Channel Surveillance Strategy and Interference Reduction in Future Wireless Networks

Duc-Tuyen Ta

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

TELECOM ParisTech

2018-ENST-0039

EDITE - ED 130

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

TELECOM ParisTech

Spécialité « Électronique et Communications »

présentée et soutenue publiquement par

Duc-Tuyen TA

10 Juillet 2018

Channel Surveillance Strategy and Interference Reduction in Future Wireless Networks

Directeur de thèse : **Van-Tam NGUYEN**

Jury

M. Samson LASAULCE, Directeur de recherche, L2S CNRS/Supélec/Univ. Paris-Sud 11	Rapporteur
Mme. Kinda KHAWAM, Maitre de conferences HDR, Université de Versailles	Rapporteur
M. Pierre DUHAMEL, Directeur de recherche, L2S CNRS/Supélec/Univ. Paris-Sud 11	Examinateur
M. Philippe CIBLAT, Professeur, Institut Télécom/Télécom ParisTech	Examinateur
M. Patrick MAILLÉ, Professeur, IMT Altantique	Examinateur
M. Marceau COUPECHOUX, Professeur, Institut Télécom/Télécom ParisTech	Examinateur
Mme/M. Linh-Trung NGUYEN, Maitre de conferences HDR, UET-VNUH, Vietnam	Examinateur
M. Van-Tam NGUYEN, Directeur Général, Institute of Applied Technology, Vietnam	Directeur de thèse

TELECOM ParisTech
école de l'Institut Mines-Télécom - membre de ParisTech
46 rue Barrault 75013 Paris - (+33) 1 45 81 77 77 - www.telecom-paristech.fr

T H È S E

Channel Surveillance Strategy and Interference Reduction in Future Wireless Networks

Duc-Tuyen TA
Supervisor: Van-Tam Nguyen

August 2018

To my loving parents and my wife.

Acknowledgements

I would like to gratefully acknowledge and express a sincere thank you to my supervisor, Assoc. Prof. Van-Tam Nguyen for giving me the opportunity to pursue doctoral study at Télécom Paris-Tech. I am truly privileged to have learned from his remarkable technical knowledge and research enthusiasm. His invaluable support and guidance during my study have certainly helped me complete this Ph.D. dissertation. I would like to express my gratitude to Professors Phillipe Ciblat (Telecom ParisTech) and Patrick Maillé (IMT Atlantique) and Assistant Professor Duy H. N. Nguyen (San Diego State University) who have regularly reviewed and constructively commented on the progress of my doctoral study. I would also to express my gratitude to jury of my thesis committee for serving as the examiner to my thesis and for their extremely valuable feedbacks.

Special thanks are due to Assoc. Prof. Linh-Trung Nguyen of University of Engineering and Technology (VNUH-Vietnam) for his encouragement to my pursuit of Ph.D. study. I would also like to gratefully acknowledge the European Catrene Cortif project and Télécom ParisTech for the financial support to my study.

I would like to express my gratitude to all my colleagues in a wonderful and memorable time at the C2S Laboratory of the Comelec Department at Télécom ParisTech. Many thanks to Dr. Nhan Nguyen-Thanh for proofreading my thesis.

My deepest love and gratitude are devoted to all of my family members : Mom and Dad, my wife Giang, my brothers, sisters, beloved nephew Milo, who always support me in each and every endeavor in my life. My Ph.D. study would not be finished without the constant and unconditional support from my family. I thank you all and hope that I made you proud of my accomplishments.

Abstract

Cognitive Radio (CR) has emerged as a promising technology to address the conflict between the spectrum scarcity and the spectrum underutilization in the future wireless communication systems by enabling the network users to detect and exploit the spectrum opportunities. The successful deployment of CR networks, however, depends not only on the efficient exploitation of the spectrum opportunities but also on the self-coexistence mechanisms between cognitive users (SUs). The objective of this thesis is to study systematically the coexistence mechanisms between SUs in both CR network architectures : centralized and distributed. Specifically, to ensure the coexistence and the fairness transmission among SUs, this research examines various mitigation techniques that mitigate the influence of the misbehaving users in the centralized-based CR networks. In the distributed-based CR networks, this research proposes a collaborative resource allocation framework that ensuring the coexistence between SUs. In addition, this research develops low-complexity and distributed algorithms to determine the best coexistence strategy for the network coordinator and cognitive users.

On the centralized infrastructure networks, this thesis examines the coexistence among SUs through the mitigation techniques to mitigate the influence of the misbehaving users. The unaddressed research problems of the multi-channel primary user emulation attack in the spectrum sensing-based CR networks and the spoofing attack in the database driven-based CR networks are taken into account. The work characterizes the interaction between misbehaving users and the network coordinator by formulating a non-cooperative game and determining the stable operating point of the system through the Nash equilibrium (NE) of the game. In addition, motivated by the appropriate modeling of the strategic interaction between the network coordinator and the attacker, the work considers the leadership and commitment in the game model by analyzing the corresponding strategy of the attacker and the network coordinator through the Strong Stackelberg Equilibrium (SSE) of the game.

On the distributed infrastructure networks, efficient resource allocation is considered as the key solution for maintaining a harmonized coexistence between independent SUs. To harvest the full capacity out of the RF spectrum, SUs also will need to use more intelligence to avoid interference while optimizing the spectrum by collaborating with other users. This work proposes the collaborative resource allocation framework, where each SU optimizes its strategy in a collaborative manner. Specifically, we tackle the collaborative paradigm between

SUs to manage power allocation and formulated these relationships through a non-cooperative game. The proposed collaborative power allocation possesses the advantages of the optimality and distributed implementation. Due to the nonconcave nature of the power allocation game, we develop the low-complexity approximation techniques to approximate the formulated game into the well-known games, which can be solved easily. Simulation results show significant performance improvements in terms of power fairness, sum-rate and convergence time.

French Summary

Introduction

La révolution des télécommunications sans fil crée une énorme demande pour l'accès au spectre des fréquences radio avec l'explosion du nombre d'appareils connectés et la grande diversité des cas d'utilisation et des exigences. Cependant, le conflit entre la pénurie de spectre libre et la sous-utilisation du spectre entraîne des inefficacités importantes des communications sans fil et entrave le déploiement de nouvelles applications. Récemment, la radio cognitive (RC) est apparue comme une technologie prometteuse pour pallier la pénurie de spectre et mieux utiliser les ressources en permettant aux utilisateurs du réseau de détecter et d'exploiter les opportunités du spectre. Le succès du déploiement des réseaux CR dépend cependant non seulement de l'exploitation efficace des opportunités de spectre, mais aussi des mécanismes d'auto-coexistence entre les utilisateurs cognitifs (UC). L'objectif de cette thèse est donc de fournir une étude systématique des mécanismes d'auto-coexistence pour les utilisateurs cognitifs dans les architectures de réseau RC centralisées et distribuées, qui répondent directement aux défis techniques causés par les utilisateurs malfaisants dans le cas des réseaux à infrastructure centralisée et les problèmes d'attribution de ressources dans les réseaux à infrastructure distribuée.

Concernant les réseaux à infrastructure centralisée, cette thèse examine la coexistence entre les UC à travers les techniques d'atténuation pour limiter l'influence des utilisateurs malfaisants. Les problèmes de l'attaque par émulation d'utilisateur primaire multicanal dans le cas des réseaux RC basés sur la détection de spectre et l'attaque par usurpation dans le cas des réseaux RC basés sur une base de données sont pris en compte. La formulation des jeux entre l'attaquant et le coordinateur du réseau, ainsi que le calcul de l'équilibre de Nash, sont ensuite étudiés. Motivées par la contrainte du temps de calcul dans l'approche du jeu, ces recherches tentent également d'exposer la modélisation appropriée de la stratégie d"interaction entre le coordinateur du réseau et l'attaquant ; et fournit des moyens pour prendre en compte le leadership et l'engagement dans le modèle du jeu grâce à l'équilibre de Stackelberg. Nous montrons par simulations numériques que des améliorations significatives peuvent être obtenues en termes de rémunération attendue du coordinateur de réseau et de temps de calcul en adoptant le modèle d'engagement.

Concernant les réseaux à infrastructure distribuée, l'attribution efficace des ressources est considérée comme la solution clé pour maintenir une coexistence harmonisée entre les UC indépendantes. De plus, pour exploiter toute la capacité du spectre RF, les UC devront également utiliser plus d'intelligence pour éviter les interférences tout en optimisant le spectre en collaborant avec d'autres utilisateurs. Ce travail propose donc le modèle d'attribution collaborative des ressources, où chaque UC optimise sa stratégie de manière collaborative. Plus spécifiquement, nous abordons le paradigme collaboratif entre les UC pour déterminer la stratégie efficace d'attribution d'énergie. L'attribution de puissance collaborative proposée possède les avantages de l'optimalité et d'une mise en œuvre distribuée. En raison de la nature non concave du problème d'attribution de puissance, nous développons des techniques d'approximation à faible complexité pour approximer le jeu à des jeux bien connus, qui peuvent être résolu facilement. Les résultats de simulation montrent des améliorations significatives des performances en termes d'équité de la répartition de la puissance, de débit cumulé et de temps de convergence.

Contexte sur l'auto-coexistence dans les radio cognitives

Dans les réseaux de radiocommunication cognitifs centralisés, il existe deux approches principales pour déterminer les possibilités de spectre : i) la détection du spectre [24] et ii) la gestion de la base de données [25, 26]. Dans la première approche, l'activité du système primaire est explorée en mesurant le spectre de l'environnement radio. Dans cette dernière approche, un gestionnaire, qui est essentiellement un serveur de base de données avec une carte de géolocalisation en ligne de l'utilisation du spectre, est chargé de gérer la coexistence entre les PU et les SU. L'approche basée sur la base de données est plus précise et fiable, mais onéreuse et nécessite une connaissance approfondie du système primaire et une diffusion rapide des mises à jour du spectre. D'un autre côté, l'approche de détection du spectre fournit une méthode moins précise mais moins coûteuse et plus souple pour découvrir des trous de spectre pour un large éventail de types de réseau. Pour les deux approches, afin de garantir la coexistence entre les UM, les réseaux CR doivent relever le défi de distinguer le signal primaire ou la requête utilisateur honnête du mauvais signal / de la requête utilisateur [15]. Plus précisément, les réseaux CR basés sur le spectre souffrent de l'attaque d'émulation primaire de l'utilisateur [16] tandis que les réseaux CR basés sur des bases de données souffrent d'attaques d'usurpation [17].

L'attaque d'émulation utilisateur primaire [19–21, 27] est une attaque du processus de détection du spectre dans lequel un utilisateur mal conçu émet le signal primaire émulé pendant la période de détection du spectre. La présence du signal primaire émulé entraînera un état présomptueusement occupé sur les canaux attaqués (c'est-à-dire que le moteur de détection de spectre perçoit les canaux comme étant occupés). Par conséquent, le PUEA limite l'accès au spectre des réseaux CR et dégrade ainsi gravement leur fonctionnement.

Récemment, plusieurs techniques ont été introduites pour atténuer les PUEA, telles que la vérification du signal en authentifiant les signaux de signaux utilisateur primaires ou le schéma de la théorie des jeux en formulant la relation entre les éléments du réseau comme un jeu. Cependant, ces approches nécessitent la modification du matériel ou du protocole utilisateur primaire, ce qui est inapplicable dans le cas du réseau radio cognitif, ou font face au problème des attaques multicanaux.

Dans les réseaux CR basés sur des bases de données, la base de données stocke un référentiel à jour de l'utilisateur principal pour gérer le fonctionnement du réseau [25, 26]. Lorsqu'un utilisateur souhaite utiliser des canaux, il doit envoyer une demande à un coordinateur, qui contient le serveur de base de données, pour acquérir une ressource de canal. Selon l'emplacement de l'utilisateur et la base de données d'utilisation du spectre, le coordinateur attribuera les canaux et paramètres de transmission disponibles à l'utilisateur. Un attaquant peut attaquer le système en utilisant un mauvais emplacement ou une mauvaise identification. En conséquence, une attribution de spectre inéquitable peut se produire ; par conséquent, les performances du système seront réduites. Toutefois, à notre connaissance, aucun travail n'examine systématiquement l'impact des attaques par usurpation d'identité sur les réseaux CR basés sur des bases de données.

Dans les réseaux CR distribués, la principale préoccupation est l'étude d'un algorithme d'allocation de puissance pour maintenir la coexistence entre les unités d'exploitation dans la coexistence des réseaux CR à base distribuée. Notez que l'étude n'est pas limitée au problème d'allocation de puissance. D'autres aspects de l'allocation des ressources, tels que la sélection des canaux, la planification des utilisateurs et la conception de la formation / du précodage des faisceaux, sont également étudiés. Avec les contraintes d'alimentation de l'utilisateur CR, cette section passe en revue l'allocation des ressources selon les deux critères suivants : (i) minimiser la puissance d'émission aux nœuds CR et (ii) maximiser le débit total aux nœuds CR. Dans ce domaine, les travaux récents se concentrent principalement sur deux approches : les jeux non coopératifs [31–33, 35–37, 43] et optimisation conjointe [38–43]. Dans la premiére approche, chaque utilisateur optimise égoïstement ses propres performances, indépendamment des actions des autres utilisateurs. Le principal avantage de cette approche est l'implémentation entiérement distribuée du contrôle de puissance avec peu ou pas de coordination entre les nœuds CR. La fonctionnalité vous permet d'utiliser *algorithmes distribués à faible complexité* pour déterminer l'allocation de puissance. Cependant, l'optimum global peut être moins probable et les performances du systéme peuvent être dégradées. D'autre part, en adoptant une approche d'optimisation pour résoudre le probléme d'allocation de source dans un réseau CR, tous les utilisateurs de CR visent à maximiser une fonction d'utilité commune. L'approche d'optimisation conjointe permet à tous les utilisateurs de emph optimiser de maniére coordonnée leurs stratégies et permet une allocation dynamique du budget de brouillage entre les utilisateurs. Cependant, cette approche doit tenir compte de *complexité accrue* et de *overhead* en raison de la demande d'informations sur les canaux de tous les

utilisateurs nécessaires pour implémenter l'algorithme d'optimisation conjointe. De plus, même lorsque les informations globales sont connues, les résultats d'optimisation montrent que les utilisateurs dont les conditions de canal sont médiocres disposent de beaucoup moins d'énergie pour optimiser les performances de l'ensemble du réseau. En conséquence, cela dégrade l'équité entre les utilisateurs du réseau.

Auto-coexistence dans les réseaux fondés sur la détection du spectre : stratégie de surveillance pour les PUEA

En fonction du type d'attaque, nous pouvons déterminer une bonne stratégie pour gérer ces derniers. Dans le PUEA malveillant, l'attaquant vise à entraver le fonctionnement des réseaux CR en émettant le signal primaire émulé à la période de détection. Ainsi, il est possible de détecter les canaux ajoutés en ajoutant un processus de détection supplémentaire dans la période de données suivante afin de récupérer l'opportunité d'utiliser les canaux attaqués dans le reste de la trame [54, 75]. En revanche, une PUEA égoïste réussie est généralement suivie d'une attaque égoïste de l'attaquant. Par conséquent, il est possible de déterminer l'identification de l'utilisateur dans n'importe quel lien de communication en implémentant un processus de surveillance des canaux, utilisé pour détecter l'occupation illégale des canaux et identifier l'attaquant égoïste PUEA [54]. Un jeu non coopératif entre le coordinateur de réseau, qui fournit le service de défense basé sur la surveillance (*i.e., le processus de détection supplémentaire et de surveillance*), et l'attaquant de PUEA est formulé. Les stratégies de surveillance, ainsi que les stratégies d'attaque, sont déterminées par le NE proche du jeu. Il convient de noter qu'il s'agit d'une des attaques à un seul canal dans lesquelles l'attaquant et le coordinateur du réseau peuvent attaquer ou surveiller au plus un canal.

Habituellement, les réseaux CR fonctionnent sur plusieurs bandes de fréquences, tandis que l'attaquant peut lancer une PUEA égoïste multicanal en raison de l'expansion rapide de la radio définie par logiciel. Dans un tel cas, puisque le canal pourrait être considéré comme indépendant sur chaque canal, le modèle simple avec un seul canal et un ensemble limité de stratégies, comme étudié dans [54, 75], pourrait être étendu au attaque multicanal avec des ressources illimitées pour l'attaquant et le coordinateur réseau by cependant, en raison des ressources limitées, l'extension du jeu pour le cas multicanal par chaque canal ne peut pas être décrite comme le comportement de l'attaque et du processus de surveillance. De plus, si le coordinateur de réseau considère chaque canal séparément, il sera nécessaire de prendre en compte un plan de surveillance séquentiel, ce qui entraîne un long temps de surveillance. Cela signifie que le modèle du processus de surveillance multicanal visant à atténuer l'influence du PUEA dans les réseaux CR est plus réaliste que le processus de surveillance à canal unique ou le modèle de surveillance séquentielle. Par conséquent, il est nécessaire d'étudier l'attaque multicanal et les techniques d'atténuation correspondantes.

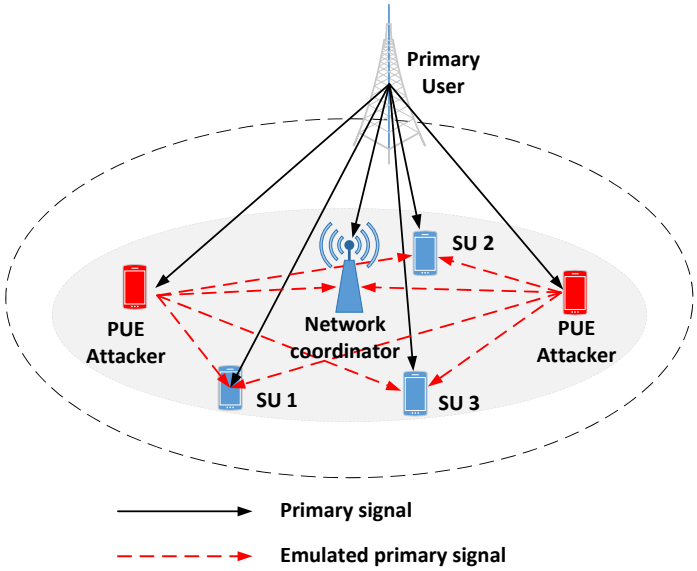


FIGURE 1 Un exemple de réseau CR basé sur la détection de spectre avec le coordinateur de réseau et les attaquants de PUEA.

Cet article discute du rôle de cette étude dans l'étude du processus d'atténuation et de l'influence de PUEA dans les réseaux CR. Plus précisément, nous mettons l'accent sur l'étude du PUEA multicanal et du processus de surveillance correspondant. En utilisant le cadre de la théorie des jeux, nous formulons la relation entre l'attaquant et le coordinateur du réseau comme un jeu stratégique et établissons la meilleure stratégie pour le coordinateur de réseau et l'attaquant à travers le NE du jeu. Puisque le coordinateur de réseau n'observe l'action de l'attaquant qu'indirectement, le texte est produit par les résultats de la détection, le jeu formulé est un jeu d'information incomplet et imparfait. Trouver une solution NE dans un tel jeu est plus compliqué en raison du vaste ensemble de stratégies [78]. Nous employons donc l'approche de représentation de forme de séquence [79, 80] au lieu de la méthode conventionnelle de représentation de forme stratégique "benchmark" [81, 82] pour formuler puis déterminer la stratégie NE pour le jeu. Les résultats de l'analyse et de la simulation confirment que la représentation de la forme de la séquence est beaucoup plus efficace que l'approche de la représentation de la forme stratégique pour la détermination NE du jeu.

Modéle de systéme

Nous considérons un réseau CR semi-duplex basé sur la détection qui permet un accès secondaire à plusieurs bandes sous licence, comme illustré dans la figure 1. Afin de simplifier l'analyse et de nous concentrer sur les effets du processus de surveillance pour atténuer l'influence du PUEA (égoïste ou malveillant), nous supposons que le réseau CR contient deux ensembles distincts : le coordinateur de réseau et les utilisateurs de CR. Le coordinateur du

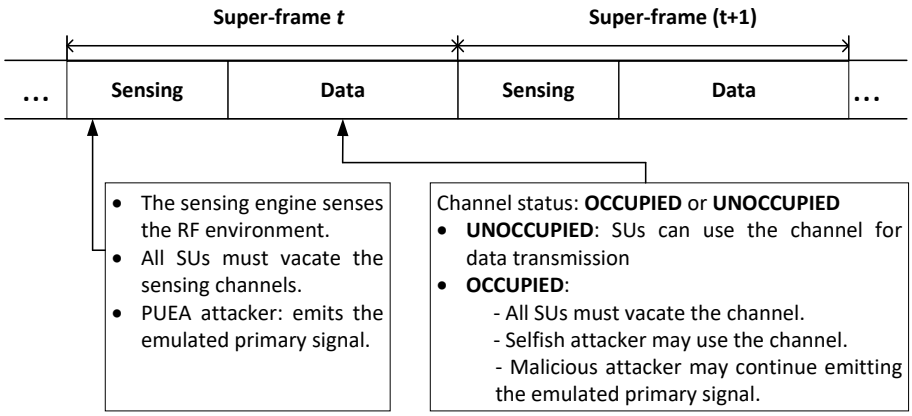


FIGURE 2 Cadre de synchronisation pour l'opération réseau.

réseau est responsable de la fourniture des services de détection et de surveillance, tandis que les utilisateurs du CR exploitent ces services pour la transmission de données opportuniste. Dans un tel modèle, l'attaquant de PUEA est également un utilisateur cognitif et peut exploiter les services fournis par le coordinateur de réseau. Noté que dans le réel, il y a peut-être plusieurs attaquants de PUEA sur le réseau. Cependant, en présence de plusieurs attaquants de PUEA, les dommages au réseau de CR seront au plus haut niveau s'ils contribuent à une attaque conjointe. Par conséquent, dans notre modèle, nous supposons que le PUEA joint par un ensemble d'attaquant est mené par un seul attaquant équivalent. Pour simplifier la présentation, nous notons *attaquant* le représentant de l'attaquant égoïste et emph le défenseur le représentant du coordinateur du réseau.

Dans un réseau CR basé sur la détection de spectre, il est supposé que le coordinateur de réseau, donc l'attaquant PUEA, a une observation partielle de la probabilité de l'activité PU en effectuant une période de détection fixe. De plus, les qualités du moteur de détection, *i.e.*, la probabilité de détection et la probabilité de fausse alarme dans chaque canal sans fil sont la connaissance préalable du coordinateur de réseau et de l'attaquant de PUEA.

En général, comme illustré dans la figure 2, le fonctionnement du réseau CR est divisé en intervalles de temps, chacun comprenant deux périodes : la détection et la transmission de données. Pendant la période de détection, l'attaquant PUEA peut émettre ou non le signal primaire émulé par rapport à un certain canal. Nous supposons que le moteur de détection ne peut pas distinguer les signaux primaires émulés et légitimes ; par conséquent, le PUEA ne sera pas détecté pendant la période de détection. De plus, avant chaque intervalle de temps, le gestionnaire de réseau ignore si le PU est actif ou non. De plus, l'attaquant ne peut pas connaître le statut réel du signal primaire sur les canaux attaqués car il est occupé à transmettre un signal primaire émulé dans le même canal. Cela signifie que l'attaquant effectue un PUEA sans information sur le statut du signal utilisateur primaire avant le début de la période de détection de chaque intervalle de temps. Il est à noter que certaines

études de littérature [21, 27] supposent que l'attaquant mène un PUEA avec le jeu de jachère (l'ensemble des canaux sur lesquels le PU n'est pas actif) avant la période de détection de chaque fois. Cependant, dans un tel cas, le modèle de système du processus de surveillance est similaire au modèle du processus de surveillance, qui traite de la PUEA sans la mise en jachère. Par conséquent, ce chapitre met l'accent sur l'étude du processus de surveillance visant à traiter les PUEA sans l'ensemble de jachère. À la période de données, si le canal attaqué est annoncé comme inoccupé, les attaquants agissent alors comme des utilisateurs normaux de CR. Inversement, si le canal attaqué est annoncé comme étant occupé, l'attaquant égoïste PUEA utilisera alors ce canal pour transmettre les données de manière égoïste alors que l'attaquant malveillant retransmettra le signal primaire émulé pour s'assurer que le réseau ne pourra pas récupérer le canal en implémentant le processus de détection.

