus t_ex messages transmitted each BP) of MSTSP as P_s ranges from 0 to 1. When $P_s = 0$, no synchronization beacon is relayed in t_ex messages, the traffic overhead equals to that of IEEE 802.11 TSF. When $P_s = 1$, all the bridge nodes relay the synchronization beacons in their t_ex messages. MSTSP is significantly more efficient than traditional approaches. Compared with IEEE 802.11 TSF ($P_s = 0$), MSTSP generates 2-5 times more overhead when P_s ranges from 0.3-0.7. We argue that the overhead of MSTSP is acceptable considering the improvement of performance in terms of synchronization precision and synchronization latency.

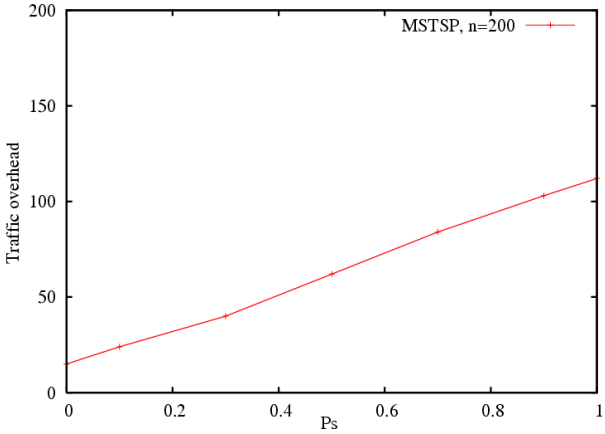

Figure A.11: Traffic overhead, MSTSP, 200 nodes

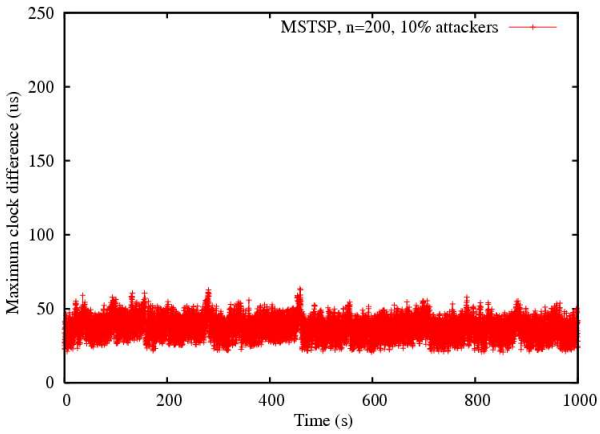

Figure A.12: Maximum synchronization error, MSTSP, 200 nodes, 10% attackers

Synchronization latency: In order to simulate the synchronization latency of MSTSP, we attribute an initial clock offset between $[-200\mu s, 200\mu s]$ to each node and measure the time between the beginning of the simulation and the time when the maximum synchronization error decreases under $100\mu s$. The result shows that with 100, 200 and 500 nodes in the network, the synchronization latency is under $10\mu s$. Besides, once the network is synchronized, MSTSP shows good stability without abrupt peaks in the maximum synchronization error as in IEEE 802.11 TSF.

Performance under attacks: Finally we study the performance of MSTSP in a hostile environment where 10% of nodes are compromised and forge the receiving time values in the t_ex messages they emit when becoming bridge nodes. Figure A.12 shows the maximum synchronization error of the rest 90% nodes with $P_s = 0.6$. We can see that with a proper P_s value, MSTSP can maintain the network synchronized even in hostile environments under malicious attacks. However, as discussed earlier in the chapter, such attacks may cause detrimental effect on the performance of IEEE 802.11 TSF and other insecure synchronization protocols.

A.6 Discussion

It is interesting that our approach uses μTESLA to secure the synchronization process while μTESLA itself requires a loose synchronization. It is not contradictory in that the bootstrapping phase allow the new arriver to acquire initial synchronization and enables the application of one-way hash chains to secure the time synchronization procedure in the synchronization phase. Once the hash chain scheme is established and the synchronization is secured, we can continue to use the hash chain scheme based on the synchronized time to further maintain the time synchronization.

In this chapter, we focus on detecting malicious attacks and preventing the network from being desynchronized by malicious nodes using erroneous time values. However, we do not provide recovery mechanisms when an attack is detected. We do not address how to eliminate the attackers either. We leave them for our future work.

In our approach, the key chain may be used up quickly. In this case, nodes need to re-issue new hash chains for μTESLA. To achieve this, nodes can broadcast the authenticated last element of the new hash chain to be used when the current chain is to be used up within a few time intervals. Better mechanisms include using 2-dimensional hash chain or interleaved hash chain to achieve seamless hash chain renewal. [Jak02] addresses the hash chain renewal issue by proposing the infinite hash chain scheme.