Puisque l'attaquant rationnel et intelligent peut apprendre à adapter la stratégie de surveillance en effectuant une période de surveillance fixe, le défenseur peut agir de manière proactive en s'engageant ou non sur sa stratégie de défense. En fonction des actions du défenseur, nous considérons les deux cas suivants :

— **Non-Engagement :** Le défenseur ne considère pas s'engager dans sa stratégie de défense. L'attaquant optimise alors son utilité attendue concernant toutes les stratégies possibles du défenseur. Nous formulons la relation entre l'attaquant et le gestionnaire de réseau en tant que 2 joueurs, un jeu de formulaire complet. La représentation en forme de séquence est utilisée pour représenter le jeu et ensuite déterminer la stratégie NE.

— **Engagement :** Le défenseur agit en tant que leader en s'y engageant dans une stratégie de surveillance (extra-détection). L'attaquant agit alors comme un suiveur en effectuant la meilleure réponse concernant la stratégie de défense observée. Le modèle Stackelberg est utilisé pour formuler la relation entre le gestionnaire de réseau et l'attaquant dans lequel le gestionnaire de réseau joue le rôle de leader et force l'attaquant à jouer le rôle de suiveur en suivant la stratégie engagée du gestionnaire de réseau.

Auto-coexistence dans les réseaux de RC basés sur les bases de données : stratégie de surveillance des attaques par usurpation d'identité

Le point clé de la mise en œuvre de l'approche basée sur la base de données de géo-localisation est la disponibilité et la précision des informations sur l'emplacement des SU. Des interférences considérables sur les systèmes primaires et secondaires apparaîtront si les informations de localisation des utilisateurs sont inexactes. En outre, une attribution de spectre inéquitable se produira si des adversaires chargent intentionnellement des messages de

demande avec une identification fausse (ID) ou des informations de localisation falsifiées. Par conséquent, les attaques par usurpation d'identité constituent une vulnérabilité critique du système DSA basé sur GDB. Cependant, au mieux de nos connaissances, il n'ya pas de travail qui examine systématiquement l'impact des attaques par usurpation dans les CRB basés sur des bases de données. Le travail connexe le plus pertinent qui considère les attaques par usurpation GPS dans un réseau de radiocommunication cognitif piloté par base de données est présenté dans [17] mais limité en raison de l'impact de la fausse localisation des signaux GPS attaqués. D'autres études sur le problème de sécurité dans les systèmes pilotés par des bases de données portent principalement sur la confidentialité des emplacements [18, 28, 29] ou sur les problèmes de confidentialité des systèmes en place [30] sans affecter l'accessibilité de la base de données et l'efficacité d'utilisation du spectre.

Dans le réseau CR basé sur une base de données, un utilisateur cognitif doit envoyer une demande au coordinateur de réseau afin de s'inscrire pour l'opération ou pour mettre à jour un nouvel emplacement ou pour rechercher des bandes de spectre. Généralement, les messages de demande contiennent l'ID physique, tel que l'adresse de contrôle d'accès au support et la géolocalisation de l'utilisateur. En raison de la souplesse de la radio définie par logiciel, les informations sur l'identité ou l'emplacement peuvent être falsifiées par l'utilisateur qui se comporte mal. Par exemple, l'attaquant peut utiliser le faux emplacement pour demander l'accès au spectre pour la transmission de données ou pour détruire le fonctionnement du réseau. De plus, l'attaquant peut usurper l'ID (*i.e.*, en utilisant un faux identifiant ou en utilisant l'identifiant d'autres utilisateurs) pour attaquer le réseau.

Processus de vérification

En fonction de la diversité des objectifs et du contenu des requêtes d'usurpation, il existe peut-être plusieurs méthodes d'atténuation permettant de gérer les attaques par usurpation d'identité. Afin de systématiser ces méthodes, nous remarquons qu'une attaque par usurpation d'identité ne se situe qu'à l'emplacement ou aux informations d'identification du message de requête. Par conséquent, en effectuant un processus de surveillance pour vérifier l'emplacement ou l'ID de l'utilisateur cognitif qui envoie la demande, le coordinateur du réseau peut détecter le mauvais emplacement ou l'occupation illégale. Par conséquent, nous proposons un processus de surveillance qui comprend deux étapes complémentaires : la *vérification de l'emplacement de la requête* et le *identification de l'utilisateur du spectre* pour traiter les attaques par usurpation d'identité et d'emplacement (Fig. 4). Le processus de vérification en deux étapes est publié dans les détails suivants :

— **Demander une vérification d'emplacement** : pour l'attaque par usurpation d'emplacement, nous proposons d'implémenter un processus de vérification d'emplacement. Les méthodes de positionnement basées sur la puissance du signal de réception, l'heure d'arrivée, les réseaux de capteurs ajoutés, etc. peuvent être utilisées pour déterminer

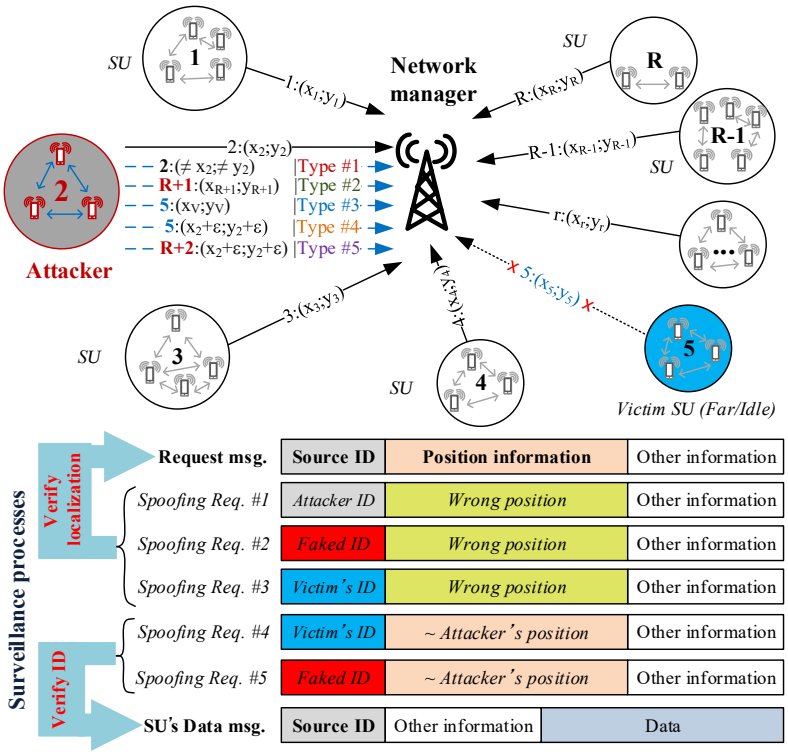


FIGURE 3 Types d'attaques d'usurpation dans les réseaux de radiocommunication cognitifs basés sur des bases de données.

la position de dérivation de la demande. En cas d'incompatibilité entre l'emplacement estimé et les informations d'emplacement dans le message de demande, l'attaque d'usurpation d'emplacement est détectée. La demande sera ignorée et une autre sanction sera imposée à l'attaquant. En pratique, en raison de la variation de l'environnement radio et des caractéristiques des méthodes de positionnement, la précision de la localisation est toujours limitée. Par conséquent, l'efficacité de cette étape de surveillance est limitée à une distance, appelée *rayon indétectable*. Toute différence de distance entre la position réelle et les informations de localisation dans la requête inférieure au rayon indétectable ne peut pas être découverte.

— **Identification des utilisateurs du spectre** : afin de fournir des contre-actions complémentaires pour l'étape ci-dessus, nous proposons d'effectuer un deuxième processus de surveillance. La surveillance supplémentaire sur une petite zone à l'intérieur d'un rayon indétectable est effectuée en balayant les bandes de spectre attribuées pour déterminer qui utilise la ressource. La raison en est que l'utilisateur doit révéler son identifiant physique pour transmettre ses propres données via des liens de communication. Si les bandes de spectre ne sont pas occupées, l'attaque est malveillante et la ressource de fréquence est réorganisée pour d'autres demandes. Si les bandes de

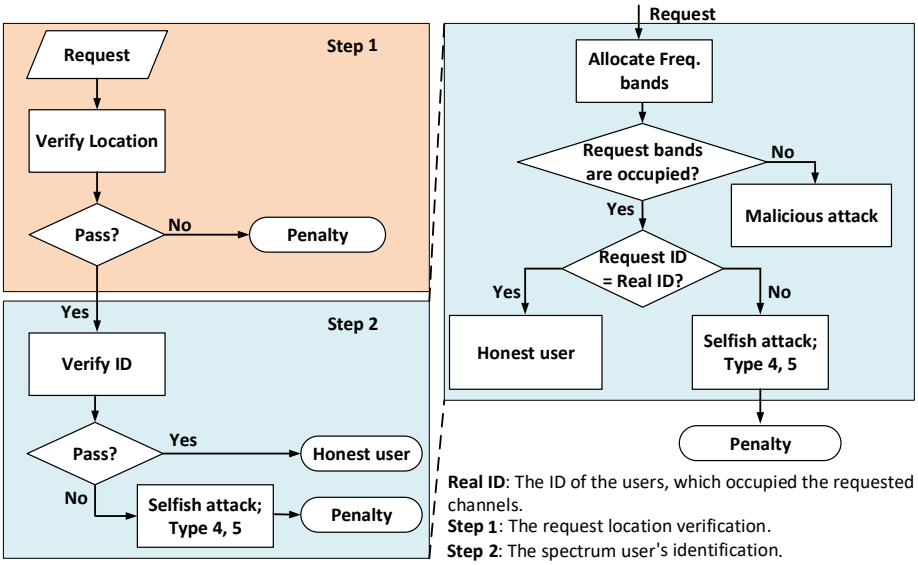


FIGURE 4 Le processus de vérification en 2 étapes pour gérer les attaques par usurpation d'identité et d'ID sur le système de partage de spectre GDB.

spectre sont occupées par des utilisateurs incompatibles, l'attaque par égoïsme (*i.e.*, type 4 et 5) peut donc être détectée et punie en conséquence.

En raison du compromis entre le gain et la perte de l'attaquant et du coordinateur de réseau, la théorie des jeux, qui étudie mathématiquement l'interaction entre des joueurs indépendants et intéressés, aide à formuler notre problème. Dans les deux sections suivantes, nous formulons deux jeux de surveillance qui décrivent l'interaction des deux méthodes de surveillance avec les stratégies d'attaque.

Demander des stratégies de vérification de l'emplacement

Dans le réseau CR basé sur une base de données, chaque utilisateur cognitif envoie les messages de demande au coordinateur de réseau via les connexions sans fil. Par conséquent, il est possible de localiser les emplacements d'envoi des demandes et d'utiliser l'emplacement estimé pour vérifier que la demande est une usurpation de l'emplacement (*i.e.*, type 1, 2 et 3) en la comparant aux informations de localisation de la requête. message. Comme le nombre de SU actifs et leurs emplacements peuvent être enregistrés dans les données d'historique, nous supposons qu'il s'agit d'une connaissance commune, accessible à la fois par le gestionnaire de réseau et par l'attaquant. L'attaquant peut alors envoyer plusieurs requêtes pour implémenter la spoofing de localisation. De même, le coordinateur de réseau peut effectuer plusieurs processus de vérification. La question ici est que, tant pour l'attaquant que pour le coordinateur du réseau, quel est le nombre optimal de demandes d'attaque et de processus de vérification ?

Pour analyser l'interaction entre le processus de location et l'usurpation de la location, nous formulons comme suit un jeu à 2 pour un joueur et un attaquant.

— **Attacker**, qui est également un utilisateur cognitif, implémente l'attaque par usurpation d'emplacement en envoyant des requêtes d'usurpation de l'emplacement jusqu'à N.
— **Defender**, qui représente le coordinateur du réseau, peut effectuer une surveillance jusqu'à M emplacements / demandes de slots (en fonction de l'infrastructure supportée).

Stratégie : Soit A le jeu de stratégie pur de l'attaquant. Ensuite, A est défini par

$$A = \{n, n = 0, 1, ..., N\}, \tag{1}$$

où n indique le nombre d'attaques d'usurpation. Si $n = 0$, l'attaquant n'agit pas pour attaquer le réseau CR.

De même, soit D le jeu de stratégie pur du défenseur. Alors, D est défini par

$$D = \{m, m = 0, 1, ..., M\}, \tag{2}$$

où m indique le nombre de vérification. Si $m = 0$, le défenseur ne fonctionne pas pour défendre le réseau CR.

Payer : Soit r le nombre de SU actives dans la zone vérifiée. Pour chaque paire de (m, n) donnée r, le gain correspondant de l'attaquant Π^A et le défenseur Π^D sont calculés par :

$$\Pi^A_{m,n,r} = n\,(G - C_A) - \pi_{m,n,r} \tag{3a}$$
$$\Pi^D_{m,n,r} = -mC_S + \pi_{m,n,r} \tag{3b}$$

où G est l'avantage d'utiliser une bande allouée, C_S et C_A sont les coûts de mise en œuvre du processus de surveillance et de l'attaque par usurpation sur une bande, et $\pi_{m,n,r}$ représente le coût pénalité attendue.

En pratique, au lieu de garder une stratégie pure, l'attaquant et le défenseur pourraient choisir leur stratégie au hasard. Cela forme une stratégie mixte pour chaque joueur. Les ensembles de stratégies mixtes de l'attaquant et du défenseur sont définis par $\{\alpha_n\}$ et $\{\delta_m\}$ où α_n et δ_m sont les probabilités d'usurper les utilisateurs de n et de surveiller les emplacements m. Les gains attendus des joueurs sont donnés par :

$$U_A = \boldsymbol{\alpha}^T \boldsymbol{\Pi}_A \boldsymbol{\delta} = \sum_n \alpha_n U_{A|n} = \sum_n \alpha_n \left(\sum_m \delta_m \Pi^A_{m,n,r} \right) \tag{4a}$$

$$U_D = \boldsymbol{\alpha}^T \boldsymbol{\Pi}_D \boldsymbol{\delta} = \sum_m \delta_m U_{D|m} = \sum_m \delta_m \left(\sum_n \alpha_n \Pi^D_{m,n,r} \right) \tag{4b}$$

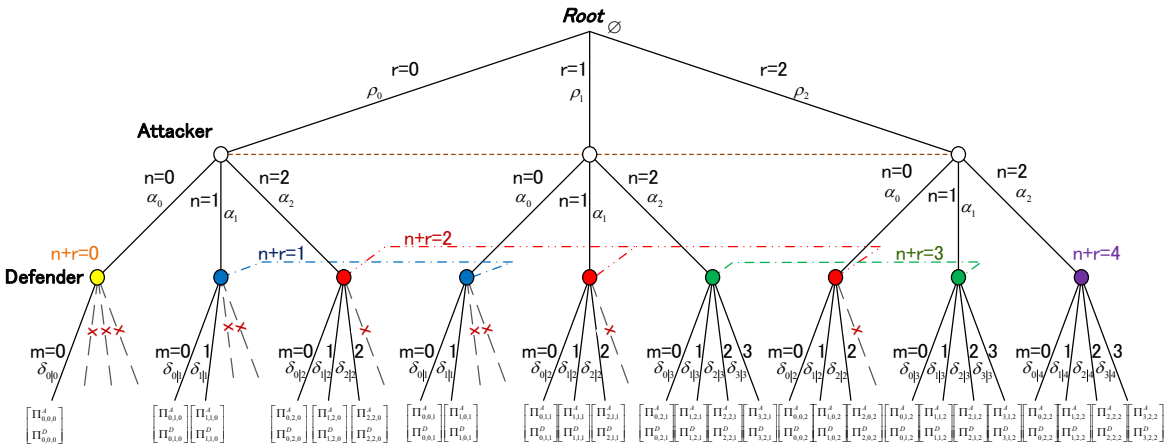


FIGURE 5 Le jeu de surveillance d'identification pour atténuer les attaques par usurpation lorsque $N = 2$, $M = 3$ et $R = 2$.

Equilibre de Nash : afin de trouver une solution à la meilleure stratégie de l'attaquant et du défenseur dans un tel jeu, nous explorons NE dans lequel chaque joueur a sélectionné la meilleure réponse aux stratégies de ses adversaires, et aucun joueur ne gagne rien en changeant uniquement sa propre stratégie. Le NE du jeu formulé (α_n^*, δ_m^*) doit donc remplir les conditions suivantes :

$$\begin{cases} U_A\left(\alpha_n^*, \delta_m^*\right) \geq U_A\left(\alpha_n, \delta_m^*\right) \\ U_D\left(\alpha_n^*, \delta_m^*\right) \geq U_D\left(\alpha_n^*, \delta_m\right) \end{cases} \tag{5}$$

Et, le problème de trouver NE est équivalent á un problème de bi-optimisation comme suit.

$$\begin{aligned} \underset{\boldsymbol{\alpha}}{\text{maximize}} \quad & \boldsymbol{\alpha}^T \boldsymbol{\Pi}_A \boldsymbol{\delta} \\ \underset{\boldsymbol{\delta}}{\text{maximize}} \quad & \boldsymbol{\alpha}^T \boldsymbol{\Pi}_D \boldsymbol{\delta} \\ \text{subject to} \quad & \mathbf{1}^T \boldsymbol{\alpha} = 1, \boldsymbol{\alpha} \geq 0 \\ & \mathbf{1}^T \boldsymbol{\delta} = 1, \boldsymbol{\delta} \geq 0 \end{aligned} \tag{6}$$

Le problème d'optimisation donné dans les équations ci-dessus peut être résolu en utilisant l'algorithme de Lemke-Howson [86].

Corollary 0.1. *Pour les cas de pénalités constantes, le jeu est équivalent au jeu bi-matrice $2 \times M$ où l'attaquant n'a que deux stratégies : ne pas attaquer et attaquer avec la pleine capacité des requêtes d'usurpation N.*

Stratégies d'identification du trafic de données

Si la demande réussit l'étape de vérification de l'emplacement, le coordinateur de réseau alloue alors la ressource de spectre à l'utilisateur. Cependant, les attaques par usurpation dídentifiant et même les attaques par usurpation démplacement pourraient passer en raison de la localisation imparfaite. Par conséquent, il est nécessaire de mener un processus de

surveillance supplémentaire pour vérifier si la ressource de spectre attribuée est utilisée ou non par le SU droit / enregistré. La vérification d'identité proposée peut être considérée comme un complément approprié au processus de vérification de l'emplacement de la demande. À l'instar de l'usurpation d'emplacement, l'attaquant peut envoyer plusieurs requêtes pour implémenter l'usurpation d'identité alors que le coordinateur du réseau peut effectuer plusieurs processus de vérification. La question ici est que, tant pour l'attaquant que pour le coordinateur du réseau, quel est le nombre optimal de demandes d'attaque et de processus de vérification ?

Nous formulons un jeu non coopératif de forme étendue pour analyser l'interaction entre l'attaque par usurpation d'identité et le processus de surveillance des identifiants comme suit.
Joueur

- **Attacker**, qui est également un utilisateur cognitif, implémente l'attaque par usurpation d'identité en envoyant jusqu'à N ID de requêtes d'usurpation.
- **Defender**, qui représente le coordinateur du réseau, peut effectuer le processus de vérification de l'identifiant pour détecter l'attaque par usurpation d'identifiant.

Stratégie :

- **Etape 1** : l'attaquant effectue une attaque par usurpation d'identité en envoyant n, $0 \leq n \leq N$ spoofing dans le type 4 ou le type 5 pour obtenir plus de ressources spectrales, où N indique la capacité d'attaque par usurpation maximale.
- **Etape 2** : le défenseur alloue des bandes de spectre $n + r$ pour les requêtes n de l'attaquant et les requêtes r des utilisateurs honnêtes.
- **Etape 3** : le défenseur analyse m, $0 \leq m \leq \min(M, n + r)$ les bandes de spectre allouées pour détecter l'attaque par usurpation, puis pénalisent l'attaquant, où M représente la capacité de surveillance maximale.

Dans ce cas, l'attaquant envoie des requêtes d'usurpation n ID sans connaître la vraie valeur de r, tandis que le défenseur analyse les bandes de spectre m en sachant le total des bandes de spectre allouées $n + r$. Par conséquent, l'ensemble de stratégies comportementales pures de l'attaquant est défini par

$$\mathbf{S_A} = \{\mathbf{n}, \mathbf{0} \leq \mathbf{n} \leq \mathbf{N}\},$$

et le jeu de stratégie comportementale pure du défenseur dépendant de $n + r$ est donné par

$$\mathbf{S}_{D|n+r} = \{m|(n + r), 0 \leq m \leq \min(M, n + r)\}.$$

Les ensembles de stratégies mixtes correspondants de l'attaquant et du défenseur sont définis par : $\boldsymbol{\alpha} = \{\alpha_n, 0 \leq n \leq N\}$ et $\boldsymbol{\delta}_{|n+r} = \{\delta_{m|n+r}, 0 \leq m \leq \min(M, n + r)\}$ où α_n est la probabilité de spoofing n demande et $\delta_{m|n+r}$ est la probabilité de surveiller les bandes de spectre m étant donné que les requêtes $n + r$ ont été allouées.

Puisque l'attaquant et le défenseur peuvent avoir les enregistrements historiques de la quantité de véritables SU situés dans la zone attaquée, nous supposons que la distribution du nombre réel de requêtes r est une connaissance commune. Sans perte de généralité, nous supposons que r suit la distribution de Poisson. La fonction de probabilité de masse (pmf) de r est donnée par :

$$f_{\Re}(r,\lambda) = \frac{\lambda^r e^{-\lambda}}{r!}, \tag{7}$$

où λ est un paramètre de distribution de Poisson, qui est égal á la valeur moyenne de r. Pour simplifier le jeu, nous supposons que r est tronqué par une valeur maximale R où $Pr[r \leq R] \geq \theta$ (θ désigne un seuil de probabilité, *e.g.*, $\theta = 0.99$). Cette hypothèse est acceptable car le jeu est formulé pour une petite zone où la différence démplacement des SU est indétectable par le processus de vérification des emplacements des expéditeurs de requêtes, et donc le nombre de SU peut être limité. Alors la probabilité de r est donnée en normalisant $f_R(r,\lambda)$ comme suit.

$$\rho_r = \frac{f_{\Re}(r,\lambda)}{\sum_{r=0}^{R} f_{\Re}(r,\lambda)} \tag{8}$$

En principe, le jeu formulé peut être converti en un jeu de forme stratégique en adoptant la transformation Harsanyi [78]. Cela signifie que le jeu de stratégie pur du défenseur peut être construit sur la combinaison de tous les ensembles de stratégies purement conditionnels possibles. Cependant, le nombre d'éléments de la stratégie du défenseur augmente de manière exponentielle avec la taille du jeu. Par conséquent, il est trop compliqué de résoudre le jeu par la transformation de Harsanyi. Au lieu de cela, nous utilisons l'approche de la séquence de représentation [76] pour exprimer le jeu formulé.

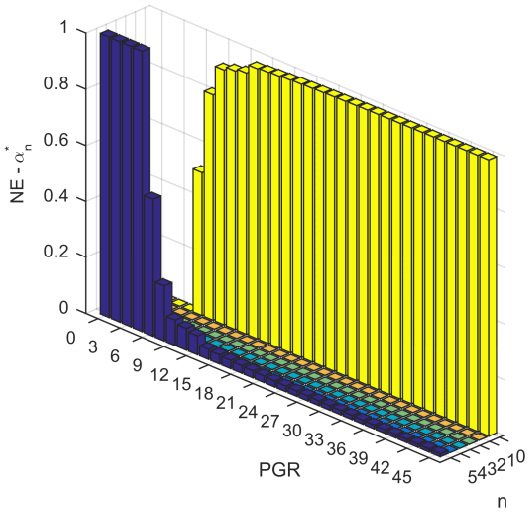
Résultats de la simulation

Afin d'analyser le NE du jeu pour les deux cas de politique de pénalité, nous définissons le ratio pénalisation/gain (PGR) qui est équivalent au nombre d'intervalles de temps d'interdiction sur un attaquant capturé. En particulier, le PGR est donné par

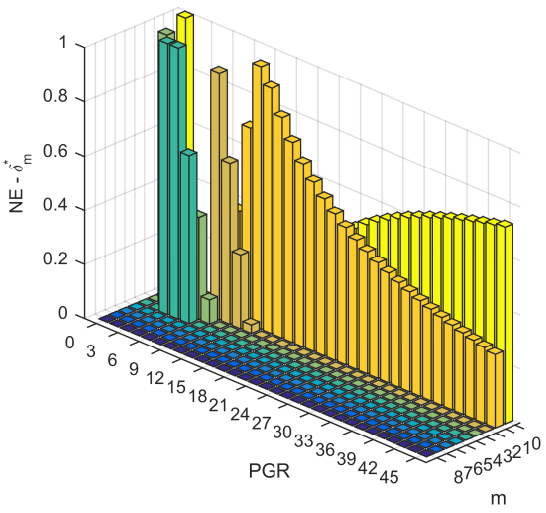
$$PGR = \frac{P}{G}, \tag{9}$$

où G est le gain de l'utilisation d'une bande de spectre dans un intervalle de demande, *i.e.*, l'intervalle entre deux temps de requête adjacents.

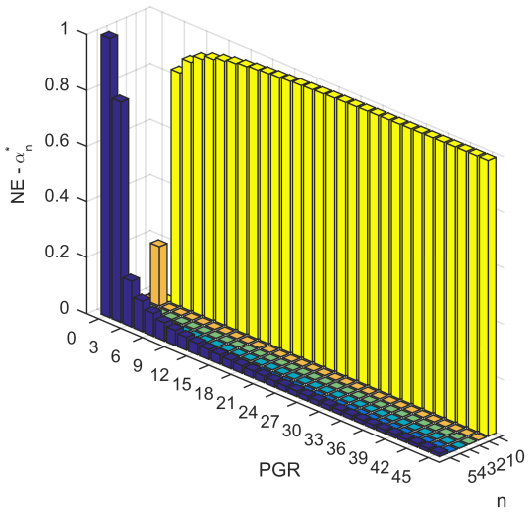
Nous étudions d'abord le processus de vérification afin d'atténuer les attaques par usurpation d'emplacement dans les réseaux CR. Pour que les résultats de la simulation soient clairs et faciles à suivre, nous commençons avec un numéro CRN avec 6 actifs dans la zone vérifiée (*i.e.*, $r = 6$) dans lequel l'attaquant peut envoyer jusqu'à 5 de demande d'usurpation (*i.e.*, $N = 5$) et le défenseur peut surveiller jusqu'à 8 emplacement de demande (*i.e.*, $M = 8$).



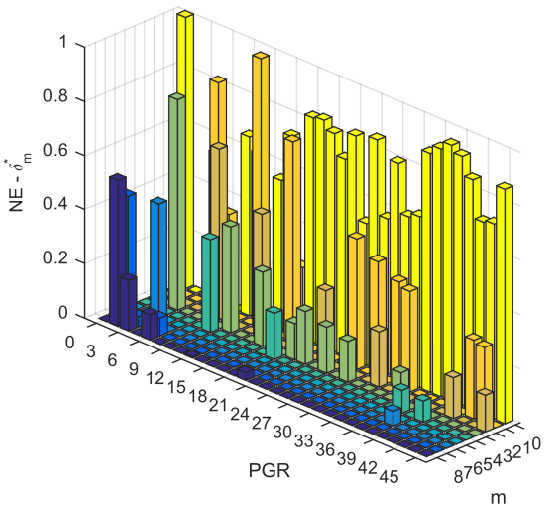
(A) Attaquant - Pénalité constante



(B) Défenseur - Pénalité constante



(C) Attaquant - Pénalité liée au montant



(D) Défenseur - Pénalité liée au montant

FIGURE 6 NE vs. PGR quand $r = 6$, $N = 5$, et $M = 8$.

Supposons que $G = 10$, $C_S = 2$ et $C_A = 1$. Noté que C_A est le coût d'envoi d'une demande au coordinateur de réseau sur un canal de contrôle, tandis que C_S est le coût de la localisation de l'expéditeur de la requête. Ainsi, il est raisonnable de supposer que $C_A \ll G$ et $C_A < C_S$. Les résultats sont obtenus en adoptant lálgorithme de Lemke-Howson sur le jeu original avec la taille $N \times M$. Les résultats de la simulation montrent que les politiques de pénalité affectent la sélection des stratégies NE des deux joueurs.

Ensuite, nous étudions le processus de vérification pour atténuer l'attaque par usurpation d'identité dans les réseaux CR. La figure ci-dessus représente la pénalité de retard moyenne que láttaquant doit subir en considérant NE, uniforme (*i.e.*, láttaquant exécute ses stratégies

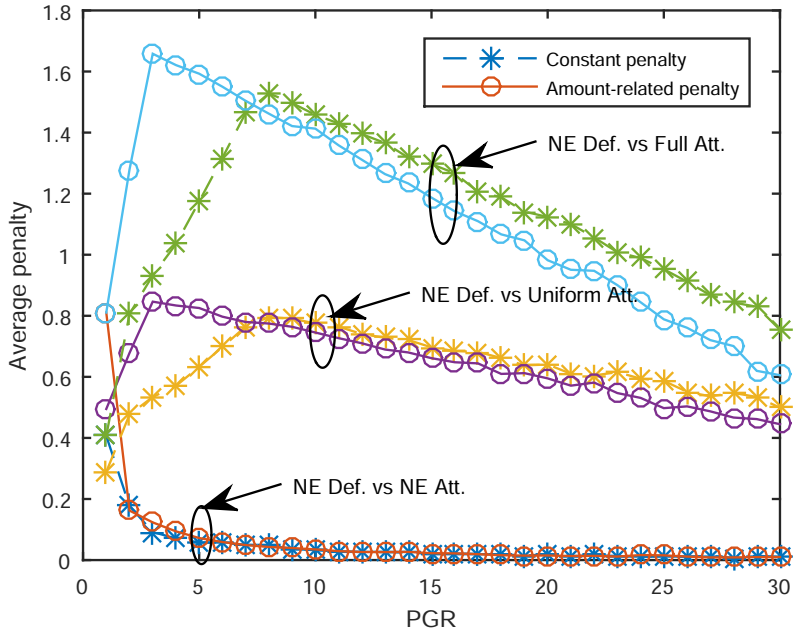


FIGURE 7 Average delay penalty vs. PGR.

pures également), et des stratégies dáttaque complètes (l'attaquant attaque toujours avec la pleine capacité). Une simulation Monte Carlo avec 10^6 samples est adoptée, quand $(M, N, R) = (3, 2, 6)$ et $\lambda = 2$. Deux politiques de pénalités sont envisagées. A partir des résultats de la simulation, nous avons observé que l'attaquant était sérieusement retardé s'il essayait d'augmenter son taux d'attaque et qu'il y avait un point optimal pour définir les pénalités *i.e.*, 8 pour la pénalité constante et 3 pour la pénalité liée à la quantité capturée, où l'attaquant subit les retards les plus importants. Cela signifie que, en utilisant NE et en définissant la pénalité appropriée, le défenseur pourrait imposer une meilleure application de la réduction de láttaque égoïste.

Auto-coexistence dans les réseaux de RC distribués : cadre de répartition des ressources en collaboration

L'absence d'un coordinateur de réseau pour contrôler le partage du spectre des réseaux d'infrastructures distribuées constitue un défi majeur pour assurer la coexistence entre les SU indépendantes. Généralement, le mécanisme de coexistence est considéré en trouvant une stratégie dállocation de ressources qui permet aux SU dútiliser simultanément la bande de fréquences. Ainsi, le principal intérêt de ce chapitre est de concevoir une stratégie efficace dállocation de ressources entre utilisateurs cognitifs tout en conservant certaines exigences de qualité de service (QoS) sur le réseau principal. Étant donné que le contrôle de la puissance est un aspect important de la conception de tout système de communication, en particulier

dans un canal multi-utilisateurs interférant tel que lénvironnement multi-utilisateur cognitif, ce chapitre se concentre sur la proposition dúne stratégie. allocation de puissance. La stratégie proposée, cependant, ne se limite pas au contrôle de puissance adaptatif. D'autres aspects de l'allocation des ressources, tels que la sélection des canaux, la planification des utilisateurs, la conception de la formation de faisceaux ou du précodage et la planification de la couche MAC, peuvent être explorés dans cette étude.

La principale contribution de ce chapitre est le développement d'un cadre de contrôle collaboratif de la puissance, dans lequel les SU utilisent une plus grande intelligence pour éviter les interférences tout en optimisant le spectre en collaborant avec d'autres pour déterminer la meilleure utilisation. de l'appareil. spectre spectral pour d'autres. En particulier, chaque utilisateur optimise sa stratégie dállocation de puissance de manière collaborative grâce à un objectif modifié, qui inclut non seulement sa propre performance, mais aussi celle des autres. Le paradigme proposé présente les avantages de l'approche distribuée, à savoir les algorithmes de convergence à faible complexité et rapide avec une implémentation distribuée, et surmonte les inconvénients de l'approche centralisée, tels que la complexité, les frais généraux, etc. Plus précisément, nous développerons de nouveaux jeux qui réduiront les écarts de performance par rapport à lóptimisation conjointe, tout en maintenant límplémentation distribuée. Contrairement au travail précédent, qui portait sur la maximisation de lútilité avec la contrainte de puissance [33, 35, 36, 38], nous considérons le problème du contrôle de puissance maintenir une certaine qualité de transmission pour chaque utilisateur.

En général, les problèmes d'optimisation du contrôle de puissance multi-utilisateurs ne sont pas concaves. L'obtention d'une solution globale est très complexe. Afin de résoudre ce problème, nous proposons une méthode simple pour résoudre efficacement ces problèmes en approximant la fonction d'utilité du jeu pour chaque région du SINR du réseau : la région SINR haute et la région SINR basse. En adoptant le processus d'approximation, nous obtenons un jeu bien connu, tel que le jeu potentiel [33] ou le jeu concave [98], plus facile que le jeu d'origine à trouver la stratégie NE. La stratégie d'allocation de puissance est ensuite analysée à travers le NE de ce jeu. L'algorithme dynamique de la meilleure réponse invite alors l'étude sur l'existence et l'unicité du NE dans le jeu.

Modèle du système et formulation du problème

Nous considérons le problème d'allocation de puissance dans un réseau CR avec des de N indépendantes SUs, chacune étant constituée d'un couple émetteur-récepteur, partageant une bande de fréquence commune. Le réseau considéré correspond à un système de communication sans fil avec des paires émetteur-récepteur indépendantes N, où la transmission de chaque émetteur provoque des interférences à la réception d'autres récepteurs.

Nous modélisons ce scénario comme un canal d'interférence gaussien avec évanouissement plat, où chaque récepteur perçoit le signal transmis avec un bruit gaussien blanc additif. Soit

$g_{j,i}$ le gain de puissance du canal j au récepteur i du réseau CR et σ_i^2 la puissance de bruit au récepteur i. Par conséquent, $g_{i,i}$ est le gain de puissance du canal entre l'émetteur et le récepteur de l'utilisateur i. Noter $\mathbf{p} = \{p_1, p_2, \ldots, p_N\}$ le vecteur comprenant les *puissance allouée* de tous les SU et $\mathbf{p}_{-i}$ le vecteur de puissance de toutes les SU sauf i. Le SINR au récepteur i, noté γ_i, est donné par

$$\gamma_i(p_i, \mathbf{p}_{-i}) = \frac{g_{i,i}p_i}{\sigma_i^2 + \sum\limits_{j \neq i} g_{j,i}p_j} \tag{10}$$

Supposons que chaque utilisateur puisse ajuster sa puissance de transmission dans une région limitée ($[0, p_i^{\max}]$) pour répondre à une contrainte donnée *cible SINR*. Pour l'utilisateur i, cela signifie que

$$\gamma_i \geq \gamma_i^{tar}, \tag{11}$$

où γ_i^{tar} est le *SINR cible* donné de l'utilisateur i.

Au cours de la période considérée, nous supposons que les gains de canal sont fixes (*i.e.*, les effets d'évanouissement se produisent à une échelle de temps beaucoup plus lente). Soit $r_i(p_i, \mathbf{p}_{-i})$ le taux de l'utilisateur i. Alors,

$$r_i(p_i, \mathbf{p}_{-i}) = \log_2(1 + \gamma_i(p_i, \mathbf{p}_{-i})) \tag{12}$$

Pour chaque utilisateur i, nous avons défini le *indicateur de performance* $f_i\left(p_i, \mathbf{p}_{-i}\right)$ qui capture un compromis entre le taux de transmission obtenu et le coût de l'énergie pour le processus de transmission de données. Ces métriques sont ensuite données par

$$f_i\left(p_i, \mathbf{p}_{-i}\right) = r_i\left(p_i, \mathbf{p}_{-i}\right) - c_i p_i, \tag{13}$$

où c_i est le facteur de tarification de l'utilisateur i [62].

Nous considérons la collaboration entre utilisateurs cognitifs en proposant la fonction *d'utilité collaborative*. Au lieu de tenir compte de ses propres performances ou de la fonction d'utilité commune, chaque utilisateur optimise sa fonction d'utilité collaborative qui comprend non seulement ses propres performances mais également celles des autres. Pour simplifier, nous supposons que la fonction dútilité collaborative de chaque utilisateur dans le cas de la bande de fréquences sous licence est

$$U_i^{col}\left(p_i, \mathbf{p}_{-i}\right) = \underbrace{f_i\left(p_i, \mathbf{p}_{-i}\right)}_{\text{performance metric}} + \underbrace{g_i\left(p_i, \mathbf{p}_{-i}\right)}_{\text{collaboration metric}} \tag{14}$$

où *métrique de collaboration* $g_i\left(p_i, \mathbf{p}_{-i}\right)$ est supposé être la somme partielle des performances des autres, *i.e.*,

$$g_i\left(p_i, \mathbf{p}_{-i}\right) = \sum_{j \neq i} \alpha_j f_j\left(p_j, \mathbf{p}_{-j}\right), \tag{15}$$

et $\alpha_j \geq 0$ est le *facteur de collaboration* pour l'utilisateur j.

Dans l'allocation collaborative d'énergie, chaque utilisateur vise à *maximum* sa fonction d'utilitaire collaboratif, *i.e.*,

$$\begin{aligned} \max_{p_i} \quad & U_i^{col}(p_i, \mathbf{p}_{-i}) \quad \forall i = 1, \ldots, N \\ \text{s.t.} \quad & p_i \in [0, p_{\max}^i] \\ & \gamma_i \geq \gamma_i^{tar} \end{aligned} \tag{16}$$

Formulation du jeu

En raison du conflit et des compromis entre les objectifs des utilisateurs du réseau, l'approche de la théorie des jeux est utilisée pour modéliser la relation entre les utilisateurs du réseau. Nous avons considéré le jeu de contrôle de la puissance collaboratif

$$\mathcal{G} \triangleq \{\mathcal{N}, \{\mathcal{P}_i(\mathbf{p}_{-i})\}_i, \{U_i^{col}(p_i, \mathbf{p}_{-i})\}_i\}, \tag{17}$$

où $\mathcal{N} = \{1, 2, \ldots, N\}$ est l'ensemble des lecteurs, $\mathcal{P}_i(\mathbf{p}_{-i})$ est le jeu de stratégie du joueur i tel que $\gamma_i \geq \gamma_i^{tar}$.

Généralement, un équilibre de Nash (NE) d'un jeu est une stratégie réalisable à partir de laquelle les joueurs ne peuvent pas gagner en ajustant indépendamment leur stratégie. Pour $\mathcal{G}$, $(p_i^*, \mathbf{p}_{-i}^*)$ est un NE si et seulement si

$$U_i^{col}(p_i^*, \mathbf{p}_{-i}^*) \geq U_i^{col}(p_i, \mathbf{p}_{-je}^*) \; \forall p_i \in \{\mathcal{P}_i(\mathbf{p}_{-i})\}_i \tag{18}$$

Pour déterminer le NE du jeu, le processus itératif en résolvant itérativement les problèmes couplés de N peut être utilisé. Dans un tel processus, chaque utilisateur sélectionne de manière itérative la meilleure réponse (BR) (ou l'une des BR) aux stratégies des autres. Les questions importantes dans l'analyse d'un jeu non coopératif sont d'étudier l'existence et l'unicité d'un équilibre, et si la mise en œuvre du BRD finit par donner un équilibre. Dans notre jeu, cependant, la question est plus difficile depuis

— la fonction objectif est non concave et non quasi concave, et

— non seulement la fonction utilitaire mais aussi le jeu de stratégie de chaque joueur sont un couplage mutuel, en fonction des actions des autres joueurs dues aux contraintes SINR.

À cette fin, nous proposons des méthodes peu complexes pour résoudre efficacement ces problèmes en rapprochant la fonction utilitaire du jeu pour chaque région du réseau SINR grâce aux fonctionnalités suivantes :

— Pour la région SINR haute (que les utilisateurs sont éloignés ou $\gamma_i \gg 1$), le taux $\log_2(1+\gamma_i)$ et $\log_2(1+\gamma_i)$ peuvent être approximés par $\log_2(\gamma_i)$, *i.e.*, $\log_2(1+\gamma_i) \approx \log_2(\gamma_i)$. Le jeu est un jeu potentiel exact. NE est unique si $\sum_{j \neq i} \alpha_j \leq 1$, $\forall i \in \mathcal{M}$.

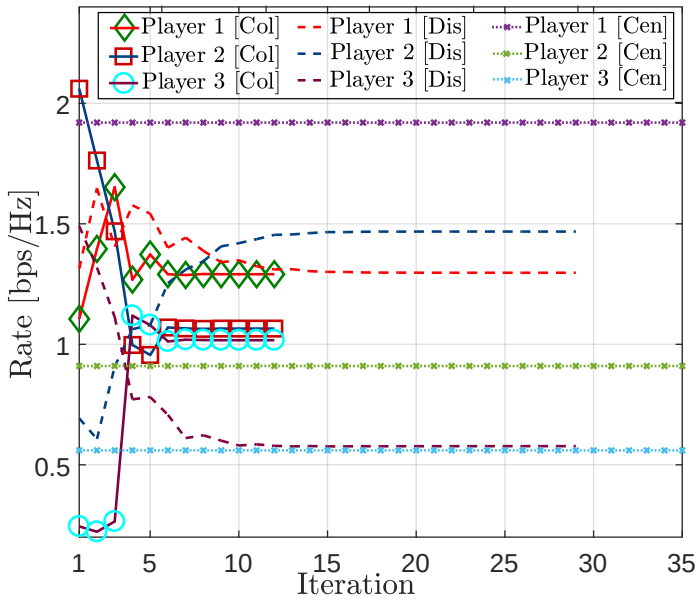


FIGURE 8 Le taux de chaque utilisateur CR avec l'allocation de puissance collaborative basée sur le jeu potentiel, le contrôle de puissance distribué et le contrôle de puissance centralisé pour le réseau CR avec une région SINR élevée où $\alpha_i = 1/3, \forall i = 1, 2, 3$.

— Pour la région SINR basse (c'est-à-dire autrement), puisque la fonction d'utilité est continue et différentiable, elle peut donc être approchée par une fonction linéaire via l'approximation de Taylor du premier ordre. Le jeu est un jeu concave.

— Pour le grand réseau, le processus hybride qui contient à la fois une approximation logarithmique et une approximation linéaire est utilisé. Le jeu est un jeu concave avec une fonction utilitaire standard. Ainsi, le NE est unique et peut être déterminé par lálgorithme BRD de la manière distribuée.

Résultats de simulation

Tout d'abord, nous considérons le réseau CR dans la région SINR haute avec l'approche de jeu potentialisée. Les facteurs de collaboration sont $\alpha_i = 1/3$ $(i = 1, 2, 3)$. Les résultats de la simulation montrent que le paradigme du contrôle collaboratif de lénergie offre une meilleure équité entre les utilisateurs, de meilleures performances et un temps de convergence réduit. De plus, le taux de somme du système dépend fortement des facteurs de collaboration. Nous affirmons que, dans le scénario SINR élevé, plus le SINR est élevé, plus le facteur de collaboration est petit. Nous examinons ensuite le réseau d'interférence sans fil dans la région des bas SINR. L'approche de jeu concave est adoptée pour déterminer l'allocation de puissance collaborative optimale. Les facteurs de collaboration sont $\alpha_i = 1/3$, $(i = 1, 2, 3)$. Afin de simplifier le probléme, nous supposons que les points initiaux pour le processus d'approximation sont nuls, *i.e.*, $z_i = 0$, $\forall i$.

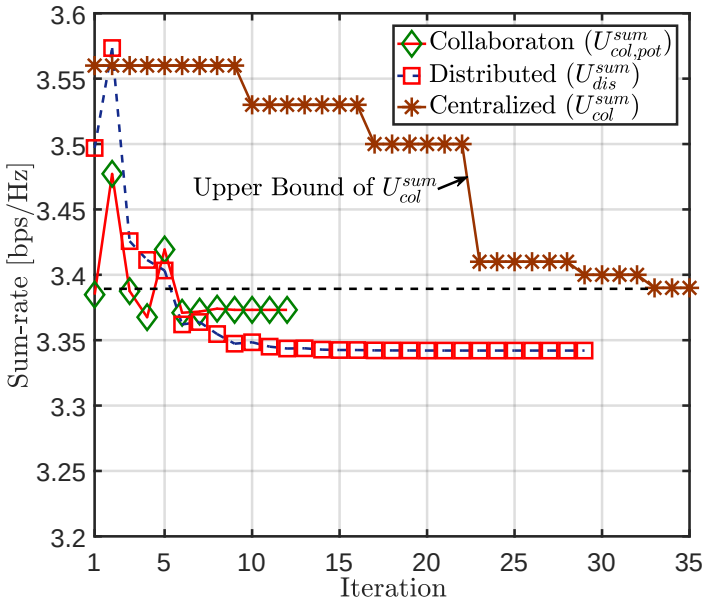


FIGURE 9 Le taux de somme du réseau avec l'allocation de puissance collaborative basée sur le jeu potentiel, le contrôle de puissance distribué et le contrôle centralisé de l'alimentation pour le réseau CR avec une région SINR élevée où $\alpha_i = 1/3, \forall i = 1, 2, 3$.

Á l'instar du premier scénario, les résultats de la simulation montrent que le paradigme collaboratif offre une meilleure équité, de meilleures performances et un temps de convergence plus court que la méthode conventionnelle. De plus, le taux de somme du systéme dépend fortement des facteurs de collaboration. En outre, nous concluons que la sélection de points zéro pour le processus d'approximation sera plus bénéfique lors de l'étude de l'allocation de puissance collaborative basée sur la structure de jeu concave.