A.7 Conclusion

In this chapter, we address the security and the scalability problems of time synchronization protocols in ad hoc networks. For single-hop ad hoc networks, we propose SSTSP, a scalable and secure time synchronization procedure that significantly improves the performance of IEEE 802.11 TSF. We base SSTSP on one-way Hash chain, a lightweight mechanism to ensure the authenticity and the integrity of the synchronization beacons. The "clock drift check" is proposed to counter replay/delay attacks. We then extend our efforts to the multi-hop case. We propose MSTSP, a secure and scalable time synchronization mechanism based on SSTSP for multi-hop ad hoc networks. In MSTSP, the multi-hop network is automatically divided into single-hop clusters. The secure intra-cluster synchronization is achieved by SSTSP and the secure inter-cluster synchronization is achieved by exchanging synchronization beacons among cluster reference nodes via bridge nodes. The proposed synchronization mechanisms are fully distributed without a global synchronization leader. We further perform analytical studies and simulations on the proposed approaches. The results show that SSTSP can synchronize single-hop networks with the maximum synchronization error under $20\mu s$ and MSTSP $55\mu s$-$85\mu s$ for multi-hop networks, which are, to the best of our knowledge, among the best results of currently proposed solutions for single-hop and multi-hop ad hoc networks. Meanwhile, our approaches can maintain the network synchronized even in hostile environments.

A.8 Proofs

This section completes the detailed proofs omitted from the main text.

A.8.1 Proof of Lemma A.1

Let D_i^n be the difference between $c_i(t_i^n)$ and ts_{ref}^n when receiving the n^{th} beacon, i.e.,

$$D_i^n = c_i(t_i^n) - ts_{ref}^n$$

Let $(n+q) * BP + d_{n+q}$ be the time when the reference node emits the $(n+q)^{th}$ beacon ($q \geq 1$), where d_{n+q} is the time elapsed between the scheduled emission time of the beacon and its actual

emission time. The timestamp in the beacon is adjusted at node i by adding t_p to ts_{ref}^{n+q}:

$$ts_{ref}^{n+q} = (n+q) * BP + d_{n+q} + t_p$$

By (A.4) we have:

$$k_i^n * (t_i^{n+m})^* + b_i^n = (ts_{ref}^{n+m})^* = (n+m) * BP + t_p \tag{A.6}$$

Apply (A.1) at t_i^n and t_i^{n+1} we get:

$$c_i(t_i^n) = k_i^n * t_i^n + b_i^n = ts_{ref}^n + D_i^n = n * BP + d_n + t_p + D_i^n \tag{A.7}$$

$$c_i(t_i^{n+1}) = k_i^n * t_i^{n+1} + b_i^n = ts_{ref}^{n+1} + D_i^{n+1} = (n+1) * BP + d_{n+1} + t_p + D_i^{n+1} \tag{A.8}$$

By the linearity of the clock we have:

$$\frac{(t_i^{n+m})^* - t_i^n}{(ts_{ref}^{n+m})^* - ts_{ref}^n} = \frac{(t_i^{n+m})^* - t_i^{n+1}}{(ts_{ref}^{n+m})^* - ts_{ref}^{n+1}} \tag{A.9}$$

Combining (A.6)–(A.9), we get:

$$\frac{D_i^{n+1}}{D_i^n} = \frac{(m-1) * BP - d_{n+1}}{m * BP - d_n} < \begin{cases} \frac{d}{m*BP-d} & m = 1 \\ \frac{(m-1)*BP}{m*BP-d} & m > 1 \end{cases}$$

where $d = max(d_j)$, $(j > 1)$. Recursively we get:

$$\frac{D_i^{n+q}}{D_i^n} < \begin{cases} (\frac{d}{m*BP-d})^q & m = 1 \\ (\frac{(m-1)*BP}{m*BP-d})^q & m > 1 \end{cases}$$

Given any synchronization error threshold Δ and D_i^n, after $[log_{\frac{d}{(m*BP-d)}} \frac{\Delta}{D_i^n}]$ BPs (if $m = 1$) or $[log_{\frac{(m-1)*BP}{(m*BP-d)}} \frac{\Delta}{D_i^n}]$ BPs (if $m > 1$), the difference between the local adjusted clock of node i and the clock of the reference node will drop below the threshold. The adjusted clock thus converges to ts_{ref}.