Enfin, pour le réseau avec un grand nombre dútilisateurs, nous avons utilisé le contrôle de puissance collaboratif basé sur lápproche de potentiel concave. Un réseau d'interférence sans fil avec $N = 5$ utilisateurs est considéré, oú les points initiaux pour le processus d'approximation sont (i) zéro et (ii) la puissance maximale, respectivement. Nous observons que, compte tenu du contrôle de puissance collaboratif basé sur lápproche concave-potentiel, le taux de somme obtenu est supérieur à celui obtenu par le contrôle de puissance réparti et est proche de celui obtenu par le contrôle de puissance centralisé. . De plus, son taux de convergence est beaucoup plus rapide que le contraire. Nous concluons que, pour le grand réseau, il sera préférable d'adopter l'approche d'approximation du jeu concave potentiel. Sinon, nous adoptons l'approche de jeu potentielle pour le réseau avec la région High SINR et l'approche de jeu concave pour le réseau avec la région Low SINR.

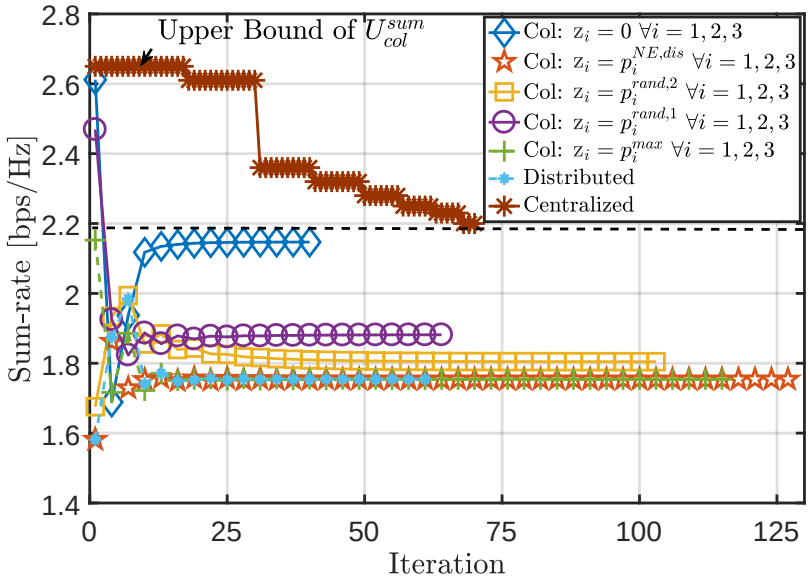


FIGURE 10 La somme de la prise en charge du réseau CR en utilisant l'allocation de puissance collaborative basée sur la structure de jeu concave pour certains z_i initiaux.

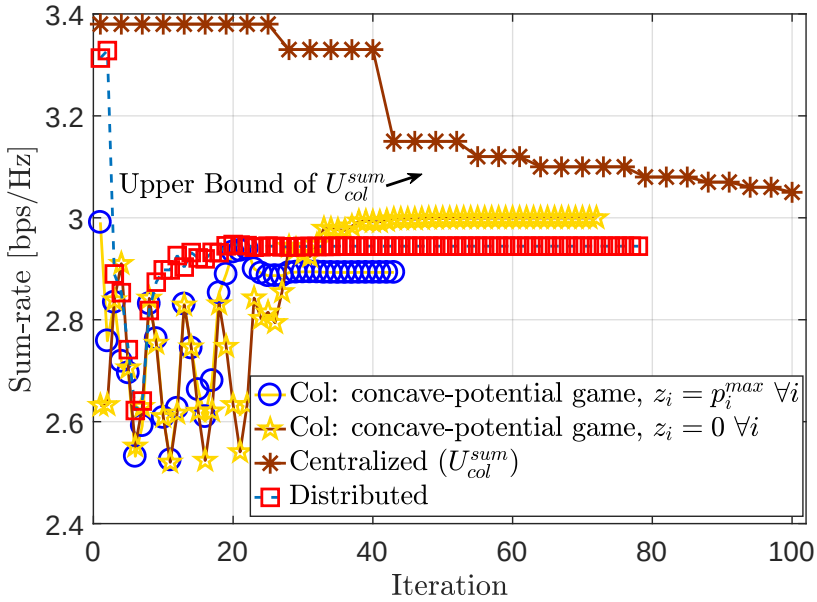


FIGURE 11 Le taux de somme du réseau CR avec $N = 5$ utilisateurs obtenu en utilisant la stratégie d'allocation collaborative basée sur le framework de jeu concave potentiel.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Context

The wireless revolution is creating a huge demand for accessing to the radio frequency (RF) spectrum with the explosion of the number of connected devices and the large diversity of use cases and requirements. According to the World Wireless Research Forum (WWRF), approximately 7 trillion wireless devices will be served in the field by 2020 [1, 2]. These will cover not only telecommunications but also new application areas such as manufacturing, e-health, traffic management and environmental monitoring. However, besides with the explosive increase of demand for wireless access, we are now facing a serious problem of an increasing scarcity of RF spectrum. The static spectrum allocation approaches, which divide the RF spectrum resources into exclusively licensed bands that are authorized for the licensed users (or referred to the primary users (PUs)) and leave some small bands for the other objectives (*e.g.*, industrial, scientific and medical, ISM bands) is not adapted to the dynamics of supply and demand for the wireless communications. In addition, the static spectrum allocation approaches have led to the spectrum underutilization since the allocated frequency band are inaccessible by unlicensed users (or referred to the secondary users (SUs)) even if it is unused by the licensed users. The conflict between the spectrum scarcity and the spectrum underutilization, therefore, results in the remarkable inefficiency of wireless communications and impedes deployment of new wireless communication-based applications.

In order to alleviate the spectrum scarcity and better utilize the RF spectrum resources, dynamic spectrum access (DSA), which allows the SUs to reuse the licensed bands without interfering with the neighboring PUs and share the unlicensed bands with other wireless users, have attracted much attention [3, 4]. As illustrated in Figure 1.1, by enabling the dynamic access, the SUs are allowed to dynamically sense the surrounding electromagnetic environments to adapt their operation and opportunistically access to temporally underutilized spectrum bands (also referred to the spectrum holes or radio white spaces) and avoid the possible harmful interference on the PUs (*i.e.*, the total interference received at the PU from

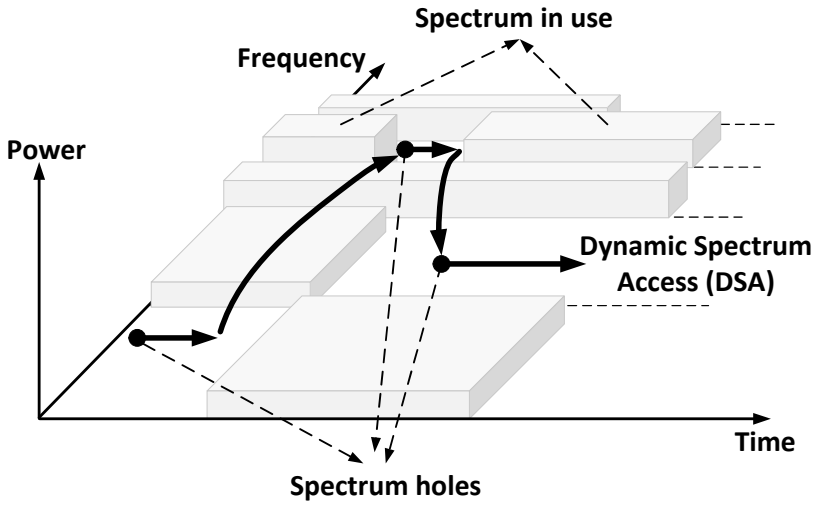


FIGURE 1.1 The spectrum holes concepts [1].

all SUs is below a threshold level). Thus, DSA promises to provide more flexibility and efficiency in spectrum usage.

In a dynamic spectrum access context, the spectrum management process consists of four main spectrum management phases, which are given as follows. In the first phase (*i.e.*, the sensing phase), the electromagnetic environment is sensed to detect the presence of the PU's signal or the activity of other SUs in the considered spectrum bands. The corresponding sensing results are then analyzed in the second phase (*i.e.*, the analysis phase) to identify the spectrum holes as well as the channel characteristics (*e.g.*, the estimated channel state information (CSI), the channel's capacity, etc.). In the next phase (*i.e.*, the reasoning phase), the estimated information on the radio environment is used for making the decision on whether or not to use the spectrum at specific times or locations. Finally, in the fourth phase (*i.e.*, the adaptation phase), certain transmission parameters are changed to achieve highly reliable communication in the secondary network and efficient utilization of the radio spectrum. Through the interaction with the radio environment, these four phases form a cognitive cycle [5], which is illustrated in Figure 1.2.

Considered as a promising candidate to achieve dynamic spectrum access, cognitive radio (CR) [3, 6] is an intelligent radio technology that can automatically detect spectrum opportunities in a wireless spectrum band; then adapt transmission parameters based on the interaction with its environment for enabling more communications to run concurrently. In particular, on licensed spectrum bands, CR enables the cognitive radio users (*i.e.*, the SUs) to dynamically access the temporarily vacant spectrum holes (*i.e.*, the entire bands that are not used by incumbent radio systems in time or space) without any interfering to and changing in the PUs devices and protocols. In addition, in consideration of the overcrowded, unlicensed spectrum bands, CR allows the SUs to opportunistically share these bands with other users. Some example applications of CRs include the emergency and public

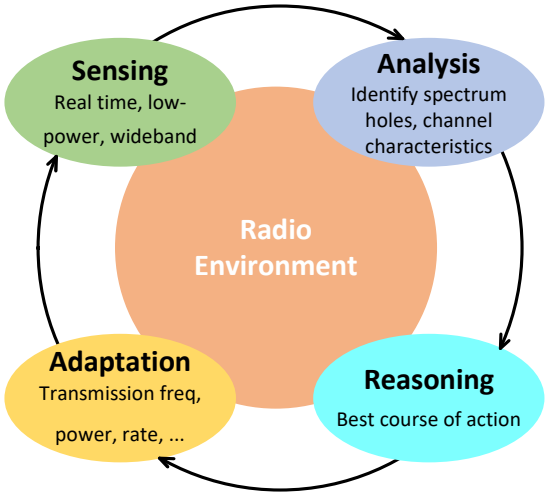


FIGURE 1.2 Cognitive radio functionality under cognitive cycle.

safety communication in the white space spectrum bands (*e.g.*, the TV bands, the wireless microphone bands, etc.), the radio communication-based military actions, or the cognitive radio satellite communications which exploit the idea of cognitive radio to solve the spectrum scarcity on satellite communications. Typically, CRs along with the software-defined radio (SDR), a fully re-configurable RF front-end, which the RF operating parameters can be altered by software. It allows cognitive radio users to easily implement new radio functions, such as the spectrum sensing, and reconfigure the operation parameters. For these reasons, it is envisioned that CR will be a key technology for the next generation wireless communication systems.

Following the conventional literature, cognitive radio networks can be classified into the following two architectures according to the network infrastructure [1, 3] as in Figure 1.3.

— **Centralized infrastructure-based CR networks**: the coordination among cognitive radio users is assumed to perform the spectrum sensing and the data transmission process. A cognitive radio base-station (or referred to CBS), which is a fixed network device with cognitive radio capabilities, plays the role of the coordinator and provides connection to SUs without spectrum access license. Cognitive users can access their own CBS both in licensed and unlicensed spectrum bands. In particular, the CBS manages the operation of the SUs inside the cell as well as the collaboration with the CBSs of the cognitive radio systems in the other cells with overlapped coverage areas to ensure the opportunistic transmission and the self-coexistence among CR networks. One example of the centralized-based CR networks is the IEEE 802.22 standard [7, 8], which defines the specification of opportunistic communications in the spectrum of TV bands (or referred to the TV White Spaces (TVWS)) and the wireless microphone bands. Another example is the IEEE 802.11af standard for the dynamic spectrum sharing between unlicensed users and licensed users in the

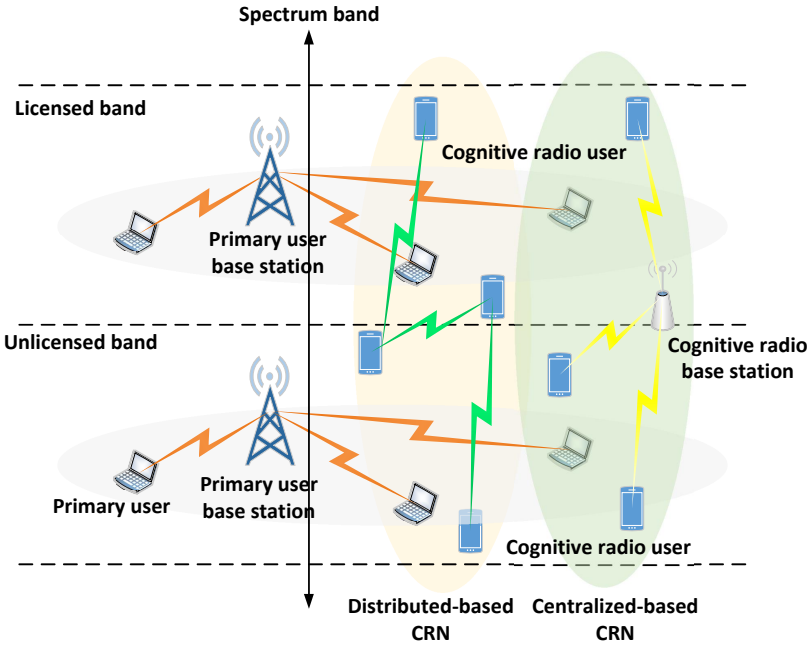


FIGURE 1.3 The classification of cognitive radio networks.

VHF and UHF bands between 54 and 790 MHz [9]. In the 802.11af standard-based CR networks, the spectrum access is provided through the authorized geo-location database with the registered location secure server, which stores the frequency usage map by geographic location and the operating parameters for cognitive users to fulfill regulatory requirements.

— **Distributed infrastructure-based CR networks**: no coordination among cognitive users is assumed to perform the spectrum sharing, the data transmission and the self-coexistence process between cognitive radio users. In particular, SUs can communicate with each other through the point-to-point ad-hoc connections on both licensed and unlicensed spectrum bands. Due to the absence of a controlling centralized entity, cognitive users jointly coordinate their spectrum access by utilizing some global mechanisms such as the network-wide synchronization and the cooperative detection and communication. The joint coordination process helps to establish a coexistence protocol among SUs and also improves the overall network performance. One example of the distributed-based CR networks is the CR approach for usage of virtual unlicensed spectrum (CORVUS) system [10], which exploited the unoccupied licensed bands for data transmission between SUs. Other examples include the Nautilus distributed, scalable and efficient coordination framework for the open spectrum ad-hoc networks [11–13] and the peer-to-peer mode of DARPA's neXt Generation (XG) dynamic access network [3, 14].

Different architectures impose different pros and cons for the establishment of CR networks. The centralized architecture can achieve better overall performance but depends on the operation of the CBS since its failure can affect the functioning of the system. The distributed architecture, on the other hand, is easy to deploy but expensive and requires a joint coordination protocol among SUs to ensure the spectrum sharing process.

The successful deployment of cognitive radio networks depends on the coexistence mechanisms between primary users and the cognitive radio users as well as the self-coexistence mechanisms among SUs [5, 7, 8, 14–16]. The former, which is characterized by the ability of CRs to detect and exploit the spectrum opportunities without causing harmful interference to PUs, mainly solved through the spectrum sensing process [7, 8] or the frequency usage map by geographic location [9, 17, 18]. The latter, on the other hand, is characterized by the ability to share the spectrum fairly for multiple users in overlapping coverage areas. In addition, when SUs share the same frequency bands, the misbehaving and rational cognitive users can try to act greedily by occupying more spectrum bands [19–21] or obstructing the network operation [22, 23]. Therefore, deployment of the self-coexistence mechanisms between SUs is a particularly important challenge that needs to be addressed in CR networks and the aim of the thesis.

1.2 Self-Coexistence Challenges in Cognitive Radio

Maintaining a harmonized coexistence between the cognitive users is a key problem in the cognitive radio networks. Depending on the network architecture, the corresponding coexistence issues are as follows.

— **Centralized-based CR networks**: the network coordinator controls the operation of the network, such as the spectrum access and also the self-coexistence among SUs. In such a case, the spectrum opportunities are determined by the spectrum sensing-based [24] approach or the database driven-based [25, 26] approach. In the former approach, primary system's activity is explored by measuring the radio environment spectrum. In the latter approach, a database server with an online geo-location map of spectrum usage is responsible for managing the spectrum access process. The studies on coexistence mechanisms in centralized-based CR networks examine the corresponding CR functionality under the presence of misbehaving users. In other words, these studies provide mitigation methods to deal with the security threats caused by misbehaving users. Specifically, an intelligent and rational misbehaving user, which is equipped with the SDR hardware, may cause the circumvention of the spectrum sensing process by:

  — **Spectrum sensing data falsification (SSDF)**: sharing the falsified local sensing result to the fusion center which causes a degradation on the accuracy of cooperative spectrum sensing process [22, 23]. Such kind of attack, which is known as the

Byzantine attack in cooperative spectrum sensing process, is usually taken by the malicious behaving users. The main goals of the misbehaving users are to decrease the probability of detection and increase the probability of false alarm of the spectrum sensing process. Consequently, it may disturb the normal operation of the network and prevent the access opportunities of other SUs.

— **Primary user emulation attack (PUEA)**: emulating the primary signals to force the other SUs in the spectrum-sensing based CR networks to vacate the spectrum bands [19–21, 27]. Such kind of attack can be caused by malicious or selfish behaving users. The malicious attacker targets at obstructing the secondary users from identifying and using vacant spectrum bands, hence ruining the operation of the CR networks, similar to the conventional Denial-of-Service (DoS) or jamming attack. On the contrary, the selfish attacker aims at illegitimately occupying channel resource and preventing other secondary users from accessing. Therefore, the PUEA considerably influences the operation of the CR networks. Moreover, the selfish PUEA may create an unfair obstruction to the CR networks and possible unnecessary interference to the nearby PUs.

— **Spoofing attacks**: spoofing the location or the identification (ID) of the cognitive users to fool the registered location server in the geo-location database driven-based CR networks [17, 18, 28–30], such as the IEEE 802.11af. One of the key points for deploying the geo-location database driven-based CR networks is the availability and the accuracy of the devices' location. Adversaries can spoof request messages with either faked identification (ID) or faked location information, hence considerable interference on both primary and cognitive radio systems and reduces the spectrum fairness between SUs.

— **Distributed-based CR networks**: due to the lack of a coordinator to control the spectrum sharing process, ensuring the coexistence between independent SUs with fair spectrum allocation and efficient spectrum utilization is a great challenge. Most of the related work in this field focused on finding a resource allocation mechanism between SUs in order to ensure the signal quality of the primary systems (*e.g.*, the interference at the PU's receiver in the licensed spectrum bands is below a threshold value) or the quality of point-to-point transmission link of the cognitive user (*e.g.*, the signal-to-interference-plus-noise-ratio (SINR) at the SUs' receiver in the unlicensed bands is above a threshold value). Acting as a rational and intelligent entity, each SU selfishly adjusts its transmission strategy (*e.g.*, the transmission power or the frequency bands) to maximize its own performance by the distributed strategy based on non-cooperative game approach [31–37] or the overall performance of the network by the centralized strategy based on the joint optimization approach [37–43].

On the spectrum sensing-based CR networks, the presence of an emulated primary signal is more dangerous than the SSDF since it leads to the prohibition of secondary users from

accessing to the channel immediately [15, 20, 44]. Consequently, this kind of attack reduces the spectrum access of the CRNs and thus severely degrades their operations. Therefore, combating the PUEA is crucial and is therefore the purpose of this thesis.

The literature work in the mitigation method to deal with the PUEA in spectrum-sensing based CR networks mainly focus on the transmitter verification scheme to authenticate the primary user signal from the emulated signals [21, 45–49] or the game theory-based scheme for overcoming the PUEA [50–54]. The former approach, however, requires a considerable change in the primary hardware or the primary transmission protocol, which is inapplicable in real scenario. In addition, the latter approach faces a vulnerability if an attacker conducts multi-channel attacks since the CR networks usually work on multiple frequency bands and because of the rapid expansion of software-defined radio. The main unaddressed research problems hence include: i) the investigation of the CR networks' security vulnerabilities and threats under the assumption of the multi-channel attacks, ii) the appropriate interaction between the network coordinator and the attacker for different types of attackers.

On the database driven-based CR networks, the spoofing attack is a critical vulnerability of the database driven-based CR networks. However, to the best of our knowledge, there is no work that systematically examines the impacts of spoofing attacks on database driven-based CR networks. The most relevant related work which considers the GPS spoofing attacks in a database driven-based CR networks is presented in [17], but limited due to the impact of false localization from the attacked GPS signals. Therefore, the consideration of spoofing attack in the database driven-based CR network and the corresponding mitigation methods of these spoofing attacks is an important unaddressed research problem that must be taken into account.

On the distributed-based CR networks, recent works on the resources allocation issues to ensure the coexistence between SUs mainly focus on the two following strategies: the distributed strategy [31–37] and the centralized strategy [38–43]. These approaches, however, face the problem of the global optimum, the system-level performance as well as the complexity and overhead. Moreover, to harvest the full capacity out of the RF spectrum, future wireless networks will need to use more intelligence to avoid interference while optimizing the spectrum by collaborating with other systems that occupy the same spectrum bands. Therefore, the collaborative paradigm between SUs in the distributed-based CR networks is underlined as a key area to be addressed. Typically, the resources allocation problems are nonconcave, hence difficult and computationally complex to solve. It poses the requirement of efficient algorithms, which provide a good trade-off between the achieved performance and the computational complexity while maintaining the distributed implementation.

In conclusion, we summarize the self-coexistence issues and the corresponding challenges in the CR networks in Figure 1.4.

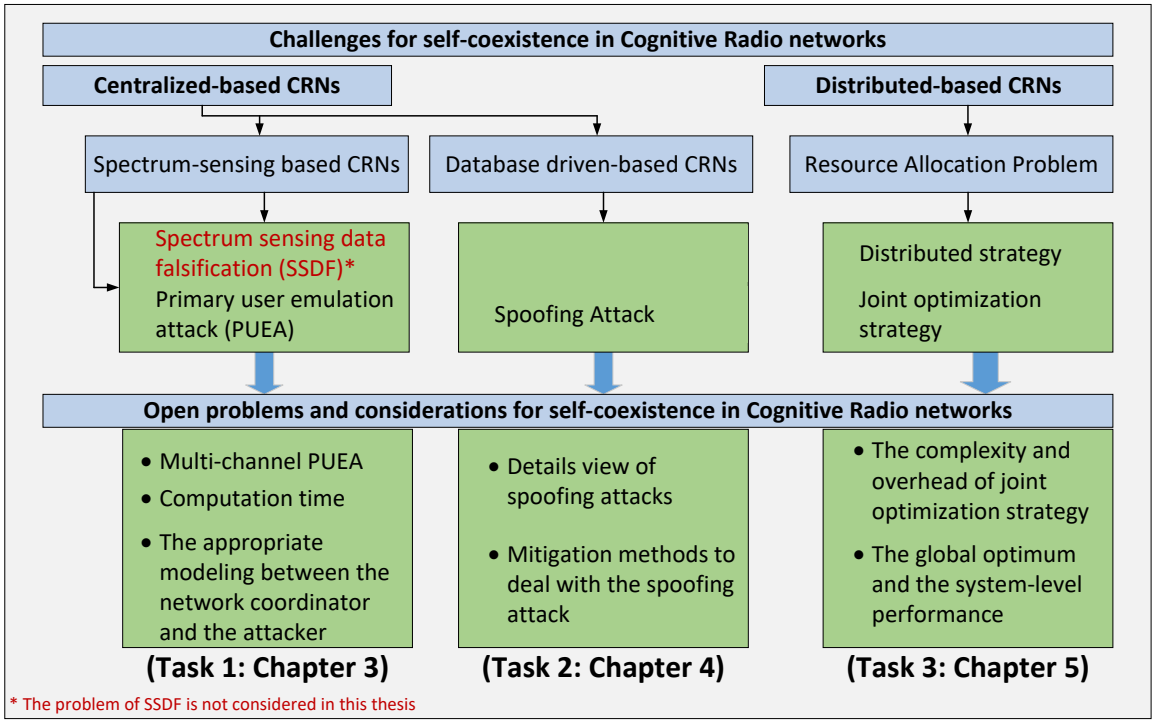


FIGURE 1.4 Self-coexistence issues and open research problems in CR networks.

1.3 Thesis Contributions and Organization

Self-coexistence mechanism between cognitive users is a key problem that needs to be addressed in order to successfully deploy the cognitive radio systems. The objective of this thesis is to provide a systematic study of coexistence mechanisms for the CR networks in both centralized and distributed architecture, which directly address these unaddressed technical challenges (i.e., Task 1, 2 and 3 in Figure 1.4). In particular, for the centralized architecture networks, the important problem of assessing and mitigating the multi-channel PUEA in the sensing-based CR network and the spoofing attack in the database driven-based CR network is investigated and solved. The main challenges faced in the thesis include the classifying and the modeling of such attacks and the designing of the corresponding mitigation methods that can mitigate the influence of these attacks (i.e., Task 1 and 2). For the distributed architecture network, this work characterizes how the cognitive users can collaborate with others and design the corresponding self-coexistence mechanism between SUs in a collaborative manner (i.e., Task 3). Since there are conflicting objectives and trade-off interactions between misbehaving users and the network coordinator in the centralized-based CR networks as well as between cognitive users in the distributed-based CR networks, the work on game theory can be readily adopted to investigate these interactions. For these reasons, the research in this thesis focuses on the coexistence mechanisms among SUs in

network architectures and adopts the game-theoretic framework to analyze the corresponding coexistence strategies.

The contributions of the thesis are as follows.

— **Task 1:** in the spectrum sensing-based CR networks, to ensure the coexistence between SUs, this work examines how to mitigate the influence of the multi-channel PUEAs by implementing the surveillance process after sensing duration. The surveillance process can observe prohibited secondary-accessing channels to detect illegal channel occupation or retrieve the opportunity of using the presumptuously occupied state channels. The formulation of the devised games between the attacker and the network coordinator, as well as the computation of the Nash Equilibrium (NE), are subsequently studied. In addition, motivated by the computation time challenge in the game-theoretic approach, this research attempts to expose the appropriate modeling of the strategic interaction between the network coordinator and the attacker and provides means for taking into account leadership and commitment in the game model. Via numerical simulations, we show that significant performance improvements in terms of the network coordinator's expected payoff and the computational time can be achieved by adopting the commitment model.

— **Task 2:** in the database driven-based CR networks, to ensure the coexistence between SUs, this research first provides a general view of spoofing attacks by classifying the request messages consisting of spoofing information into five types according to spoofed contents and behaviors of the attacker. In order to counteract these spoofing attacks, we consider two surveillance processes corresponding to the spoofed contents (*i.e.*, the location or the identification) and formulate the corresponding surveillance games on request location verification and data traffic identification. The verification strategy of the network coordinator is obtained through the corresponding NE strategies of the game. The results show that the network coordinator can enforce the attacker to reduce the number of spoofing attacks by performing surveillance processes according to NE at an appropriate penalty.

— **Task 3:** in the distributed-based CR networks, this research proposed a collaborative resource allocation framework to ensure the coexistence among cognitive users. In such framework, each user allocates the radio resources such as the transmission power or the frequency bands by optimizing a collaborative function that comprises not only its own performance but also the others' performance. The proposed framework possesses the advantages of distributed implementation such as the low-complexity and fast-converging algorithms and overcomes the disadvantages of the conventional studies such as the increased complexity and overhead, of the conventional studies. Specifically, we will formulate a new game that will narrow the performance gap compared to the joint optimization problem, while maintaining the distributed implementation. Since the maximization problem of the collaborative function is shown to be nonconcave,

obtaining a global solution is highly complex. To address this problem, we provide the low-complexity algorithms for efficiently solving these issues by approximating the utility function of the game for each region of the SINR of the network: the high-SINR region (i.e., the users are far apart), and ii) the network in the low-SINR region (otherwise). Via numerical simulations, we show that the proposed paradigm provides better fairness between cognitive users while achieving higher performance and lower convergence time.

The remainder of the thesis is organized as follows.

Chapter 2 presents some relevant background on self-coexistence mechanisms for SUs in CR networks, including the mitigation techniques to deal with the PUEA and spoofing attack in the centralized-based CR networks, and the resource allocation strategies in the distributed CR networks, that are useful for the development of various mitigation/allocation techniques in subsequent chapters.

Chapter 3 considers the coexistence mechanism between SUs in the spectrum sensing-based CR networks by deploying a surveillance process to deal with the multi-channel PUEAs. Such a process, which is implemented by the network coordinator after sensing duration, can observe prohibited secondary-accessing channels to detect illegal channel occupation and retrieve the opportunity of using the presumptuously occupied state channels. The formulation of the games between the attacker and the network coordinator, as well as the computation of the Nash Equilibrium (NE), are subsequently studied. Motivated by the computation time challenge in the game-theoretic approach, this research attempts to expose the appropriate modeling of the strategic interaction between the network coordinator and the attacker by providing means for taking into account leadership and commitment in the game model. In such model, the network coordinator exploits the leader position by committing to its surveillance plan and forcing the attacker to follow this strategy. Numerical simulations show that significant performance improvements in terms of the network coordinator's expected payoff and the computational time can be achieved by adopting the commitment model.

Chapter 4 is concerned with the coexistence mechanism between SUs in the database driven-based CR networks through the mitigation methods to deal with the spoofing attacks. We first classify the spoofing attacks according to the contents of spoofing requests and remark that the spoofing attack only locates at the location and the identification information. Due to these characteristics, our focus then is on the development of the corresponding countermeasures. Specifically, we propose a surveillance process, which includes two complementing steps: the request location verification and the spectrum user's identification to deal with the location and ID spoofing attacks, respectively. Two surveillance games on request location verification and data traffic identification are formulated by adopting a game theoretical framework. Simulation results show the significant reduction of spoofing attacks by performing surveillance processes.

Chapter 5 studies the collaborative paradigm and present the advantage that this paradigm shift can provide for designing a coexistence mechanism among SUs in the distributed-based CR networks through the example of collaborative power allocation problem. In a collaborative manner, each user optimizes its strategy through a modified objective, referred as the collaborative function. Since the maximization problem of the collaborative function is shown to be nonconcave, obtaining a global solution is highly complex. To address this problem, we provide the low-complexity algorithms for efficiently solving these issues by approximating the utility function of the game for each region of the SINR of the network (i.e., the high-SINR region and the low-SINR region) to obtain a well-known game, such as the potential game or the concave game, and analyze the power allocation through the NE of such game. The study of the existence and uniqueness of the NE in these games is then presented. The simulation results confirm the improvement in terms of performance, convergence time, as well as fairness of the system.

Chapter 6 presents the concluding remarks and gives suggestions for further studies.

1.4 Publications and Awards

— **Journals**

1. **Duc-Tuyen Ta**, N. Nguyen-Thanh, P. Maillé, and V. T. Nguyen, "Strategic Surveillance Against Primary User Emulation Attacks in Cognitive Radio Networks," IEEE Transaction on Cognitive Communications and Networking - *accepted for publication.*
2. Nhan Nguyen-Thanh, **Duc-Tuyen Ta**, and Van-Tam Nguyen, "Spoofing Attack and Surveillance Game in Geo-location Database Driven Spectrum Sharing," IET Communications - *major revision.*
3. **Duc-Tuyen Ta**, Duy H.N. Nguyen, N. Nguyen-Thanh, and V. T. Nguyen, "Collaborative Paradigm for Next Generation Wireless Networks," EURASIP Journal on Wireless Communications and Networking - *major revision.*

— **International Conferences**

1. N. Nguyen-Thanh, H. Le-Duc, **Duc-Tuyen Ta** and V. T. Nguyen, "Energy efficient techniques using FFT for deep convolutional neural networks," *International Conference on Advanced Technologies for Communications (ATC)*, Hanoi, 2016, pp. 231-236.
2. **Duc-Tuyen Ta**, N. Nguyen-Thanh, P. Maillé, P. Ciblat and V. T. Nguyen, "Mitigating Primary Emulation Attacks in Multi-Channel Cognitive Radio Networks: A Surveillance Game," *IEEE Global Telecommunications Conference (GLOBECOM)*, Washington, DC, 2016.

3. **Duc-Tuyen TA**, N. Nguyen-Thanh, P. Ciblat and V. T. Nguyen, "Extra-sensing game for malicious primary user emulator attack in cognitive radio network," *European Conference on Networks and Communications (EuCNC)*, Paris, 2015, pp. 306-310.

— **Award**

1. Travel award in the 2015 European Conference on Networks and Communications (EuCNC).

Chapter 2

Background on Self-Coexistence in Cognitive Radio

This chapter presents some of the current state-of-the-art self-coexistence solutions among SUs in CR networks. The first part of this chapter discusses self-coexistence mechanisms in centralized-based CR networks through the mitigation techniques to deal with threats caused by misbehaving users: the PUEAs and the spoofing attacks. The second part of this chapter then presents some recent resource allocation schemes for the coexistence of SUs in the distributed-based CR networks.

2.1 Coexistence in the Centralized Infrastructure Networks

To provide the secondary users access opportunities in CR networks without interference to primary systems, the spectrum holes exploration is a key function in CR systems [55]. Generally, there are two main approaches to determine the spectrum opportunities in CR networks: i.) spectrum sensing-based [24], and ii.) database driven-based [25, 26]. In the former approach, primary system's activity is explored by measuring the radio environment spectrum. In the latter approach, a coordinator, which is essentially a database server with an online geo-location map of spectrum usage, is responsible for managing the coexistence between PUs and SUs. The database driven-based approach is more accurate and reliable, but expensive and requires perfect knowledge of the primary system, and fast dissemination of spectrum updates. On the other hand, the spectrum sensing-based approach provide a less accurate but cheaper and more flexible method for discovering spectrum holes for a wide range of network types. For both approaches, to ensure the coexistence among SUs, the CR networks face with the challenges of distinguishing primary signal or honest user request from misbehaving user signal/request [15]. Specifically, the spectrum sensing-based CR networks suffer from the primary user emulation attack [16] while the database driven-based CR networks suffer from the spoofing attack [17].

2.1.1 Primary User Emulation Attack in Sensing-based CR networks

This section provides a brief review of PUEA and the corresponding mitigation techniques in CR system. The advantages and disadvantages of each mitigation technique will be sequentially presented.

The primary user emulation attack, originally investigated in [19–21, 27], is an attacking approach to the spectrum sensing process, where a misbehaving user emits the emulated primary signal (*i.e.*, by mimics of the primary signal characteristics) during the sensing period. The presence of the emulated primary signal will lead to a presumptuously occupied state on the attacked channels (*i.e.*, the spectrum sensing engine perceives the channels as being occupied). Consequently, the PUEA limits the spectrum access of the CR networks and thus severely degrades their operation. Generally, there are two types of misbehavior associated with the PUEA: malicious and selfish. In the former type of attack, the attacker (*i.e.*, the misbehaving user) targets at obstructing other secondary users from identifying and using vacant spectrum bands, similar to the conventional Denial-of-Service or jamming attack. In the latter type of attack, the attacker targets at illegitimately occupying channel resource and preventing other secondary users from accessing the channel. In that sense, the selfish PUEA is associated with an illegal benefit while creating an unfair obstruction to the CR networks and possible unnecessary interferences to the nearby primary users. Recently, several techniques have been presented to mitigate the PUEAs. Examples of the main techniques to mitigate the PUEA in the spectrum sensing-based CR networks are as follows.

First is the transmitter verification scheme to authenticate the primary user signal from the emulated signals. In [21, 45], the authors proposed the localization-based transmitter verification approach to detect the PUEA. Specifically, the cognitive radio system uses the received signal strength (RSS) measurements to estimate the location of the source of a signal and then determines whether the signal is from an incumbent or an attacker through the known location of the primary user. However, this approach requires the precise location of the primary users, which is inapplicable in the mobile primary transmitter case. Furthermore, the localization-based verification approach can be disrupted since the received power of the primary signal at CR users can be completely emulated by a revived transmission (*i.e.*, send different signal strengths in different directions simultaneously) with an array antenna [46]. Also, it requires multi-node collaboration, which is expensive in terms of bandwidth and energy. In [47], the authors proposed the primary signal feature verification scheme, which utilized the characteristics of the primary signal to distinguish a primary signal from an emulated one. However, recent achievements in hardware processing enable CR devices to generate an emulated primary signal perfectly, without too much effort. A physical layer authentication scheme by embedding the authentication tag at the primary signal to identify and mitigate PUE attack is studied in [48]. In this work, the CR system is capable of

authenticating the PU's transmission, hence can mitigate the PUE attack. However, it requires changes in the hardware and the transmission protocol of the primary users, which is not desirable in practice. Moreover, this approach might not seem very efficient if the attacker emits a copy of the incumbent signal. Another approach to determine PUEA is the clustering-based verification, which is proposed for the cooperative spectrum sensing-based CR networks [56]. Specifically, the network coordinator gives different weight to each spectrum sensing report of individual cognitive users according to their relative locations and some trust factor. The final decision is made to maximize the legitimate primary signal detection probability. Such an approach is also investigated in [49], where each cognitive user updates its belief about the state of the channel (*i.e.*, attacked or not) with neighboring users. A final belief then convergences after a sufficient number of observations. However, the clustering approach is costly due to the required number of observations as well as the overhead for exchanging reports.

Second is the game theory-based scheme for overcoming the PUEA in CR networks. While the PUEA attacker targets at preventing other users from accessing, the network coordinator or the other cognitive user targets at identifying and mitigating the PUEA. Due to the conflicting objectives and the trade-off between cost and benefit of both attacker and network coordinator/user, game theory, a mathematical framework of conflict and cooperation between independent, rational decision-makers [50], has been utilized to formulate the problem. In [51], authors proposed an anti-jamming approach to defend CR networks against PUEA by treating the emulated primary signal as a jamming signal and adopting the channel hopping as the defensive scheme. A similar approach, with the zero-sum scholastics game, is adopted to formulate the jamming/anti-jamming model between CR network and the jammer in [52]. Also, a Stackelberg-based game theoretic approach is proposed in [57]. However, there is still vulnerability if the attacker conducts multi-channel attacks. Moreover, the misbehavior of the attacker, *i.e.*, selfish or malicious, is not considered. A surveillance-based approach is then proposed to determine a good strategy to deal with each type of PUEA [53, 54]. For the malicious misbehavior PUEA, the goal is to fool the CR system by emitting the emulate primary signal during the sensing period. Hence, it is possible to add an extra-sensing process in the data period if the channel was declared occupied in order to retrieve the opportunity of using the attacked channel in the remainder of the frame. For the selfish misbehavior PUEA, the goal is to illegally occupy the channel and prevent others from accessing it. Hence, a successful PUE attack in sensing duration is usually followed by a selfish use of the attacked channel by the attacker. Meanwhile, it is possible to determine user's identification in any communication link by implementing a channel surveillance process, which observes prohibited secondary-accessing channels after sensing duration, to detect illegal channel occupation and identify the selfish PUEA attacker. A non-zero sum game between the network coordinator, who provides the surveillance-based defense service, and the PUEA attacker is formulated. The surveillance strategies, as well as the attack strategies, are

determined through the close-form Nash equilibrium (NE). The results figured out the strong influence of the players' gain-to-cost ratio and gain-to-penalty ratio to the players' strategies. However, the multi-channel attacks are also not considered.

Since the CR networks usually work on multiple frequency bands, and because of the rapid expansion of software-defined radio, the multi-channel PUEAs, as well as the corresponding mitigation method, must be considered.

2.1.2 Spoofing Attack in Database Driven-based CR networks

This section reviews the spoofing attack in database driven-based CR networks. As mentioned above, the spectrum sensing-based approach explores the primary user's activity by measuring the radio environment spectrum. However, the rapid change and complexity of radio propagation environment due to shadowing and fading bring in too many uncertainties, leading to low sensing accuracy. The demand-and-request approach through a coordinator, which contained an online geo-location map of spectrum usage, like database driven-base will provide a more accurate and reliable scheme[25]. Therefore, in 2012, FCC enforced the adoption of the database driven-based approach for exploiting CR in the TV White Space (TVWS) and the 3.5 GHz band [26].

In the database driven-based CR networks, the FCC rules require cognitive users to learn spectrum availability at their corresponding locations from a central database of incumbents. In general, the database stores an up-to-date repository of incumbents (*i.e.*, the television stations, wireless microphones, etc.) and use this information to determine the available spectrum bands at a cognitive user's location. In particular, whenever a user has a demand to use channels, it should send a request to a coordinator, which contains the database server, to acquire channel resource. Based on the location information and the database system, the coordinator will assign the available channels, the corresponding transmission parameters of the available spectrum bands and the detailed configuration to the user. Of course, the coordinator will charge a service fee.

For example, let's consider two famous database driven-based CR standards: IEEE 802.11af [9], IEEE 802.19 [58]. The IEEE 802.11af is a wireless local area network (WLAN) standard, which operates in the TVWS. In 802.11af, the location of each network user must be known to ensure a good channel assignment and limit interference to the primary system. Generally, the access points and stations determine their position using a satellite positioning system (*e.g.*, Global Positioning System - GPS) and use the Internet to query a coordinator to discover the available frequency bands at a given time and location. In contrast, the IEEE 802.19 address the issues of coexistence between unlicensed wireless networks since those may operate in same frequency bands in the same location. In IEEE 802.19, the coordinator is CDIS (coexistence discovery and information server), and a network object, (*i.e.*, a device or a group of devices, which must include either a fixed or a portable device that has internal

geo-location capabilities and can access a database of channels in use to load availability information for its current location). This loading service can be performed through a direct wireless connection to the server or through a backhaul connection. In mobility use case, the location and mobility information should be updated at least every 60 seconds.

One key point for implementing database-driven CR system is the availability as well as the accuracy of the devices' location. Considerable interference on both incumbent and cognitive radio systems as well as interference between cognitive radio systems will appear if the users' location information is inaccurate. Moreover, unfair spectrum allocation will happen if adversaries intentionally spoof request messages with faked location information. Therefore, spoofing attack is a critical vulnerability of the GDB driven-based DSA system. However, to the best of our knowledge, there is no work systematically examining the impacts of spoofing attacks in database driven-based CR networks. The most relevant related work which considers the GPS spoofing attacks in a database driven-based CR networks is presented in [17], but limited due to the impact of false localization from the attacked GPS signals. The study points out that a simple GPS spoofing attack (*i.e.*, random attack) can cause a significant interference to the incumbent system even in an extremely sparse network. The remain works on database driven-based CR networks mainly focus on location privacy issues [18, 28, 29] or the incumbent system privacy issues [30] by proposing an encryption technique to protect sensitive incumbents' operational privacy without affecting database's accessibility and spectrum utilization efficiency.

Another important point for implementing database driven-based CR networks is demand-and-request protocol. In particular, when a user wants to register for operation, to update new location, or to query for spectrum bands, it must send a request to a resource manager. The request messages usually contain the physical/network ID and the location of the user. However, due to the flexibility of the software-defined radio, ID or location information could be spoofed. For example, the attacker can use the GPS spoofing attack by broadcasting incorrect GPS signals or by rebroadcasting genuine signals captured elsewhere or at a different time to fake the estimated location of other users [17]. In addition, some communication protocols do not provide mechanisms for authenticating the source or destination of a message, such as the protocols in the TCP/IP suite or the Voice over IP (VoIP), which allows users/callers to forge ID information and present false names and numbers [59, 60]. The attacker hence it can spoof the ID (*i.e.*, uses a fake ID or uses the ID of other users) to attack the network.

Finally, due to the aim of attack, the spoofing attack can be categorized into the accidental, malicious and selfish attack. An *accidental spoofing request* occurs when the sender is not aware of the incorrectness of its location information due to either a malfunctioning or an attack (similar to [17]). A *malicious spoofing request* comes when the sender intentionally provides false location information for causing more interference to the whole system. In contrast, a *selfish spoofing request* appears when the sender abusively queries for more

spectrum resources under faked ID. The corresponding mitigation method for each kind of attack needs to be investigated.

In summary, a general view of spoofing attack in database driven-based CR networks, which occur in both the ID and the location information of request messages, as well as the corresponding surveillance method, must be considered.

2.2 Coexistence in the Distributed Infrastructure Networks

This section examines some recent advances in resource allocation for CR networks coexistence. The resource allocation at the CR networks aims at efficiently exploiting the available spectrum hole for the newly-deployed CR nodes. While interference suppression in the primary network is the most important implementation aspects, the resource allocation among CR nodes, such as the power allocation problem, is also key to optimize the CR network performance. In this section, the main concern is the study of a power allocation algorithm for maintaining the coexistence between SUs in the distributed-based CR networks coexistence. Note that the study is not limited to the power allocation problem. Other resource allocation aspects, such as channel selection, user scheduling, and beamforming/precoding design, are also investigated. With CR user's power constraints, this section reviews resource allocation under the following two criteria: (i) minimizing the transmit power at the CR nodes and (ii) maximizing the sum-rate at the CR nodes. In this domain, recent work mainly focuses on two approaches: non-cooperative game [31–37] and joint optimization [38–43]. Some of the concepts of game theory applicable to resource allocation are presented in Appendix A.

2.2.1 Game Theoretical Approach

In this section, we investigate different power control schemes from a game-theoretical point of view, where each CR user acts as a rational player. The major advantage of the game theoretical approach is the fully distributed implementation of the power control with little or no coordination among CR nodes. In a game, each user selfishly optimizes its own performance regardless of the actions of other users. Denote the utility function of user i as $U_i(p_i, \mathbf{p}_{-i})$ where $\mathbf{p}_{-i}$ is the power vector of all users except user i, the power control game can be formally expressed as

$$\max_{p_i \in \mathcal{S}_i} U_i(p_i, \mathbf{p}_{-i}) \tag{2.1}$$

Herein, $\mathcal{S}_i$ is the set of admissible strategies for user i, which can include one or more of the following constraints:

— $0 \leq p_i \leq p_i^{max}$: p_i^{max} is the maximum transmit power by user i.

— $I_i \leq I_i^{max}$: where I_i and I_i^{max} are the interference and maximum allowable interference induced to the primary network. I_i can be defined as $I_i \triangleq g_i^{PU} p_i$ where g_i^{PU} is the channel gain from user i to the primary network.

— $\gamma_i \geq \gamma_i^{min}$: where γ_i and γ_i^{max} are the SINR and the target SINR for user i. The SINR γ_i at user i can be defined as

$$\gamma_i = \frac{g_{i,i}p_i}{\sum_{j \neq i} g_{j,i}p_j + \sigma^2} \tag{2.2}$$

where $g_{j,i}$ denotes the channel gain from user j's transmitter to user i's receiver, $g_{j,i}$ denotes the channel gain from user i's transmitter to it's receiver and σ^2 denotes the background Gaussian noise.

Depending on the type of utility function $U_i(\cdot)$, solutions to the individual problem in (2.1) can be found and different games formulated with various convergence characteristics. In most instances and under certain conditions, the underlying games settle at the Nash equilibrium $\mathbf{p}^* = [p_i^*]$, a stable and predictable state [61] at which no user has incentive to unilaterally change its power level, *i.e.*,

$$U_i(p_i^*, \mathbf{p}_{-i}^*) \geq U_i(p_i, \mathbf{p}_{-i}^*), \forall p_i \in \mathcal{S}_i \tag{2.3}$$

for every user i. In general, the utility function contains two main components

$$U_i(p_i, \mathbf{p}_{-i}) = P_i(p_i, \mathbf{p}_{-i}) - C_i(p_i) \tag{2.4}$$

where $P_i(\cdot)$ is the payoff for user i and $C_i(p_i)$ is the nonnegative cost for playing the game.