A.8.2 Proof of Lemma A.2

It takes $(l+3)$ BPs before node i can re-adjust its local clock to the new reference clock: during the first $(l+1)$ BPs, the new reference node is elected via contention; during the following two BPs, each node validates the timestamp sent by the new reference node in previous BP and gets enough validated timestamps to adjust its local clock. Let $t_{ref}^n = n * BP + d_n$[3] be the time when the last beacon is emitted by the old reference node. The beacon is received by i at local unadjusted time t_i^n. The difference between $c_i(t_i^n)$ and ts_{ref}^n is D_i^-. Let $t_{ref}^{n+l+3} = (n+l+3) * BP + d_{n+l+3}$ be the local time of the old reference node when the new reference node emits its beacon in the $(l+3)^{th}$ BP with which node i begins to adjust its local clock to the new reference clock. The difference between $c_i(t_i^{n+l+3})$ and ts_{ref}^{n+l+3} is D_i^+. Between ts_{ref}^n and ts_{ref}^{n+l+3}, the synchronization error cannot be controlled since no adjustment is done during this period. After ts_{ref}^{n+l+3} all the nodes synchronize to the new reference node, and the synchronization error decreases. We prove

[3] d_n is defined the same as in lemma A.1.

in the following that $D_i^+ < (l+2) * D_i^-$.

By (A.4) we get:

$$k_i^n * (t_i^{n+m})^* + b_i^n = (ts_{ref}^{n+m})^* = (n+m) * BP + t_p \tag{A.10}$$

Apply (A.1) at t_i^n and t_i^{n+l+3} we get:

$$c_i(t_i^n) = k_i^n * t_i^n + b_i^n = ts_{ref}^n + D_i^- = n * BP + d_n + t_p + D_i^- \tag{A.11}$$

$$c_i(t_i^{n+l+3}) = k_i^n * t_i^{n+l+3} + b_i^n = ts_{ref}^{n+l+3} + D_i^+ = (n+l+3) * BP + d_{n+l+3} + t_p + D_i^+ \tag{A.12}$$

By the linearity of the clock we have:

$$\frac{(t_i^{n+m})^* - t_i^n}{(ts_{ref}^{n+m})^* - ts_{ref}^n} = \frac{(t_i^{n+m})^* - t_i^{n+l+3}}{(ts_{ref}^{n+m})^* - ts_{ref}^{n+l+3}} \tag{A.13}$$

Combining (A.10)–(A.13), we get

$$\frac{D_i^+}{D_i^-} = \frac{(m-l-3)BP - d_{n+l+3}}{mBP - d_n}$$

Note that $d_n, d_{n+l+3} \ll BP$, we have

$$\frac{D_i^+}{D_i^-} = \frac{m-l-3}{m} + o(1)$$

We can see from the proof that the optimal value of m in terms of the performance when the reference node changes is $l+3$ in that the adjusted clock of each node is expected to converge to the same time when a new round of synchronization begins. Even in the worst case where $m = 1$, D_i^+ can be bounded by $(l+2) * D_i^-$.

A.8.3 Proof of Lemma A.3

In the stablized case, each cluster reference node A synchronizes via a synchronization route composed of a suite of cluster reference nodes to the fastest cluster reference node r_n:

$$A, r_1, r_2, ..., r_{n-1}, r_n$$

On this route, r_{i-1} adjusts its clock once each BP according to the timestamps in the beacons emitted by r_i. Since the local adjusted clock of r_n can be regarded as linear in that no adjustment is performed at the fastest cluster reference node in MSTSP, the adjusted clock of r_{n-1} can be regarded as linear because r_{n-1} adjusts its clock c_{n-1} by adding approximately the same time difference $(\rho'_n - \rho'_{n-1}) * BP$ in each BP.

Recursively we can prove that the local adjusted time of A, c_A, can be regarded as linear. This makes (A.5) hold and justifies that SSTSP can be applied in the multi-hop case for intra-cluster time synchronization.

In reality, the mobility of the nodes and the dynamic nature of clusters increase the synchronization error of intra-cluster in a multi-hop network.

A.8.4 Proof of Theorem A.2

We consider node i who synchronizes via a synchronization route R to the fastest cluster reference node r_n:

$$r_1, r_2, \cdots, r_{n-1}, r_n \quad 1 \leq n \leq N+1$$

In an m-hop ad hoc network, we have $N \sim O(m)$. We now study the synchronization error between two reference nodes in neighbor clusters r_j, r_{j+1}. According to MSTSP, in the k^{th} BP, r_j receives the synchronization beacon of r_{j+1} via bridge nodes containing the disclosed hash element with which it checks the integrity and authenticity of the beacon sent by r_{j+1} in the $(k-1)^{th}$ BP and adjusts its clock accordingly, thus the difference of the adjusted clock of r_j and r_{j+1} can be bounded by $2BP\Delta\rho'_{max}$:

$$|c_j(t) - c_{j+1}(t)| < 2BP\Delta\rho'_{max}$$

Recursively we get

$$|c_1(t) - c_n(t)| < 2nBP\Delta\rho'_{max}$$

Since r_n is the fastest reference nodes, we have

$$0 < c_1(t) - c_n(t) < 2nBP\Delta\rho'_{max}$$

Apply Lemma A.1, we have

$$|c_i(t) - c_1(t)| < \epsilon$$

It follows that

$$2nBP\Delta\rho'_{max} - \epsilon < c_i(t) - c_n(t) < 2nBP\Delta\rho'_{max} + \epsilon$$

which holds for each node in the network. For any two nodes A and B, applying the above inequality leads to

$$|c_A(t) - c_B(t)| < 2NBP\Delta\rho'_{max} + 2\epsilon$$

Bibliography

[80299] *ANSI/IEEE Standard 802.11*, 1999.

[AB03] T. Alpcan and T. Basar. A game theoretic approach to decision and analysis in network intrusion detection. In *Proc. 42nd IEEE Conference on Decision and Control (CDC 2003)*, volume 3, pages 2595–2600, Dec. 2003.

[AB04] T. Alpcan and T. Basar. A game theoretic analysis of intrusion detection in access control systems. *Proc. 43rd IEEE Conference on Decision and Control (CDC 2004)*, 2:1568–1573, Dec. 2004.

[ABD06] T. Alpcan, T. Basar, and S. Dey. A power control game based on outage probabilities for multicell wireless data networks. *IEEE Transactions on Wireless Communications*, 5(4):890–899, April 2006.

[AC] E. Accinelli and E.J.S. Carrera. Contraction of best response functions and uniqueness of nash-cournot equilibrium.

[ADBA04] A. Agah, S.K. Das, K. Basu, and M. Asadi. Intrusion detection in sensor networks: a non-cooperative game approach. *Proc. 3rd IEEE International Symposium on Network Computing and Applications, 2004. (NCA 2004)*, pages 343–346, Aug. 2004.

[AEAJ03] E. Altman, R. El-Azouzi, and T. Jimenez. Slotted aloha as a stochastic game with partial information. In *Proc. 1st International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt 03)*, March 2003.

[BH03] L. Buttyán and J.-P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks Application*, 8(5):579–592, 2003.

[BH07] Levente Buttyan and Jean-Pierre Hubaux. *Security and Cooperation in Wireless Networks*. Cambridge University Press, 2007.

[Bha97] R. Bhandari. Optimal physical diversity algorithms and survivable networks. In *Proc. 2nd IEEE Symposium on Computers and Communications, (ISCC 97)*, pages 433–441, Jul 1997.

[BHO+02] S. Bohacek, J.P. Hespanha, K. Obraczka, J. Lee, and C. Lim. Enhancing security via stochastic routing. In *Proc. 11th International Conference on Computer Communications and Networks (ICCCN 02)*, pages 58–62, Oct. 2002.

[Bia00] G. Bianchi. Performance analysis of the ieee 802.11 distributed coordination function. *IEEE Journal on Selected Areas in Communications (JSAC)*, 18(3):535–547, Mar 2000.

[BSS02] J. P. Brumbaugh-Smith and D. R. Shier. Minimax models for diverse routing. *INFORMS Journal on Computing*, 14(1):81–95, 2002.

[BT97] D. Bertsekas and J. N. Tsitsiklis. *Parallel and Distributed Compuation: Numerical Methods*. Athena Scientific, 1997.

[CCH07] M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormhole-based anti-jamming techniques in sensor networks. *IEEE Transactions on Mobile Computing*, 6(1):100–114, Jan. 2007.

[CGAH05] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux. On selfish behavior in csma/ca networks. In *Proc. IEEE INFOCOM 2005*, volume 4, pages 2513–2524, March 2005.

[CL07a] L. Chen and J. Leneutre. A game theoretic framework of distributed power and rate control in ieee 802.11 wlans. In *Proc. 15th IEEE International Conference on Network Protocols (ICNP 07)*, pages 338–339, Oct. 2007.

[CL07b] L. Chen and J. Leneutre. On the power and rate control in ieee 802.11 wlans - a game theoretical approach. In *Proc. 16th International Conference on Computer Communications and Networks (ICCCN 07)*, pages 450–456, Aug. 2007.

[CL07c] L. Chen and J. Leneutre. Selfishness, not always a nightmare: Modeling selfish mac behaviors in wireless mobile ad hoc networks. In *Proc. ICDCS 2007*, pages 16–23, Jun. 2007.