Payoff

The following list includes some common payoff functions and corresponding sets of admissible strategies as follows.

— *Power minimization with hard QoS requirement:*

$$P_i(p_i, \mathbf{p}_{-i}) = -p_i \quad \text{and} \quad \mathcal{S}_i = \{p_i | 0 \leq p_i \leq p_i^{max}, I_i \leq I_i^{max}, \gamma_i \geq \gamma_i^{min}\} \tag{2.5}$$

— *Power minimization with soft QoS requirement:*

$$P_i(p_i, \mathbf{p}_{-i}) = -(\gamma_i - \gamma_i^{min})^2 \quad \text{and} \quad \mathcal{S}_i = \{p_i | 0 \leq p_i \leq p_i^{max}, I_i \leq I_i^{max}\} \tag{2.6}$$

— *Rate maximization with power constraint:*

$$P_i(p_i, \mathbf{p}_{-i}) = -\log(1 + \gamma_i) \quad \text{and} \quad \mathcal{S}_i = \{p_i | 0 \leq p_i \leq p_i^{max}, I_i \leq I_i^{max}\} \tag{2.7}$$

— *Energy efficiency:*

$$P_i(p_i, \mathbf{p}_{-i}) = f(\gamma_i)/p_i \tag{2.8}$$

where $f : R^+ \rightarrow [0, 1]$ is a sigmoidal efficiency function (*e.g.*, the packet success rate) and $\mathcal{S}_i = \{p_i | 0 \leq p_i \leq p_i^{max}, I_i \leq I_i^{max}\}$.

Cost

The involvement of player i in a power control game may impose a certain cost to achieve its own payoff. Some common cost function can be introduced into the utility function $U_i(p_i, \mathbf{p}_{-i})$ are listed as follows.

— *Power cost*: $C_i(p_i) = \alpha_i p_i$ where each may attempt to back off its power instead of transmit at its maximum. This pricing strategy may enable each user to adopt more socially optimal power control and substantially enhance the NE efficiency if reasonable deviations from the target SINR are allowed.

— *Interference temperature cost*: $C_i(p_i) = \alpha_i I_i$ where each user attempts to minimize the interference induced to primary network.

Solutions

One of the most popular solutions for the power allocation problem is Foschini-Miljanic's algorithm [32], a power control scheme that enables users to eventually achieve their fixed target SINRs. In this algorithm, the allocation among the users can be considered as a strategic non-cooperative game where each user selfishly transmits at its minimum transmit power to achieve the target SINR. Interestingly, as long as the target SINRs are feasible, the outcome of the NE is a Pareto-optimal solution at a minimal aggregate transmit power [32].

When each user aims to maximize its own data rate, the potential game framework can be applied to study the adaptive power control among the users [33]. The supermodular game framework has been investigated in [36, 62] with the objective of maximizing the packet transmission success rate at each user. In such games, pricing strategies [62] are added to encourage the users to adopt more socially optimal power control. As a result, the efficiency of the NE is substantially enhanced if reasonable deviations from the target SINR are allowed.

When only users at their required QoS are scheduled, i.e, (2.6), the admission control is considered. Joint admission and power control have been studied in [63–67] for single-input-single-output (SISO) systems. In another work [68], admission control for ad-hoc cognitive networks has been examined with consideration of QoS protection to a PU.

Another important consideration regarding the resource allocation in CR networks is the energy efficiency, *i.e.*, (2.8). In [37, 42, 43], the authors formulate the problem of energy efficiency which maximizes the energy efficiency of the CR network while ensuring the minimum rate requirement for the PU. A maximum power constraint and a minimum SINR constraint are enforced for the CR systems. Generally, the resource allocation problem is a non-concave problem with non-linear constraints. The solution is then achieved by adopting

the fractional programming and game theoretic approach. The extension for the resource allocation in multiple-input-multiple-output (MIMO) CR systems is considered in [69].

In the distributed approach, each user only needs the local information to make the independent and rational decision. The feature makes it possible to use *low-complexity distributed algorithms* to determine the power allocation. However, the global optimum may be less likely to be achieved and the system-level performance may be degraded.

2.2.2 Joint Optimization Approach

Taking an optimization approach to solve the source allocation problem in a CR network, all CR users aim to maximize a common utility function $U(\mathbf{p}) = \sum_{i=1}^{K} w_i U_i(p_i, \mathbf{p}_{-i})$, where $w_i \geq 0$ is the weight for user i. In particular, the common utility function can be the weighted sum-rate [38–41] or the total energy efficiency [37, 42, 43]. Mathematical frameworks, such as geometric programming [38–41] or the factional programing [37, 42, 43], are employed to establish the optimal power allocation. The achievable utility, usually Pareto-optimal, then serves as the benchmark for the efficiency of the Nash equilibrium in the game with the corresponding utility function $U_i(p_i, \mathbf{p}_{-i})$'s.

Besides the weighted sum-rate utility, some common utility function related to the fairness between cognitive users in the joint optimization are listed as following [70].

— *Weighted minimum-rate utility*: $U_1(p) = \min_i w_i \log_2(1 + \gamma_i)$.
— *Weighted proportional fairness utility*: $U_2(p) = \sum_i w_i \ln(\log_2(1 + \gamma_i))$.
— *Weighted harmonic-mean-rate utility*: $U_3(p) = (\sum_i 1/w_i \log_2(1 + \gamma_i))^{-1}$.

Different common objective functions correspond to different allocation strategies, as well as capturing the different trade-offs between system efficiency and user fairness. A feasible power allocation reaches max-min fairness if for each user i, it cannot increase p_i without decreasing the power p_j of user $j \neq i$, where $p_j \leq p_i$. The works in [71] shows that, by using the max-min fairness as the objective function, it greatly improves the fairness without considerably degrading the system utility. In contrast, a feasible power allocation reaches proportionally fairness if for each user i, it's power cannot increase by $y\%$ without reducing the total percentage of other users' power by more than $y\%$ to ensure the feasible allocation. The proportional fairness offers a better trade-off between the max-min and the maximum sum-rate allocation. The last one, harmonic-mean-rate approach, is equivalent to maximizing the average of the system's sum-rate. In summary, in term of utility, the order is $U_1(p) \leq U_2(p) \leq U_3(p)$ while in term of fairness, the order is reversed [72].

The joint optimization approach allows all the users to *coordinately optimize* their strategies and enables a dynamic allocation of the interference budget among users. However, this approach needs to cope with the *increased complexity* and *overhead* due to the demand for the channel information of all users necessary for implementing the joint optimization algorithm. Moreover, even when the global information is known, the optimization results

show that users with poor channel conditions are allocated with much less power in order to optimize the performance of the whole network. Consequently, it degrades the fairness between users in the network.

2.3 Concluding Remarks

In summary, this section has discussed various studies on self-coexistence mechanisms in the centralized and distributed CR networks. The key aspect of those studies is the consideration of the coexistence among SUs and the coexistence between the network coordinator and the misbehaving users, which share the same frequency resources. When the network is centralized, the mitigation method to mitigate the influence of PUEA or the spoofing attack caused by the misbehaving users is considered. When the network is distributed, the resource allocation to ensure the data transmission of cognitive users is considered.

First, it is worth to mention that most of the related work in the literature study the sensing-based CR networks with single channel PUEA. In addition, due to the resource limitation, the extension of the simple model with a single channel and a limited set of strategies by considering separately each channel, could not be extended to describe the behavior of the multiple channel attack. These observations motivate us to study the multi-channel PUEA as well as the corresponding mitigation approach in CR networks. In addition, most of the studies discussed above analyze the player's strategies through the Nash equilibrium, which may not be an efficient strategy in practice. The observation motivates us to adopt the Stackelberg model, which is close to the real-life security problems [73, 74], to formulate and analyze the strategic interaction between the network coordinator and the misbehaving user.

Second, the spoofing attack in database driven-based CR network is not well investigated. Only the work in [17] considers the location spoofing attacks, but limited to the impact of false localization from the attacked GPS signals. It motivates us to study the classification of spoofing attacks, their impact on the CR system as well as the corresponding approach to deal with such kind of attacks.

Finally, efficient radio resource management at CR network deployment is imperative in mitigating the interference to the primary network and maximizing the CR network performance. However, the related work in literature study is not very effective because of the lack of a global solution for game theoretical approach, and the increased complexity, in addition to overhead cost for the joint optimization approach. These reasons motivate us to propose a novel collaborative power allocation paradigm that will narrow the performance gap compared to the joint optimization while maintaining the distributed implementation with low-complexity and fast-converging algorithms.

Chapter 3

Self-Coexistence in Spectrum Sensing-based Networks: Surveillance Strategy for PUEAs

3.1 Introduction

Recently, the study of primary user emulation attack and the corresponding mitigation techniques in the spectrum sensing-based CR networks have attracted considerable research attention. As mentioned in Chapter 2, in general, these mitigation techniques can be classified into: i.) the transmitter verification approach which verifies the primary user signal from the emulated signals [21, 45, 46, 48] and ii.) the game theory-based approach which formulates the relationship between the attack and the mitigation process as a strategic non-cooperative game. Unfortunately, the first approach is only applicable in cases where information such as the precise location of the primary users, the propagation channel characteristics, the added authentication tag is available, or a large number of observations and the overhead for exchanging reports are available. Due to the conflicting objectives and the trade-off between the cost and benefit of both attack and mitigation process, the second approach utilizes the game theory to formulate the relationship between the attacker and the network coordinator/user. An anti-jamming game to defend CR networks against PUEA by treating the emulated primary signal as a jamming signal and using the channel hopping as the defensive scheme is proposed in [51]. A similar approach, with the zero-sum stochastic game, is performed to formulate the anti-jamming model between the CR network and the jammer in [52]. Also, a Stackelberg-based game is introduced in [57]. However, there is still

The materials presented in Chapter 3 have been presented at the 2015 European Conference on Networks and Communications (EuCNC) in Paris, France [75], the 2016 IEEE Global Communications Conference in Washington, DC, USA [76], and submitted in the IEEE Transaction on Cognitive Communications and Networking [77].

vulnerability if the attacker conducts multi-channel attacks. Moreover, the misbehavior (*i.e.*, selfish or malicious) of the attacker is not considered.

In the spectrum sensing-based CRNs, depending on the type of attack, we can determine a good strategy to deal with the latter. In the malicious PUEA, the attacker aims at obstructing the operation of the CR networks by emitting the emulated primary signal at the sensing period. Thus, it is possible to sense the 'occupied'-declared channels by adding an extra-sensing process in the next data period in order to retrieve the opportunity of using the attacked channels in the remainder of the frame [54, 75]. In contrast, a successful selfish PUEA in sensing period is usually followed by a selfish use of the attacked channel by the attacker. Hence, it is possible to determine user's identification in any communication link by implementing a channel surveillance process, which observes prohibited secondary-accessing channels after sensing period, to detect illegal channel occupation and identify the selfish PUEA attacker [54]. A noncooperative game between the network coordinator, who provides the surveillance-based defense service (*i.e.*, the extra-sensing and the surveillance process), and the PUEA attacker is formulated. The surveillance strategies, as well as the attack strategies, are determined through the close-form NE of the game. It is to be noted that these work only considered the single-channel attack where the attacker and the network coordinator can attack or monitor at most one channel.

Usually, the CR networks work on multiple frequency bands while the attacker can launch a multi-channel selfish PUEA due to the rapid expansion of software-defined radio. For such a case, since the channel occupancy could be considered to be independent on each channel, the simple model with a single channel and a limited set of strategies, as investigated in [54, 75], could be extended to the multi-channel attack with unlimited resources for both attacker and network coordinator by considering separately each channel. However, due to the limited resources, the extension of the game for multi-channel case by considering separately each channel cannot describe the behavior of the attack and the surveillance process. In addition, if the network coordinator considers each channel separately, it will need to take into account a sequential monitoring plan, which comes at the cost of long surveillance time. It means that the model of the multi-channel surveillance process to mitigate the influence of the PUEA in CR networks is more realistic than the single-channel surveillance process or the sequential monitoring model. Therefore, it is necessary to investigate the multi-channel attack and the corresponding mitigation techniques.

Inspired by the mentioned work, this chapter considers a game theoretical approach to study the mitigation process to deal with the influence of PUEA in the CR networks. Specifically, our focus is on investigating the multi-channel PUEA and the corresponding surveillance process. Using the game-theory framework, we formulate the relationship between the attacker and the network coordinator as a strategic game and establish the best strategy for the network coordinator and the attacker through the NE of the game. Since the network coordinator observes the attacker's action only indirectly, *i.e.*, through

the sensing results, the formulated game is an incomplete and imperfect information game. Finding a NE solution in such a game is more complicated due to the large strategy set [78]. We, therefore, employ the sequence-form representation approach [79, 80], instead of the conventional (benchmark) strategic-form representation approach [81, 82], to formulate and then determine the NE strategy for the game. Analysis and simulation results confirm that the sequence-form representation approach is much more efficient than the strategic-form representation approach in order to determine the NE of the game.

It is worth mentioning that all the mentioned studies have considered the case that the network coordinator and the PUEA attacker perform the attack and the surveillance process simultaneously without or with partial information regarding the other's strategy. However, an intelligent and rational attacker can learn to adapt to the surveillance strategy of the network coordinator by conducting a fixed period of monitoring before performing a selfish or a malicious PUEA [83]. In such a case, the NE of the game may not be an effective strategy for the network coordinator and the attacker. Instead of simply playing a NE strategy, the network coordinator can leverage its position of leader by committing to a defense strategy and forcing the attacker as the follower to plays its best response regarding the observed surveillance strategy. The leadership and commitment are remarkably close to real-life security problems, such as patrolling scenarios, for which these types of commitments are necessary by the security agencies [73, 74]. For example, security personnel patrolling an infrastructure decides on a patrolling strategy first, before their adversaries act taking this committed strategy into account. Motivated by the appropriate modeling of the strategic interaction between the network coordinator and the attacker, in the latter part of this chapter, we take into account the leadership and commitment in the game model by using the Stackelberg games [84]. The corresponding attack and surveillance strategies of the attacker and the network coordinator are analyzed through the Strong Stackelberg Equilibrium (SSE) [85] of the game. We then analyze and interpret the impact of the system parameters, such as the presence probability of the PU's signal, the loss and the benefit of each player, on the obtained NE strategies. A comparison to the conventional surveillance game in which the network coordinator does not commit to its surveillance strategy is then presented in this work.

3.2 System Model

We consider a half-duplex, sensing-based CR network which allows secondary access to multiple licensed bands, as illustrated in Figure 3.1. In order to simplify the analysis and focus on the effects of the surveillance process to mitigate the influence of the (selfish or malicious) PUEA, we assume that the CR network contains two separate sets: the network coordinator and the CR users. The network coordinator is responsible for providing sensing and surveillance services, while CR users exploit these services for opportunistic data

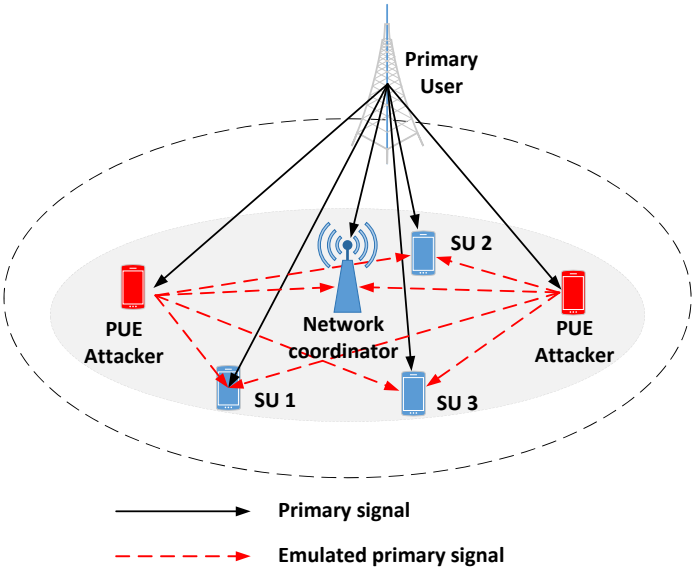


FIGURE 3.1 An example of a spectrum sensing-based CR network with the network coordinator and the PUEA attackers.

transmission. In such model, the PUEA attacker is also a cognitive user and can exploit the services, which are provided by the network coordinator. Noted that in the real, there are maybe several PUEA attackers in the network. However, in the presence of several PUEA attackers, the damage to the CR network will be at the highest level if they contribute a joint attack. Therefore, in our model, we assume that the joint PUEA by an attacker set is conducted by only one equivalent attacker. For simplicity of presentation, we denote by *attacker* the representative of the selfish attacker set and *defender* the representative of the network coordinator.

In a spectrum-sensing based CR networks, it is assumed that the network coordinator, hence the PUEA attacker, has a partial observation on the probability of the PU activity by conducting a fixed sensing period. In addition, the qualities of the sensing engine, *i.e.*, the probability of detection and the probability of false alarm in each wireless channel, are the prior knowledge for the network coordinator and the PUEA attacker.

Generally, as illustrated in Figure 3.2, the CR network operation is divided into time slots, each of which includes two periods: sensing and data transmission.

— In the sensing period, the network coordinator senses the radio environment to detect the presence of the primary signal on each channel. To ensure the accuracy of the spectrum sensing process, it is assumed that all cognitive users must vacate the channels. Various sensing techniques, such as the cooperative sensing, are adopted to improve the sensing accuracy. Due to the inherently unreliable nature of the wireless medium, there are two possible sensing results for each channel: "*unoccupied*", *i.e.*, the network coordinator decides that the channel is not occupied by the PUs, and

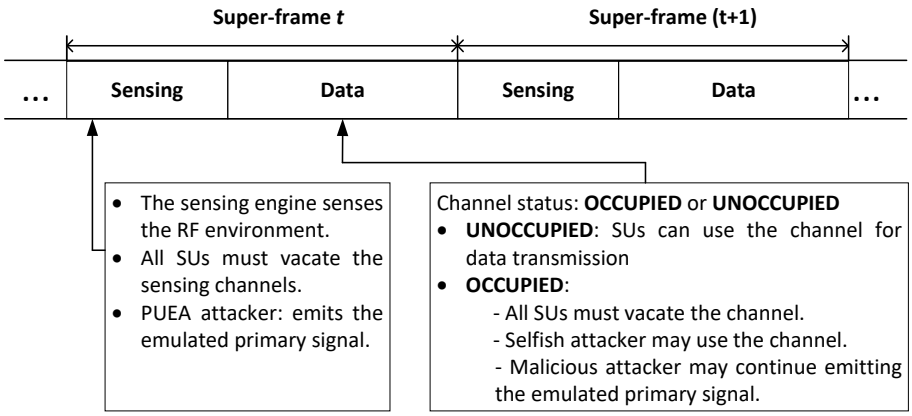


FIGURE 3.2 Timing frame for the network operation.

"*occupied*", *i.e.*, the network coordinator decides that the channel is occupied by the PUs [21]. Since the sensing service is provided by the network coordinator, which is independent of the CR users set, the sensing results are assumed to be fair. Hence, before every data period, the network coordinator broadcast the channel status to all users.

— In the data period, based on the provided channel status, if the channel is announced to be unoccupied, users may adopt multiple coordination or contention approaches to obtain channel access. On the contrary, if the channel is announced to be occupied, all CR users are prohibited to use the channel. Any secondary access to the prohibited channel is illegal and considered as an attack.

Note that because of the imperfect sensing (*i.e.*, the probability of detection is smaller than 1 and the probability of false alarm is higher than 0), a PU can be undetected and then undergoes interference from CR users. This problem is well-known in the CR network literature [8, 21, 83]. We do not solve this issues in this chapter, but rather focus on addressing the PUEA issue, which has negative effects even without sensing errors. In addition, the details of the data transmission like channel coding and modulation are irrelevant to the discussion in this chapter.

3.2.1 Attack and Surveillance Process

During the sensing period, the PUEA attacker can either emit or not emit the emulated primary signal relative to a certain channel. We assume that the sensing engine cannot distinguish the emulated and legitimate primary signals; hence, the PUEA will not be detected in the sensing period. In addition, before each time slot, the network manager ignores whether the PU is active or not. In addition, the attacker cannot know the true status of the primary signal on the attacked channels because it is busy transmitting an emulated primary signal in the same channel. This means that the attacker conducts a PUEA without information on

the status of the primary user signal before the start of sensing period of each time slot. It is to be noted that some literature studies [21, 27] assume that the attacker conducts a PUEA with the *fallow set* (*i.e.*, the set of channels on which the PU is not active) before sensing period of each time. However, in such a case, the system model of the surveillance process is similar to the model of the surveillance process, which deals with PUEA without the fallow set. Hence, our focus in this chapter is on the study of the surveillance process to deal with PUEA without the fallow set. At data period, if the attacked channel is announced to be unoccupied, the attackers then act as normal CR users. Conversely, if the attacked channel is announced to be occupied, the selfish PUEA attacker then use this channel to transmit data selfishly while the malicious attacker then re-transmits the emulated primary signal to ensure that the network cannot retrieve the channel by implementing the re-sensing process.

Concerning the defense against a selfish PUEA attacker, we assume that a fixed format of the data frame is used to exchange data with all CR users, including selfish users. The format contains the identification of the user, *e.g.*, the *medium access control* (MAC) address. Consequently, CR users can be identified by observing the transmitted signals during the data time. The network coordinator then performs the channel surveillance process on prohibited secondary access channels to detect an illegal occupation, hence the selfish attacker. Once the attacker has been detected, punishments such as bandwidth limitation can be adopted to penalize the attacker. Concerning the defense against malicious PUEA attacker, we propose to re-sense the channel before transmitting data to re-determine the true status of the channel by an extra-sensing process, which is assumed to be implemented by network coordinator within the data frame.

Since the rational and intelligent attacker can learn to adapt the surveillance strategy by conducting a fixed period of monitoring, the defender can act pro-actively by committing to or not committing regarding its defense strategy. Depending on the defender's actions, we consider the two following cases:

— **Non-Commitment:** The defender does not consider to commit to it defense strategy. The attacker then optimizes its expected utility regarding all possible strategies of the defender.

— **Commitment:** The defender acts as a leader by committing to it surveillance (extra-sensing) strategy. The attacker then acts as a follower by performing the best response regarding the observed defense strategy.

3.2.2 Notations

For the t^{th} channel ($t = 1, \ldots, N$), we suppose that the presence probability of the PU is π_t. Other specific notations used throughout the paper are defined as follows:

— p_N^t is the probability that the channel is detected as occupied if the attacker does not attack the channel. Denoting by p_d^t and p_f^t the probability of detection and the

probability of false alarm when the attacker does not attack the channel, one can easily check that $p_N^t = \pi_t p_d^t + (1 - \pi_t) p_f^t$.

— p_A^t is the probability that the attacked channel is detected as occupied. Denoting by $p_{d|A}^t$ and $p_{f|A}^t$ the corresponding probability of detection and the probability of false alarm of the sensing engine when the attacker attacks on the channel [1], one can easily check that $p_A^t = \pi_t p_{d|A}^t + (1 - \pi_t) p_{f|A}^t$.

— ρ_N^t is the probability that the t^{th} channel is not used by the PU when the sensing engine notifies as occupied and the attacker does not attack. Using Bayes rule, we obtain that $\rho_N^t = (1 - \pi_t) p_f^t / p_N^t$.

— ρ_A^t is the probability that the t^{th} channel is not used by the PU when the sensing engine notifies as occupied and the attacker attacks. Using Bayes rule, we have $\rho_A^t = (1 - \pi_t) p_{f|A}^t / p_A^t$.