[CL07d] L. Chen and J. Leneutre. Toward secure and scalable time synchronization in ad hoc networks. *Computer Communication*, 30(11-12):2453–2467, 2007.

[CL08] L. Chen and J. Leneutre. A game theoretic framework of distributed power and rate control in IEEE 802.11 WLANs. *IEEE Journal on Selected Areas in Communications (JSAC)*, 26(7):1128–1137, 2008.

[EAV05] D. Kumar E. Altman, A. Kumar and R. Venkatesh. Cooperative and non-cooperative control in ieee 802.11 wlans. In *Proc. 19th International Teletraffic Congress (ITC-19)*, 2005.

[EGE02] J. Elson, L. Girod, and D. Estrin. Fine-grained network time synchronization using reference broadcasts. *SIGOPS Operating System Review*, 36(SI):147–163, 2002.

[FH06] M. Felegyhazi and J.-P. Hubaux. Game theory in wireless networks: A tutorial. Technical report, EPFL, 2006.

[FHB06] M. Felegyhazi, J.-P. Hubaux, and L. Buttyan. Nash equilibria of packet forwarding strategies in wireless ad hoc networks. *IEEE Transactions on Mobile Computing*, 5(5):463–476, May 2006.

[GKS03] S. Ganeriwal, R. Kumar, and M. B. Srivastava. Timing-sync protocol for sensor networks. In *Proc. 1st International Conference on Embedded Networked Sensor Systems (SenSys 03)*, pages 138–149, New York, NY, USA, 2003. ACM.

[GvHS05] S. Ganeriwal, S. Čapkun, C. Han, and M. B. Srivastava. Secure time synchronization service for sensor networks. In *Proc. 4th ACM workshop on Wireless security (Wise 05)*, pages 97–106, New York, NY, USA, 2005. ACM.

[HA04] M. Hayajneh and C.T. Abdallah. Distributed joint rate and power control game-theoretic algorithms for wireless data. *IEEE Communications Letters*, 8(8):511–513, Aug. 2004.

[HB01] J.P. Hespanha and S. Bohacek. Preliminary results in routing games. In *Proc. 20th American Control Conference (ACC 01)*, volume 3, pages 1904–1909 vol.3, 2001.

[HFLY03] Y. Huang, W. Fan, W. Lee, and P.S. Yu. Cross-feature analysis for detecting ad-hoc routing anomalies. *Proc. IEEE ICDCS 2003*, pages 478–487, May 2003.

[HN06] T.E. Hunter and A. Nosratinia. Diversity through coded cooperation. *IEEE Transactions on Wireless Communications*, 5(2):283–289, February 2006.

[HPJ02] Y. Hu, A. Perrig, and D. B. Johnson. Ariadne: a secure on-demand routing protocol for ad hoc networks. In *Proc. MobiCom 02*, pages 12–23, 2002.

[HRGD05] M. Heusse, F. Rousseau, R. Guillier, and A. Duda. Idle sense: an optimal access method for high throughput and fairness in rate diverse wireless lans. *SIGCOMM Computing and Communication Review*, 35(4):121–132, 2005.

[HVB01] G. Holland, N. Vaidya, and P. Bahl. A rate-adaptive mac protocol for multi-hop wireless networks. In *Proc. MobiCom 01*, pages 236–251, New York, NY, USA, 2001. ACM.

[Jak02] M. Jakobsson. Fractal hash sequence representation and traversal. In *Proc. IEEE International Symposium on Information Theory (ISIT 02)*, 2002.

[JHHN04] M. Janani, A. Hedayat, T.E. Hunter, and A. Nosratinia. Coded cooperation in wireless communications: Space-time transmission and iterative decoding. *IEEE Transactions on Signal Processing*, 52(2):362–371, February 2004.

[JK02] Y. Jin and G. Kesidis. Equilibria of a noncooperative game for heterogeneous users of an aloha network. *IEEE Communications Letters*, 6(7):282–284, Jul 2002.

[JS07] J.J. Jaramillo and R. Srikant. DARWIN: Distributed and adaptive reputation mechanism for wireless ad-hoc networks. In *Proc. ACM MobiCom*, Montreal, Canada, September 2007.

[KAMG05] A. Kumar, E. Altman, D. Miorandi, and M. Goyal. New insights from a fixed point analysis of single cell ieee 802.11 wlans. In *Proc. IEEE INFOCOM 2005*, volume 3, pages 1550–1561 vol. 3, March 2005.

[KL03] M. Kodialam and T.V. Lakshman. Detecting network intrusions via sampling: a game theoretic approach. In *Proc. IEEE INFOCOM 2003*, volume 3, pages 1880–1889 vol.3, March-3 April 2003.

[KMR05] G. Khanna, A. Masood, and C. N. Rotaru. Synchronization attacks against 802.11. In *Workshop of the 12th Networks and Distributed Systems Symposium (NDSS 05)*, Feb. 2005.

[KMT98] F.P. Kelly, A.K. Maulloo, and D.K.H. Tan. Rate control in communication networks: Shadow prices, proportional fairness and stability. *Journal of the Operational Research Society*, 49:237–252, March 1998.

[KRMK06] M. Kefayati, H. R. Rabiee, S. G. Miremadi, and A. Khonsari. Misbehavior resilient multi-path data transmission in mobile ad-hoc networks. In *Proc. the 4th ACM workshop on Security of ad hoc and sensor networks (SASN 06)*, pages 91–100, New York, NY, USA, 2006. ACM.

[KV03] P. Kyasanur and N.H. Vaidya. Detection and handling of mac layer misbehavior in wireless networks. In *Proc. International Conference on Dependable Systems and Networks (DSN 2003)*, pages 173–182, June 2003.

[LCM06] Y. Liu, C. Comaniciu, and H. Man. Modelling misbehaviour in ad hoc networks: a game theoretic approach for intrusion detection. *International Journal of Security and Networks (IJSN)*, 1(3/4), 2006.

[Lib] L. Libman. *Noncooperative Failure Recovery in Large-Scale Networks*. PhD thesis, Technion Israel Institute of Technology.

[LKP07] M. Li, I. Koutsopoulos, and R. Poovendran. Optimal jamming attacks and network defense policies in wireless sensor networks. In *Proc. IEEE INFOCOM 2007*, pages 1307–1315, May 2007.

[LLF04] W. Lou, W. Liu, and Y. Fang. Spread: enhancing data confidentiality in mobile ad hoc networks. In *Proc. IEEE INFOCOM 2004*, volume 4, pages 2404–2413, March 2004.

[LLG06] L. Lai, K. Liu, and H. El Gamal. The three-node wireless network: Achievable rates and cooperation strategies. *IEEE Transactions on Information Theory*, 52(3):805–828, March 2006.

[LMR05] P.P.C. Lee, V. Misra, and D. Rubenstein. Distributed algorithms for secure multipath routing. In *Proc. IEEE INFOCOM 2005*, volume 3, pages 1952–1963 vol. 3, March 2005.

[LN05] G. Lin and G. Noubir. On link layer denial of service in data wireless lans: Research articles. *Wireless Communication and Mobile Computing*, 5(3):273–284, 2005.

[LSM00] W. Lee, S. J. Stolfo, and K. W. Mok. Adaptive intrusion detection: A data mining approach. *Artificial Intelligence Review*, 14(6):533–567, 2000.

[LTW04] J.N. Laneman, D.N.C. Tse, and G.W. Wornell. Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *IEEE Transactions on Information Theory*, 50(12):3062–3080, December 2004.

[LW03] J.N. Laneman and G.W. Wornell. Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks. *IEEE Transactions on Information Theory*, 49(10):2415–2425, October 2003.

[LZ03] T. Lai and D. Zhou. Efficient,and scalable ieee 802.11 ad-hoc-mode timing synchronization function. In *Proc. 17th International Conference on Advanced Information Networking and Applications (AINA 03)*, pages 318–323, March 2003.

[MMV94] J.K. MacKie-Mason and H.R. Varian. Pricing the Internet. In B. Kahin and J. Keller, editors, *Public Access to the Internet*. Prentice-Hall, Englewood Cliffs, NJ, 1994.

[MP02] C. Manikopoulos and S. Papavassiliou. Network intrusion and fault detection: a statistical anomaly approach. *IEEE Communications Magazine*, 40(10):76–82, Oct 2002.

[MQ05] P. Marbach and Y. Qiu. Cooperation in wireless ad hoc networks: A market-based approach. *IEEE/ACM Transactions on Networking*, 13(6):1325–1338, December 2005.

[MSP00] R.K. Mallik, R.A. Scholtz, and G.P. Papavassilopoulos. Analysis of an on-off jamming situation as a dynamic game. *IEEE Transactions on Communications*, 48(8):1360–1373, Aug 2000.

[MST98] M. Meneganti, F.S. Saviello, and R. Tagliaferri. Fuzzy neural networks for classification and detection of anomalies. *IEEE Transactions on Neural Networks*, 9(5):848–861, Sep 1998.

[MV65] W. Mayeda and M. Van Valkenburg. Properties of lossy communication nets. *IEEE Transactions on Circuits and Systems*, 12(3):334–338, 1965.