3.3 The Selfish Primary Emulation Attack

3.3.1 Problem Formulation

This section examines the surveillance process to deal with the multi-channel selfish PUEA in the spectrum-sensing based CR networks. Let us consider a CR network with N available channels in which the attacker can select up to M channels to implement the selfish PUEA and the network coordinator can select up to L channels to perform the surveillance process. Typically, we have $M \leq N$, $L \leq N$. Noted that The case $M > N$ (or $L > N$) is equivalent to $M = N$ (or $L = N$). Moreover, if $M = L = N$ the considered scheme would turn out to be the same as a single channel surveillance problem, that has already been studied in the literature [54]. Therefore, we assume that $M \leq N$ and $L \leq N$. An example of the channel surveillance game for a CRN with $(N, M, L) = (2, 1, 1)$ is illustrated in Figure 3.3 [2].

By adopting the game theoretical framework, we formulate the interaction between the selfish PUEA and the surveillance process as a two-players extensive-form game, including the player set, the strategy set, the payoff and the expected payoff for each player, as follows.

Player set

The player set of the game is $\Gamma = \{$*Attacker, Defender*$\}$

— **Attacker** who emits the emulated primary signal to attack the CR network for a selfish purpose.

— **Defender** who monitors the occupied channels to catch the illegal occupation by the selfish PUEA attacker.

1. Suppose that the energy detection is adopted for spectrum sensing and the attacker emits the emulated primary signal at the same power as PU. If the threshold value for the energy detection is not changed, one can easily to find the value of $p_{d|a}^t$ and $p_{f|a}^t$ from p_d^t and p_f^t.

2. We denote by p_m^n the probability of the m^{th} sensing result when the attacker plays S_n.

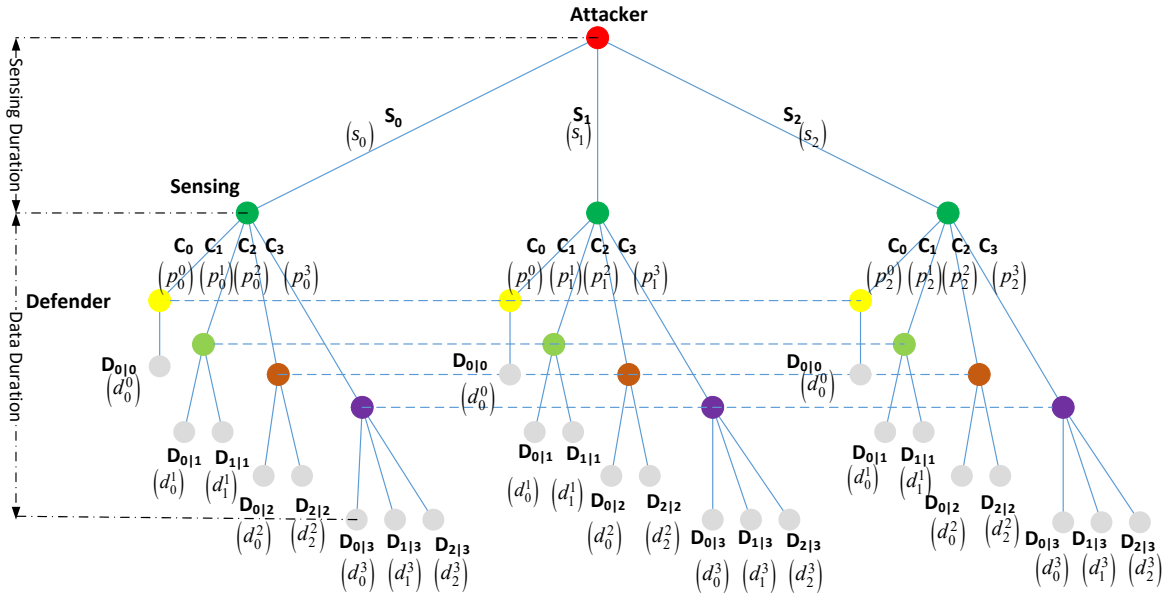


FIGURE 3.3 The surveillance process to deal with the selfish PUEA in a CR network with $N = 2$ available channels where the attacker can attack one channel ($M = 1$) and the defender can monitor one channel ($L = 1$) at a time.

Strategy set

For the attacker, let S_0 be the action not to transmit any emulated signal and let S_i $(i = 1, \ldots, K_1 - 1)$ be the action to transmit an emulated primary signal on a non-empty subset of available channels. Thus, the strategy set of the attacker is given by

$$\Sigma_S = \{S_0, S_1, S_2, \ldots, S_{K_1-1}\}, \tag{3.1}$$

where the total number of pure strategies is the total number of channel subsets with equal or less than M elements, *i.e.*,

$$K_1 = \sum_{i=0}^{M} \binom{N}{i}, \tag{3.2}$$

and $\binom{}{}$ is the binomial coefficient.

For the CR network with N available channels, there are 2^N possible sensing results. Let $\mathbf{C}$ be the set of sensing results. For the k^{th} element $C_k \in \mathbf{C}$ $(k = 0, \ldots, 2^N - 1)$, we denote by $s(C_k)$ the number of occupied channels. The defender can take the action $D_{j|k}$ $(j \neq 0)$ to implement a surveillance process on the j^{th} subset of occupied channels of C_k or $D_{0|k}$ not to monitor any channel. For a given C_k, let Σ_D^k be the corresponding strategy set of the defender. Hence, the size of Σ_D^k is given by

$$\sum_{j=0}^{min(L,s(C_k))} \binom{s(C_k)}{j}. \tag{3.3}$$

TABLE 3.1 The relationship between the player payoffs and the presence of the PU for a pair of actions at the t^{th} channel in the selfish PUEA case.

PU	**Attacker**	**Sensing**	**Defender**	**Payoff** (Attacker, Defender)
Inactive	Attack	Occupied	Surveillance	$(-C_A^t - P_A^t, -C_S^t + G_S^t)$
			No Surveillance	$(-C_A^t + G_A^t, 0)$
		Unoccupied	No Surveillance	$(-C_A^t, 0)$
	No Attack	Occupied	Surveillance	$(0, -C_S^t)$
			No Surveillance	$(0, 0)$
		Unoccupied	No Surveillance	$(0, 0)$
Active	Attack	Occupied	Surveillance	$(-C_A^t, -C_S^t)$
			No Surveillance	$(-C_A^t, 0)$
		Unoccupied	No Surveillance	$(-C_A^t, 0)$
	No Attack	Occupied	Surveillance	$(0, -C_S^t)$
			No Surveillance	$(0, 0)$
		Unoccupied	No Surveillance	$(0, 0)$

Due to the incomplete information, strategies of the defender are formulated by combining the action sets of each sensing result, *e.g.*, $\left(D_{0|0}, D_{1|1}, D_{2|2}, D_{1|3}\right)$, etc. Thus, the pure strategy set of the defender is written as

$$\Sigma_D = \{D_0, D_1, \ldots, D_{K_2-1}\}\big|_{D_j \in \Sigma_D^0 \times \Sigma_D^1 \times \ldots \Sigma_D^{2^N-1}} \tag{3.4}$$

The size of Σ_D is given by

$$K_2 = \prod_{k=0}^{2^N-1} \sum_{j=0}^{min(L, s(C_k))} \binom{s\left(C_k\right)}{j}. \tag{3.5}$$

Payoff

To calculate the payoff of two players for a pair of actions, we first introduce the related gain and cost for each player's actions at each channel. For the attacker, at the t^{th} channel, let C_A^t be the cost for implementing selfish PUEA, G_A^t be the benefit of using the channel for any CR user at one data frame and P_A^t be the penalty value for being captured by the defender. Similarly, for the defender, let C_S^t be the cost for implementing the surveillance process of the data frame and G_S^t be the benefit for capturing the selfish PUEA attacker during the surveillance process of the data frame.

For each channel, if the PU was active in the data period then the PU signal would interfere with the attacker's data transmission. Without loss of generality, we assume that the PU signal would be well in that case. Consequently, the attacker will gain nothing from the selfish PUEA. Also, the defender cannot distinguish the PU signal from the attacker's

TABLE 3.2 Action payoffs for the attacker (left) and the defender (right) at the t^{th} channel in the scenario of selfish PUEA.

Attacker	**Defender**	
	Surveillance (when occupied)	No surveillance
Attack	$p_A^t\left(-C_A^t-\rho_A^t P_A^t\right);\, p_A^t\left(-C_S^t+\rho_A^t G_S^t\right)$	$-C_A^t+p_A^t\rho_A^t G_A^t; 0$
No Attack	$0; -p_N^t C_S^t$	$0; 0$

signal [3]. We hence obtain the payoff of each player for a pair of actions regarding the presence of the PU at the t^{th} channel as given in Table 3.1. The corresponding expected payoffs (w.r.t. PU presence and sensing results) for the attacker and the defender are shown in Table 3.2.

Expected Payoff

To compute the corresponding expected payoff for each player, we imagine a game as a finite, rooted tree where each leaf in the game tree represents a terminal state (*i.e.*, the state at which the game ends). Let $\mathbf{Z}$ be the set of terminal states where $\theta_s(z)$ and $\theta_d(z)$ are the corresponding actions of the attacker and the defender that lead to a terminal state $z \in \mathbf{Z}$, respectively. Let $\delta_s(z)$ and $\delta_d(z)$ be the corresponding probabilities of the action $\theta_s(z)$ and $\theta_d(z)$, respectively.

For the strategy pair $\{\theta_s(z), \theta_d(z)\}$, the payoff of the attacker is given by

$$U_S\left(\theta_s(z), \theta_d(z)\right) = \sum_{t \text{ is considered in } \theta_s(z)} U_S^{t,\theta_d(z)}, \tag{3.6}$$

where $U_S^{t,\theta_d(z)}$ is the payoff of the attacker at channel t which is considered in action $\theta_s(z)$ when the defender plays strategy $\theta_d(z)$. Similarly, the payoff of the defender for the strategy pair $\{\theta_s(z), \theta_d(z)\}$ is given by

$$U_D\left(\theta_s(z), \theta_d(z)\right) = \sum_{k \text{ is considered in } \theta_d(z)} U_D^{\theta_s(z),k}, \tag{3.7}$$

where $U_D^{\theta_s(z),k}$ is the payoff of the defender at channel k which is considered in action $\theta_d(z)$ when the attacker plays strategy $\theta_s(z)$.

3. Due to the interference between the PU's signal and the attacker's signal, the defender cannot identify the ID (*i.e.*, the identification) of the attacker.

Let $P(z)$ be the probability of the sensing result on the path from the root to z, the expected payoffs of the attacker and the defender are given by

$$\Omega_S = \sum_{z \in Z} P(z)\, \delta_s(z)\, \delta_d(z)\, U_S(\theta_s(z), \theta_d(z)), \tag{3.8a}$$

$$\Omega_D = \sum_{z \in Z} P(z)\, \delta_s(z)\, \delta_d(z)\, U_D(\theta_s(z), \theta_d(z)). \tag{3.8b}$$

3.3.2 The Non-Commitment Case

The class of extensive-form game like the multi-channel surveillance game can be solved through the strategic-form representation by using Harsanyi transformation [78] and the Lemke-Howson algorithm [86]. Such representation, however, results in an exponential increment in the size of the game, thus making it computationally impractical. For example, for $N = M = L = 1$, the payoff matrix of the game is 3×12. However, for $N = 4, M = L = 1$, the payoff matrix of the game is 5×14929920. It means that it is very complicated to find the NE points of the game with a large number of available channels N by using the strategic-form representation. Hence, we adopt the sequence-form representation approach to present and determine the NE of the game.

Sequence Strategy Set

In an extensive-form game, a *sequence* is defined as a chain of action choices that a player would have to take in order to get from the root of the game tree to a given node. Also, the action from a root to itself is considered as an empty sequence and denoted by $\emptyset$. For the multi-channel surveillance game, by considering *the sensing result as an element of the attacker's sequence*, the sequence strategy set of the attacker is defined as

$$\begin{aligned} \mathbf{\Sigma}_{S,seq} &= \{\sigma_{Si}, i = 1, \ldots, K_3\} \\ &= \left\{\emptyset, S_0, S_1, S_2, \ldots, S_{K_1-1}, S_{\emptyset|C_0}, S_{0|C_1}, \ldots\right\} \end{aligned} \tag{3.9}$$

where $S_{j|C_j}$ is the sequence strategy of the attacker from the root to the node C_j through S_j, K_3 is the size of the sequence strategy set of the attacker

$$K_3 = 1 + K_1 + K_1 \times 2^N = 1 + K_1 \times \left(2^N + 1\right) \tag{3.10}$$

For the defender, the sequence strategy set is given by

$$\begin{aligned} \mathbf{\Sigma}_{D,seq} &= \{\sigma_{Dj}, j = 1, \ldots, K_4\} \\ &= \left\{\emptyset, D_{0|C_k}, D_{1|C_k}, \ldots, D_{|C_k|,C_k}, \ldots\right\}_{C_k \in \mathbf{C}} \end{aligned} \tag{3.11}$$

where K_4 is given by

$$K_4 = 1 + \sum_{k=0}^{2^N-1} |\Sigma_D^k| = 1 + \sum_{k=0}^{2^N-1} \sum_{j=0}^{min(L,|C_k|)} \binom{|C_k|}{j} \tag{3.12}$$

Mixed Sequence Strategy Set

The players can choose their actions based on a pure or a mixed-strategy (*i.e.*, the set of an assignment of a probability to each pure strategy). Since pure strategy equilibrium is just a special case of mixed ones, we consider the mixed sequence strategy. Let Φ_S and Φ_D be the set of mixed sequence strategy of the attacker and the defender, respectively. We have

$$\Phi_S = \{\phi_s^i\}_{i=1,\ldots,K_3} \tag{3.13a}$$

$$\Phi_D = \{\phi_d^j\}_{j=1,\ldots,K_4} \tag{3.13b}$$

where ϕ_s^i is the probability of the attacker's i^{th} sequence and ϕ_d^j is the probability of the defender's j^{th} sequence.

The relationship between these mixed strategies is represented by a *realization plan* under the following conditions: i.) the probability of the empty sequence ($\emptyset$) is 1, and ii.) the mixed strategy of a sequence at any decision node is the sum of all mixed strategies from it. Hence, the realization plan for the attacker's sequence strategy is given by

$$\begin{cases} \phi_s(\emptyset) = 1 \\ \phi_s(S_0) + \sum_{k=1}^{K_1-1} \phi_s(S_i) = 1 \\ \sum_{i=0}^{2^N-1} \phi_s\left(S_{0|C_i}\right) = \phi_s(S_0) \\ \sum_{i=0}^{2^N-1} \phi_s\left(S_{1|C_i}\right) = \phi_s(S_1) \\ \vdots \\ \sum_{i=0}^{2^N-1} \phi_s\left(S_{K_1-1|C_i}\right) = \phi_s(S_{K_1-1}) \\ 0 \le \phi_s^i \le 1, i = 1, \ldots, K_3 \end{cases} \tag{3.14}$$

Similarly, the realization plan for the defender's sequence strategy is given by

$$\begin{cases} \phi_d(\emptyset) = 1 \\ \phi_d\left(D_{\emptyset|C_k}\right) + \sum_{t=1}^{|\Sigma_D^k|} \phi_d\left(D_{t|C_k}\right) = 1, \ k = 0, \ldots, 2^N - 1 \\ 0 \le \phi_d^j \le 1, j = 1, \ldots, K_4 \end{cases} \tag{3.15}$$

Generally, these realization plans can be re-written in the matrix-form as

$$\begin{cases} \mathbf{E}\Phi_S = \mathbf{e} \\ \Phi_S \ge 0 \end{cases}, \quad \text{and} \quad \begin{cases} \mathbf{F}\Phi_D = \mathbf{f} \\ \Phi_D \ge 0 \end{cases}, \tag{3.16}$$

where $\mathbf{E}$, $\mathbf{F}$ are the *constraint matrices* of size $(K_1+1)\times K_3$ and $(K_2+1)\times K_4$, $\mathbf{e}$ and $\mathbf{f}$ are the vector of length K_3 and K_4 in which the first element is 1 and all other elements are 0.

Payoff

For the t^{th} channel, the payoff of the attacker and the defender are computed as in Table 3.2. We suppose that $\mathbf{\Pi}_S$ and $\mathbf{\Pi}_D$ are the payoff matrix of the attacker and the defender, respectively.

The expected payoff of the attacker Ω_S and defender Ω_D are determined as in (3.6) and (3.7), respectively.

Nash Equilibrium

In game theory, the Nash Equilibrium (NE) of a game is defined as the point where each player has selected the best response (or one of the best responses) to the other players' strategies [87]. The best response is the strategy (or strategies) playing in which a player gains the highest payoff given other players' strategies. In the multi-channel surveillance game, for a given strategy Φ_D, Φ_S is the best response to Φ_D if and only if it is an optimal solution of the following linear program:

$$\begin{aligned} \underset{\Phi_S}{\text{maximize}} \quad & \Phi_S^T\left(\mathbf{\Pi}_S\Phi_D\right) \\ \text{subject to} \quad & \mathbf{E}\Phi_S = \mathbf{e} \\ & 0 \le \Phi_S \le 1 \end{aligned} \tag{3.17}$$

The dual-form of linear program (3.17) is given by:

$$\begin{aligned} \underset{\mathbf{p}}{\text{minimize}} \quad & \mathbf{e}^T\mathbf{p} \\ \text{subject to} \quad & \mathbf{E}^T\mathbf{p} \ge \mathbf{\Pi}_S\Phi_D \end{aligned} \tag{3.18}$$

From two linear programs (3.17) and (3.18), we have

$$\mathbf{e}^T\mathbf{p} = \left(\mathbf{E}\Phi_S\right)^T\mathbf{p} = \Phi_S^T\mathbf{E}^T\mathbf{p} \ge \mathbf{\Phi_S^T\Pi_S\Phi_D} \tag{3.19}$$

Thus, the feasible solutions $(\Phi_S, \mathbf{p})$ of these two linear programs (3.17) and (3.18) are optimal if and only if the values of two objective functions are equal, *i.e.*, $\Phi_S^T\left(\mathbf{\Pi}_S\Phi_D\right) = \mathbf{e}^T\mathbf{p}$ or

$$\Phi_S^T\left(-\mathbf{\Pi}_S\Phi_D + \mathbf{E}^T\mathbf{p}\right) = 0$$

A similar program is established for the defender strategy Φ_D and the corresponding dual solution $\mathbf{q}$. Feasible solutions Φ_D and $\mathbf{q}$ of these two linear programs are optimal if and only if the values of two objective functions are equal, *i.e.*, $\Phi_D^T\left(-\mathbf{\Pi}_D^T\Phi_S + \mathbf{F}^T\mathbf{q}\right) = 0$.

In summary, the problem of finding a NE of the multi-channel surveillance game can be formulated as a problem of finding $(\mathbf{p}, \mathbf{q}, \Phi_S, \Phi_D)$, which satisfies the following conditions:

$$\begin{aligned}
&\Phi_S^T \left(-\mathbf{\Pi}_S \Phi_D + \mathbf{E}^T \mathbf{p}\right) = 0 \\
&\Phi_D^T \left(-\mathbf{\Pi}_D^T \Phi_S + \mathbf{F}^T \mathbf{q}\right) = 0 \\
&\mathbf{E}^T \mathbf{p} \geq \mathbf{\Pi}_S \Phi_D \\
&\mathbf{F}^T \mathbf{q} \geq \mathbf{\Pi}_D^T \Phi_D \\
&\mathbf{E} \Phi_S = \mathbf{e} \\
&\mathbf{F} \Phi_D = \mathbf{f} \\
&\Phi_S \geq 0 \\
&\Phi_D \geq 0
\end{aligned} \tag{3.20}$$

To solve the linear programs (3.20), we introduce a non-negative vector

$$\mathbf{z} = \left(\mathbf{\Phi_S}, \mathbf{\Phi_D}, \mathbf{p}^{'}, \mathbf{p}^{''}, \mathbf{q}^{'}, \mathbf{q}^{''}\right)^T,$$

where $\mathbf{p}^{'}$, $\mathbf{p}^{''}$ and $\mathbf{q}^{'}$, $\mathbf{q}^{''}$ are non-negative vectors of the same dimension that $\mathbf{p} = \mathbf{p}^{'} - \mathbf{p}^{''}$ and $\mathbf{q} = \mathbf{q}^{'} - \mathbf{q}^{''}$. Furthermore, let

$$\mathbf{M} = \begin{bmatrix}
0 & -\mathbf{\Pi}_S & \mathbf{E}^T & -\mathbf{E}^T & 0 & 0 \\
-\mathbf{\Pi}_D^T & 0 & 0 & 0 & \mathbf{F}^T & -\mathbf{F}^T \\
-\mathbf{E} & 0 & 0 & 0 & 0 & 0 \\
\mathbf{E} & 0 & 0 & 0 & 0 & 0 \\
0 & -\mathbf{F} & 0 & 0 & 0 & 0 \\
0 & \mathbf{F} & 0 & 0 & 0 & 0
\end{bmatrix} \tag{3.21}$$

and $\mathbf{b}^T = \begin{pmatrix} 0, & 0, & \mathbf{e}, & -\mathbf{e}, & \mathbf{f}, & -\mathbf{f} \end{pmatrix}^T$. The value of $(\mathbf{p}, \mathbf{q}, \Phi_S, \Phi_D)$ that satisfies (3.20) can be found through the standard Linear Complementary Programing (LCP) [88] as follows:

$$\begin{aligned}
&\text{find} \quad \mathbf{z} \\
&\text{s.t} \quad \mathbf{Mz} + \mathbf{b} \geq \mathbf{0} \\
&\qquad \mathbf{z}^T (\mathbf{Mz} + \mathbf{b}) = 0 \\
&\qquad \mathbf{z} \geq 0
\end{aligned} \tag{3.22}$$

By solving (3.22), we obtain the solution of (3.20). This solution is the NE point of the game. The LCP problem above is solved by the *Lemke algorithm* [79, 88, 89]. The original work on sequence-form game representation [79] has proved that the algorithm terminates with at least one solution [4].

4. Please refer to the Appendix B

Strategic-form vs. Sequence-form representation

Proposition 3.1. *In the non-commitment multi-channel surveillance game, the size of payoff matrix in the sequence-form representation is exponentially smaller than the size of payoff matrix in the strategic-form representation.*

Proof. From (3.10) and (3.12), the size of payoff matrix in the sequence form representation is $K_3 \times K_4$, This size is clearly linear in size of the game (N, M, L). It means that the sequence form method is more efficient and robust than the conventional strategic-form representation approach in order to determine the NE strategy of the game. For example, for a CR network with $N = 4, M = L = 1$, the payoff matrix in sequence form representation is 86×49. This size is much smaller than one with the strategic-form approach (*i.e.*, (5×14929920)). Therefore, we adopted the sequence form representation method to determine the NE point of the game. □

From the Proposition 3.1, we observed that the strategy space of the sequence form representation is exponentially smaller than the strategy space of the strategic-form representation. Since the two methods operate similarly [79, 89], the computation time of each algorithm depends on the size of the input. Thus, it is faster to run the Lemke algorithm on the sequence-form representation than the Lemke–Howson algorithm on the strategic-form.

3.3.3 The Commitment Case

Due to the rationality of the attacker and the rapid expansion of software-defined radio, the attacker can observe the (mixed) surveillance strategy of the defender. To overcome this issues, the defender can act pro-actively by committing to or not committing regarding its defense strategy. How to determine the committing strategy of the defender as well as the best response of the attacker is an important question. We then build the Stackelberg model based surveillance game, which will reduce the computational requirement for finding the Strong Stackelberg equilibrium (SSE) and may result in a better expected payoff depending on the system parameters. In such a game, the defender acts as the *Leader* by monitoring the occupied channels to catch the illegal occupations while committing to a (mixed) surveillance strategy. In contrast, the attacker acts as the *Follower* by optimizing its outcome regarding the committed surveillance strategy.