[MW03] A.B. MacKenzie and S.B. Wicker. Stability of multipacket slotted aloha with selfish users and perfect information. In *Proc. IEEE INFOCOM 2003*, volume 3, pages 1583–1590 vol.3, March-3 April 2003.

[Mye91] R.B. Myerson. *Game Theory: Analysis of Conflict*. Harvard University Press, Cambridge, MA, 1991.

[NHH04] A. Nosratinia, T.E. Hunter, and A. Hedayat. Cooperative communication in wireless networks. *IEEE Communications Magazine*, 42(10):74–80, October 2004.

[NTP] *NTP Project, http://www.eecis.udel.edu/m̃ills/ntp.html*.

[OR94] M. J. Osborne and A. Rubinstein. *A Course in Game Theory*. MIT Press, 1994.

[Pap01] C. Papadimitriou. Algorithms, games and the Internet. In *Proc. ACM Symposium on the Theory of Computing (STOC)*, Heraklion, Greece, July 2001.

[PH03] P. Papadimitratos and Z.J. Haas. Secure link state routing for mobile ad hoc networks. In *Proc. Symposium on Applications and the Internet Workshops, 2003*, pages 379–383, Jan. 2003.

[PH06] P. Papadimitratos and Z.J. Haas. Secure data communication in mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 24(2):343–356, Feb. 2006.

[PHS02] P. Papadimitratos, Z. J. Haas, and E. G. Sirer. Path set selection in mobile ad hoc networks. In *Proc. ACM MobiHoc 02*, pages 1–11, New York, NY, USA, 2002.

[PP06] A. Patcha and J.-M. Park. A game theoretic formulation for intrusion detection in mobile ad hoc networks. *International Journal of Network Security*, 2(2):146–152, 2006.

[PST+02] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. Spins: security protocols for sensor networks. *Wireless Networks*, 8(5):521–534, 2002.

[QCJS03] D. Qiao, S. Choi, A. Jain, and K. G. Shin. Miser: an optimal low-energy transmission strategy for ieee 802.11a/h. In *Proc. MobiCom 03*, pages 161–175, New York, NY, USA, 2003. ACM.

[RB06] A. Rachedi and A. Benslimane. A secure architecture for mobile ad hoc networks. In *Proc. 2nd International Conference on Mobile Ad-Hoc and Sensor Networks (MSN 2006)*, Dec. 2006.

[RBM05] K. Römer, P. Blum, and L. Meier. Time synchronization and calibration in wireless sensor networks. In *Handbook of Sensor Networks: Algorithms and Architectures*. John Wiley and Sons, 2005.

[RK04] C. H. Rentel and T. Kunz. Network synchronization in wireless ad hoc networks. Technical Report SCE-04-08, Carleton University, 2004.

[RKAO93] T. L. Magnanti R. K. Ahuja and J. B. Orlin. *Network Flows: Theory, Algorithms, and Applications*. Prentice Hall, 1993.

[Ros65] J. B. Rosen. Existence and uniqueness of equilibrium points for concave n-person games. *Econometrica*, 33(3):520–534, 1965.

[Rub98] A. Rubinstein. *Modeling Bounded Rationality*. MIT Press, 1998.

[SA02] F. Stajano and R. Anderson. The resurrecting duckling: security issues for ubiquitous computing. *Computer*, 35(4):22–26, Apr 2002.

[SCS04] J. Sheu, C. Chao, and C. Sun. A clock synchronization algorithm for multi-hop wireless ad hoc networks. In *Proc. ICDCS 2004*, pages 574–581, 2004.

[SE07] Y. E. Sagduyu and A. Ephremides. A game-theoretic analysis of denial of service attacks in wireless random access. In *Proc. Wiopt 2007*, pages 1–10, April 2007.

[SEA03] A. Sendonaris, E. Erkip, and B. Aazhang. User cooperation diversity (parts I,II). *IEEE Transactions on Communications*, 51(11):1927–1948, November 2003.

[Shi04] M. Shigeno. A survey of combinatorial maximum flow algorithms on a network with gains. *Journal of the Operations Research Society of Japan*, 47(4):244–264, 2004.

[SMG02a] C.U. Saraydar, N.B. Mandayam, and D.J. Goodman. Efficient power control via pricing in wireless data networks. *IEEE Transactions on Communications*, 50(2):291–303, Feb 2002.

[SMG02b] C.U. Saraydar, N.B. Mandayam, and D.J. Goodman. Efficient power control via pricing in wireless data networks. *IEEE Transactions on Communications*, 50(2):291–303, February 2002.

[SNCR03] V. Srinivasan, P. Nuggehalli, C.F. Chiasserini, and R.R. Rao. Cooperation in wireless ad hoc networks. In *Proc. IEEE INFOCOM 2003*, volume 2, pages 808–817, March-3 April 2003.

[SNW06] K. Sun, P. Ning, and C. Wang. Secure and resilient clock synchronization in wireless sensor networks. *IEEE Journal on Selected Areas in Communications*, 24(2):395–408, Feb. 2006.

[SSA06] D. Subhadrabandhu, S. Sarkar, and F. Anjum. A statistical framework for intrusion detection in ad hoc networks. In *Proc. IEEE INFOCOM 2006*, pages 1–13, April 2006.

[SV04] J. So and N. H. Vaidya. A distributed selfstabilizing time synchronization protocol for multi-hop wireless networks. Technical report, UIUC, 2004.

[SZC05] H. Song, S. Zhu, and G. Cao. Attack-resilient time synchronization for wireless sensor networks. In *Proc. IEEE International Conference on Mobile Ad hoc and Sensor Systems Conference (MASS 2005)*, Nov. 2005.

[TG05] G. Tan and J. Guttag. The 802.11 mac protocol leads to inefficient equilibria. *Proc. IEEE INFOCOM 2005*, 1:1–11 vol. 1, March 2005.

[TWSC07] A. Tang, J. Wang, S.H.Low, and M. Chiang. Equilibrium of heterogeneous congestion control: Existence and uniqueness. *IEEE/ACM Transactions on Networking*, 15(4):824–837, August 2007.

[Way] K. D. Wayne. *Generalized Maximum Flow Algorithms*. PhD thesis, Cornell University.

[WLLD03] J. Wang, L. Li, S.H. Low, and J.C. Doyle. Can shortest-path routing and TCP maximize utility. In *Proc. IEEE Infocom*, San Francisco, CA, April 2003.

[WMP05] Y. Wang, M. Martonosi, and L. Peh. A new scheme on link quality prediction and its applications to metric-based routing. In *Proc. 3rd international conference on Embedded networked sensor systems (SenSys 05)*, pages 288–289, New York, NY, USA, 2005. ACM.

[WSS03] A.D. Wood, J.A. Stankovic, and S.H. Son. Jam: a jammed-area mapping service for sensor networks. In *Proc. 24th IEEE Real-Time Systems Symposium (RTSS 03)*, pages 286–297, Dec. 2003.

[WSZ07] A.D. Wood, J.A. Stankovic, and G. Zhou. Deejam: Defeating energy-efficient jamming in ieee 802.15.4-based wireless networks. In *Proc. 4th Annual IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON 07)*, pages 60–69, June 2007.

[WW95] A. Washburn and K. Wood. Two-person zero-sum games for network interdiction. *Operations Research*, 43(2):243–251, 1995.

[XTZW05] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proc. ACM MobiHoc 05*, pages 46–57, New York, NY, USA, 2005. ACM.

[XWTZ04] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel surfing and spatial retreats: defenses against wireless denial of service. In *Proc. 3rd ACM workshop on Wireless security (WiSe 04)*, pages 80–89, New York, NY, USA, 2004.

[XY08] Y. Xi and E.M. Yeh. Pricing, competition, and routing for selfish and strategic nodes in multi-hop relay networks. In *Proc. IEEE Infocom*, Phoenix, AZ, April 2008.

[Yat95] R.D. Yates. A framework for uplink power control in cellular radio systems. *IEEE Journal on Selected Areas in Communications*, 13(7):1341–1347, Sep 1995.

[YP01] J. Yang and S. Papavassiliou. Improving network security by multipath traffic dispersion. In *IEEE Military Communications Conference (MILCOM 01)*, volume 1, pages 34–38 vol.1, 2001.

[ZL00] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In *Proc. MobiCom 00*, pages 275–283, New York, NY, USA, 2000. ACM.

[ZL05] D. Zhou and T.-H. Lai. A compatible and scalable clock synchronization protocol in ieee 802.11 ad hoc networks. In *Proc. 34th International Conference on Parallel Processing (ICPP 05)*, pages 295–302, June 2005.

[ZLLY07a] S. Zhong, L. Li, Y. Liu, and Y. Yang. On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks: An integrated approach using game theoretic and cryptographic techniques. *Wireless Networks*, 13(6):799–816, 2007.

[ZLLY07b] S. Zhong, L. Li, Y. G. Liu, and R. Yang. On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks: an integrated approach using game theoretic and cryptographic techniques. *Wireless Networks*, 13(6):799–816, 2007.