Strategy Set

In the Stackelberg game, the strategy of each player is the set of its actions in the path from the root to each terminal state. As defined above, Z is the set of terminal states, whose size is given by

$$K_5 = K_1 \sum_{k=0}^{2^N-1} \sum_{j=0}^{min(L,s(C_k))} \binom{s\,(C_k)}{j}. \tag{3.23}$$

Thus, there are K_5 pure strategies, so we can write the pure strategy set of the defender as follows:

$$\Theta_D = \{\theta_d(z)\}_{z \in Z}. \tag{3.24}$$

Similarly, there are K_5 pure strategies, so we can write the pure strategy set of the attacker as follows:

$$\Theta_S = \{\theta_s(z)\}_{z \in Z}. \tag{3.25}$$

For example, the game illustrated in Figure 3.3 contains $K_5 = 3 \times 8 = 24$ terminal states. For each terminal state, we have a pure strategy of the attacker and a corresponding pure strategy of the defender, *e.g.*, $(S_0, D_{0|0})$, $(S_0, D_{0|1})$, $(S_0, D_{1|1})$, etc.

The mixed strategies for the defender and the attacker are respectively defined by

$$\Delta_D = \{\delta_d(z)\}_{z \in Z}, \tag{3.26a}$$

$$\Delta_S = \{\delta_s(z)\}_{z \in Z}. \tag{3.26b}$$

Expected Payoff

The expected payoffs of each player are computed as given in (3.8a) and (3.8b), respectively.

Strong Stackelberg Equilibrium

In the commitment model, the best strategy for the defender is the Strong Stackelberg Equilibrium (SSE) [90], which is defined as follows:

Definition 3.2. *A pair of strategies $(\gamma_s(\delta_d), \delta_d)$ forms a Strong Stackelberg Equilibrium (SSE) if it satisfies the following:*

1. *The follower plays a best response*

$$\Omega_S(\gamma_s(\delta_d), \delta_d) \geq \Omega_S(\delta_s, \delta_d) \, \forall \delta_s \in \Delta_S, \delta_d \in \Delta_D,$$

2. *The leader plays a best response*

$$\Omega_D(\gamma_s(\delta_d), \delta_d) \geq \Omega_D\left(\gamma_s(\delta_d'), \delta_d'\right) \forall \delta_d' \in \Delta_D,$$

3. *If the follower has the choice of best response, then it advantages the leader*

$$\Omega_D(\gamma_s(\delta_d), \delta_d) \geq \Omega_D\left(\delta_s', \delta_d\right) \forall \delta_s' \in \Delta_S^*(\delta_d), \delta_d \in \Delta_D,$$

where $\gamma_s(\cdot)$ denotes the follower's response function and $\Delta_S^*(\delta_d)$ denotes the set of the follower's best responses to δ_d.

From the Definition 3.2, we observe that the expected payoff of the defender in the SSE strategy is always at least as high as one in any NE profile [90]. The reason is that, in the commitment model, the leader can at the very least choose to commit to its NE strategy. If it does so, then among its best responses the follower will choose one that maximizes the utility of the leader due to the tie-breaking assumption. In the non-commitment model, however, the follower will choose from his best responses to this defender strategy but not necessarily the ones that maximize the leader's utility.

For a given mixed strategy of the defender, the best pure strategy of the attacker belongs to its set of best-mixed strategies because *its expected payoff is a linear function* [90–93]. Therefore, we restrict the attacker's pure strategies to find out the optimal strategy of the defender. The *Multiple Linear Programs* (MLP) [91] method is adopted to determine the SSE equilibrium of the game by solving a set of linear programs for *each pure strategy* of the attacker as follows.

Multiple Linear Program (MLP)

$$\max_{\delta_d} \sum_{z \in Z} P(z)\, \delta_s(z)\, \delta_d(z)\, U_D(z) \tag{3.27}$$

$$s.t \sum_{z \in Z | \sigma_s(z) = S_j} P(z)\, \delta_s(z)\, \delta_d(z)\, U_S(z) \geq \sum_{z' \in Z | \sigma_s(z') = S_k} P(z')\, \delta_s(z')\, \delta_d(z)\, U_S(z') \tag{3.28}$$

$$\sum_{z \in Z | C_k \text{leads to } z} \delta_d(z) = 1, \forall C_k \in C \tag{3.29}$$

$$0 \leq \delta_d(z) \leq 1, \forall z \in Z \tag{3.30}$$

Typically, MLP is a natural divide-and-conquer approach. The main idea is to consider each pure strategy of the follower in turn by solving the corresponding linear program. For each linear program, given a pure strategy of the attacker, we must find the corresponding mixed strategy of the defender that satisfies: i.), the given pure strategy of the attacker is the best response and ii.), the expected payoff of the defender is maximized. By solving all separated linear programs, we can determine the optimal mixed strategy for the defender. In particular, for the multi-channel surveillance game, we must consider K_1 linear programs, each for a pure strategy of the attacker as presented by (3.27)-(3.30). Each linear program works as follows: the first constraint (3.28) says the given attacker strategy must be the best response to the defender's strategy. Other constraints (3.29), (3.30) provide the bound for the defender's strategy. The objective (3.27) ensures the defender's expected payoff is maximal. In general, we adopt Algorithm 1 to determine the SSE strategy of the game. The SSE strategy is achieved by choosing one with the highest optimal solution value in the solutions of K_1 linear program. Since each of the linear programs can be solved in polynomial time, the MLP gives a *polynomial time* to calculate the SSE of the game.

Algorithm 1 MLP Algorithm

1: **for** each pure strategy of the attacker $\delta_s^*(z)$ **do**
2: Compute the best response of the defender $\delta_d^*(z)$ by using MLP
3: Store the expected payoff $U_D\left(\delta_s^*\left(z\right), \delta_d^*\left(z\right)\right)$
4: Compare the expected payoff for each pair of $\left(\delta_s^*\left(z\right), \delta_d^*\left(z\right)\right)$
5: Determine the SSE strategy

Commitment vs. Non-commitment

Hereafter we analyze the expected payoffs associated with two players, as well as the time required to determine the equilibrium strategies, allowing for a clear comparison between non-commitment and commitment strategies for the network manager.

Corollary 3.3. *In the multi-channel surveillance game, the defender's expected payoff obtained in SSE strategy is at least as high as one in any NE strategy.*

Proof. It is direct consequence of Definition 3.2. □

Corollary 3.4. *In the multi-channel surveillance game, finding the NE strategy in the non-commitment case is approximately* 2^N *time more complex than computing the SSE strategy in the commitment case.*

Proof. To determine the NE strategy in the non-commitment case, the computational algorithms must consider all possible mixed strategies of both players. It means that we must solve at least K_3 linear programs, each with K_2 variables, through the sequence-form representation [76]. In contrast, the MLP algorithm considers only K_1 linear program of a smaller number of variables ($K_5 \ll K_2$) for each attacker's pure strategy in order to determine the SSE strategy. We conclude that the algorithm to determine the NE strategy in the non-commitment case is approximately 2^N times more complex than the MLP algorithm to determine the SSE strategy in the commitment case. □

Two corollaries suggest that, in the surveillance process, the commitment model leading to the SSE defense strategy is a better candidate to mitigate selfish PUEA in CR networks than the non-commitment approach (leading to the NE defense strategy).

3.4 The Malicious Primary Emulation Attack

We formulate the relationship between the malicious PUEA and the extra-sensing process in a similar ways as the case of selfish PUEA. The game is illustrated in Figure 3.4 with $N = 2, M = L = 1$.

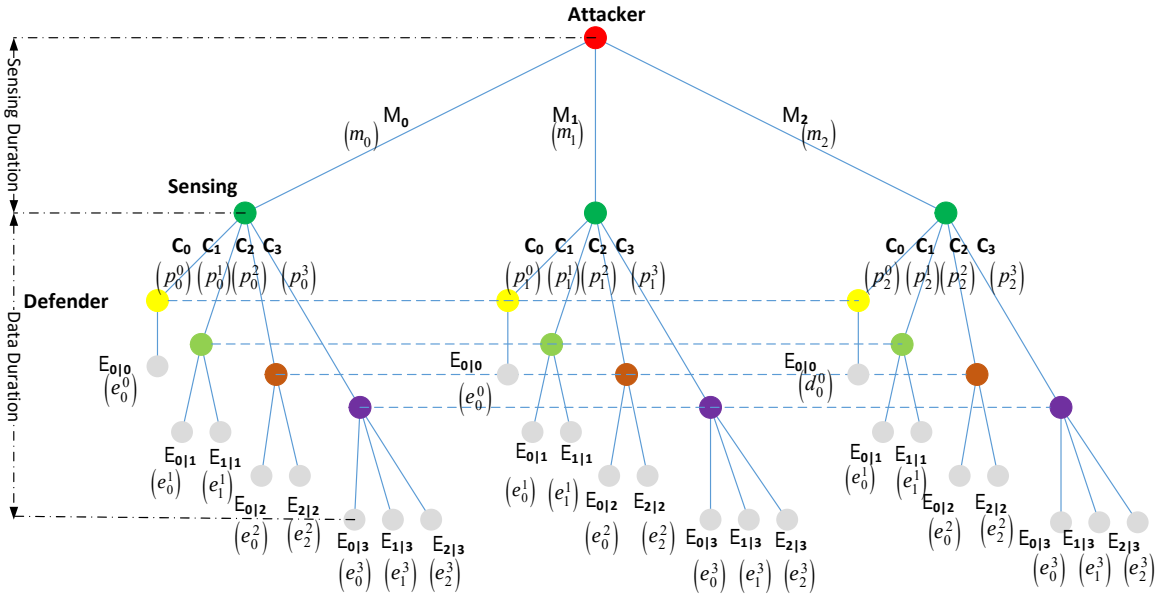


FIGURE 3.4 The extra-sensing process to deal with the malicious PUEA in a CR network with 2 available channels where the attacker/defender can attack/monitor one channel at a time.

Player set

The player set of the game is $\Gamma = \{Attacker,\ Defender\}$

— **Attacker** who emits the emulated primary signal to attack the CR network for a malicious purpose.

— **Defender** who re-senses the occupied channels to mitigate the influence of the malicious PUEA and retrieve the opportunity of using the channels which are announced to be occupied.

Strategy set

For the attacker, let M_i be the action to emit an emulated primary signal on a non-empty subset of available channels for malicious PUEA and let M_0 be the action not to transmit any emulated signal. Thus, the strategy set of the attacker is given by

$$\Sigma_M = \{M_0, M_1, M_2, \ldots, M_{K_1-1}\}. \tag{3.31}$$

For a given C_k, let Σ_E^k be the corresponding strategy set of the defender, where $E_{j|k}\,(j \neq 0)$ is the action to implement an extra-sensing process on the j^{th} subset of occupied channels of C_k and $E_{0|k}$ is the action not to re-sense any channel. Due to the incomplete information, strategies of the defender are formulated by combining the action sets of each sensing result, *e.g.*, $\left(E_{\emptyset|0}, E_{\emptyset|1}, E_{\emptyset|2}, E_{\emptyset|3}\right)$, etc. These actions lead to a defender's pure strategy set of size

TABLE 3.3 The relationship between the player payoffs and the presence of the PU for a pair of actions at the t^{th} channel in the malicious PUEA case.

PU	**Attacker**	**Sensing**	**Defender**	**Payoff** (Attacker, Defender)
Inactive	Attack	Occupied	Extra-sensing	$(-2\,C_M^t, -C_E^t + G_E^t)$
			No Surveillance	$(-2\,C_M^t + G_M^t, 0)$
		Unoccupied	No Surveillance	$(-C_M^t, 0)$
	No Attack	Occupied	Extra-sensing	$(0, -C_E^t + G_E^t)$
			No Extra-sensing	$(0, 0)$
		Unoccupied	No Extra-sensing	$(0, 0)$
Active	Attack	Occupied	Extra-sensing	$(-2\,C_M^t, -C_E^t)$
			No Extra-sensing	$(-2\,C_M^t, 0)$
		Unoccupied	No Extra-sensing	$(-C_M^t, 0)$
	No Attack	Occupied	Extra-sensing	$(0, -C_E^t)$
			No Extra-sensing	$(0, 0)$
		Unoccupied	No Extra-sensing	$(0, 0)$

TABLE 3.4 Action payoffs for the attacker (left) and the defender (right) at the t^{th} channel in the scenario of malicious PUEA.

Attacker	**Defender**	
	Surveillance (when occupied)	No surveillance
Attack	$p_A^t\,(-2\,C_M^t)\,;\, p_A^t\,(-C_E^t + \rho_A^t G_E^t)$	$-2\,C_M^t + p_A^t \rho_A^t G_M^t; 0$
No Attack	$0; -p_N^t C_E^t + p_N^t \rho_N^t G_E^t$	$0; 0$

K_2 as follows.

$$\Sigma_E = \{ES_0, ES_1, \ldots, ES_{K_2-1}\}|_{ES_j \in \Sigma_E^0 \times \Sigma_E^1 \times \ldots \Sigma_E^{2^N-1}} \tag{3.32}$$

Payoff

To calculate the payoff of two players for a pair of actions, we first introduce the related gain and cost for each player's actions at each channel. For the attacker, at the t^{th} channel, let C_M^t be the cost for implementing malicious PUEA, G_M^t be the benefit of the malicious PUEA, which is equivalent to the degradation of the network due to malicious PUEA. For the defender, let C_E^t be the cost for implementing the extra-sensing process in the data frame and G_E^t be the benefit of obtaining the available channel by the extra-sensing process. Similar as the case of multi-channel surveillance process to deal with the selfish PUEA, we have the payoff of each player for a pair of actions regarding the presence of the PU at the t^{th} channel in Table 3.1. The corresponding expected payoffs of two players are shown in Table 3.4.

Expected Payoff

Let $\theta_m(z)$ and $\theta_e(z)$ be the corresponding actions of the attacker and the defender that lead to a terminal state $z \in Z$. We suppose that $\delta_m(z)$ and $\delta_e(z)$ are the corresponding probabilities of the action $\theta_m(z)$ and $\theta_e(z)$.

For the strategy pair $\{\theta_m(z), \theta_e(z)\}$, the payoff of the attacker is given by

$$U_M(\theta_m(z), \theta_e(z)) = \sum_{t \in \theta_m(z)} U_M^{t,\theta_e(z)}, \tag{3.33}$$

where $U_M^{t,\theta_d(z)}$ is the attacker's payoff at channel $t \in \theta_m(z)$ when the defender plays $\theta_e(z)$.

Similarly, the defender's for the strategy pair $\{\theta_m(z), \theta_e(z)\}$ is given by

$$U_E(\theta_m(z), \theta_e(z)) = \sum_{k \in \theta_e(z)} U_E^{\theta_m(z),k}, \tag{3.34}$$

where $U_E^{\theta_m(z),k}$ is the defender's payoff at channel $k \in \theta_e(z)$ when the attacker plays $\theta_m(z)$.

The expected payoffs of the attacker and the defender are given by

$$\Omega_M = \sum_{z \in Z} P(z)\, \delta_m(z)\, \delta_e(z)\, U_E(\theta_m(z), \theta_e(z)), \tag{3.35a}$$

$$\Omega_E = \sum_{z \in Z} P(z)\, \delta_m(z)\, \delta_e(z)\, U_M(\theta_m(z), \theta_e(z)). \tag{3.35b}$$

The non-commitment case with the sequence-form representation and the commitment case with the Stackelberg game are then formulated as same as the multi-channel surveillance game to deal with the selfish PUEA, respectively.

3.5 The General Primary Emulation Attack

In general, a rational PUEA attacker may perform either the selfish PUEA attack or the malicious one on some channels and the other type of attack for the other channels. The game, therefore, is a simultaneous-move game with incomplete information. To simplify the analysis of the game, we assume that the channel surveillance service contains both functions: extra-sensing and monitoring. In other words, by performing the channel surveillance process on the 'occupied'-declared channels, the network coordinator can determine the true status of the channel and detect the illegal occupation. We formulate the game between the general PUEA attacker and the network coordinator as follows.

TABLE 3.5 The relationship between the player payoffs and the presence of the PU for a pair of actions at the t^{th} channel in the general PUEA case.

PU	**Attacker**	**Sensing**	**Defender**	**Payoff** (Attacker, Defender)
Inactive	Selfish	Occupied	Surveillance	$(-C_A^t - P_A^t, -C_S^t + G_S^t)$
			No Surveillance	$(-C_A^t + G_A^t, 0)$
		Unoccupied	No Surveillance	$(-C_A^t, 0)$
	Malicious	Occupied	Surveillance	$(-C_A^t, -C_S^t + G_S^t)$
			No Surveillance	$(-C_A^t, 0)$
		Unoccupied	No Surveillance	$(-C_A^t, 0)$
	No Attack	Occupied	Surveillance	$(0, -C_S^t + G_S^t)$
			No Surveillance	$(0, 0)$
		Unoccupied	No Surveillance	$(0, 0)$
Active	Selfish	Occupied	Surveillance	$(-C_A^t, -C_S^t)$
			No Surveillance	$(-C_A^t, 0)$
		Unoccupied	No Surveillance	$(-C_A^t, 0)$
	Malicious	Occupied	Surveillance	$(-C_A^t, -C_S^t)$
			No Surveillance	$(-C_A^t, -C_S^t)$
		Unoccupied	No Surveillance	$(-C_A^t, -C_S^t)$
	No Attack	Occupied	Surveillance	$(0, -C_A^t)$
			No Surveillance	$(0, 0)$
		Unoccupied	No Surveillance	$(0, 0)$

Player set

The player set of the game is $\Gamma = \{$*Attacker, Defender*$\}$, with the attacker can implement both the the selfish and malicious PUEA.

Strategy set

For the t^{th} channel, the attacker may choose one of three possible actions: S_t to implement the selfish PUEA (*i.e.*, attacks and then uses the attacked channel if it is noticed to be occupied), M_t to implement the malicious PUEA (i.e, emits the primary emulated signal at the sensing period to fool the operation of the network), and NA_t not to attack the channel. Thus, the strategy of the attacker is formulated by the combining the actions sets on each channel. For example, if $N = M = 2$, the attack can choose $(NA_1 - NA_2)$, $(NA_1 - S_2)$, $(NA_1 - A_2)$, etc. Let Σ_A^i, $(i = 1, 2, \ldots, N)$ be the set of the attacker's actions at each channel. The pure strategy set of the attacker is then given by

$$\Sigma_A = \{A_0, A_1, \ldots, A_{K_6-1}\}|_{A_j \in \Sigma_A^1 \times \Sigma_A^2 \times \ldots \Sigma_A^N}, \tag{3.36}$$

where

$$K_6 = K_1 \times 3^M \tag{3.37}$$

TABLE 3.6 Action payoffs for the attacker (left) and the defender (right) at the t^{th} channel in the scenario of selfish PUEA without the fallow set.

Attacker	**Defender**	
	Surveillance (when occupied)	No surveillance
Selfish	$p_A^t\left(-C_A^t-\rho_A^t P_A^t\right);\, p_A^t\left(-C_S^t+\rho_A^t G_S^t\right)$	$-C_A^t+p_A^t\rho_A^t G_A^t; 0$
Malicious	$p_A^t\left(-C_S^t\right);\, p_A^t\left(-C_S^t+\rho_A^t G_S^t\right)$	$-C_S^t; 0$
No Attack	$0; -p_N^t C_S^t+p_N^t\rho_N^t G_S^t$	$0; 0$

Similarly, the pure strategy set of the defender is given by

$$\Sigma_D=\{D_0,D_1,\ldots,D_{K_2-1}\}|_{D_j\in\Sigma_D^0\times\Sigma_D^1\times\ldots\Sigma_D^{2^N-1}} \tag{3.38}$$

Payoff

For the t^{th} channel, let C_A^t be the cost for implementing PUEA, G_A^t be the benefit of PUEA, which is equivalent to the benefit of using the channel for any CR user at one data frame, P_A^t be the penalty value for being captured by the defender, C_S^t be the cost for implementing the surveillance process of the data frame, and G_S^t be the benefit of capturing the selfish PUEA attacker or obtaining the available channel during the surveillance process. We have the payoff of each player for a pair of actions regarding the presence of the PU at the t^{th} channel in Table 3.5. The corresponding expected payoffs of two players are shown in Table 3.6.

Expected Payoff

Let $\mathbf{Z}'$ be the set of terminal states in the game. Hence, the size of $\mathbf{Z}'$ is

$$K_7=K_6\times K_2 \tag{3.39}$$

Suppose that $\theta_a(z)$ and $\theta_d(z)$ are the corresponding actions of the attacker and the defender that lead to a terminal state $z\in Z'$. Let $\delta_a(z)$ and $\delta_d(z)$ be the corresponding probabilities of the action $\theta_a(z)$ and $\theta_d(z)$. For the strategy pair $\{\theta_a(z),\theta_d(z)\}$, the payoff of the attacker is given by

$$U_A\left(\theta_a(z),\theta_s(z)\right)=\sum_{t\in\theta_a(z)}U_A^{t,\theta_s(z)}, \tag{3.40}$$

where $U_A^{t,\theta_s(z)}$ is the attacker's payoff at channel $t\in\theta_a(z)$ when the defender plays $\theta_s(z)$.

Similarly, the defender's for the strategy pair $\{\theta_a(z),\theta_s(z)\}$ is given by

$$U_D\left(\theta_a(z),\theta_d(z)\right)=\sum_{k\in\theta_s(z)}U_D^{\theta_a(z),k}, \tag{3.41}$$

where $U_D^{\theta_a(z),k}$ is the defender's payoff at channel $k \in \theta_d(z)$ when the attacker plays $\theta_a(z)$.

The expected payoffs of the attacker and the defender are given by

$$\Omega_A = \sum_{z \in Z} P(z)\, \delta_a(z)\, \delta_d(z)\, U_A(\theta_a(z), \theta_d(z)), \tag{3.42a}$$

$$\Omega_D = \sum_{z \in Z} P(z)\, \delta_a(z)\, \delta_d(z)\, U_D(\theta_a(z), \theta_d(z)). \tag{3.42b}$$

The non-commitment case with the sequence-form representation and the commitment case with the Stackelberg game are then formulated as same as the multi-channel surveillance game to deal with the selfish PUEA, respectively. Similar to the selfish PUEA or the malicious PUEA scenarios, the size of the defender's sequence strategy in the non-commitment case is K_4. However, the size of the attacker's sequence strategy is

$$K_8 = 1 + K_6 \left(2^N + 1\right) \tag{3.43}$$

It means that, in the general PUEA, the size of the payoff matrix of each player in the non-commitment case with the strategic-form representation is $K_8 \times K_4$, which is much bigger than one in the selfish/malicious PUEA. For example, in the CR network with $N = 2, M = 2, L = 1$, the size of payoff matrices in the selfish/malicious PUEA with the non-commitment model is 176×49 while one in the general PUEA is 1584×49. However, it is much smaller than the one in the general PUEA with the strategic-form representation (176×14929920).

In the commitment case, the size of the strategy of the attacker and the defender is

$$K_9 = K_7 \sum_{k=0}^{2^N-1} \sum_{j=0}^{min(L, s(C_k))} \binom{s(C_k)}{j}. \tag{3.44}$$

3.6 Simulation Results

This section presents some numerical results to validate our analysis and analyze the influence of system parameters on the equilibrium strategies. The numerical simulations have been conducted in Matlab environment with CPLEX 12.4 [94] for optimization. We assume that the average SNR of the primary signal received at the spectrum sensor is -10 dB, the false alarm probability P_f is 0.1 [5] and the number of samples is 1500 samples. The detection probability (P_d) is computed from the false alarm probability and the number of samples through the *Constant False Alarm Rate* (CFAR) criterion, where the threshold is determined by keeping the false alarm rate constant. Without loss of generality, we assume that the benefit of a successful attack exceeds the attack cost for the attacker, *i.e.*,

5. As the IEEE Standard for Cognitive Wireless RAN IEEE.802.22 [8]

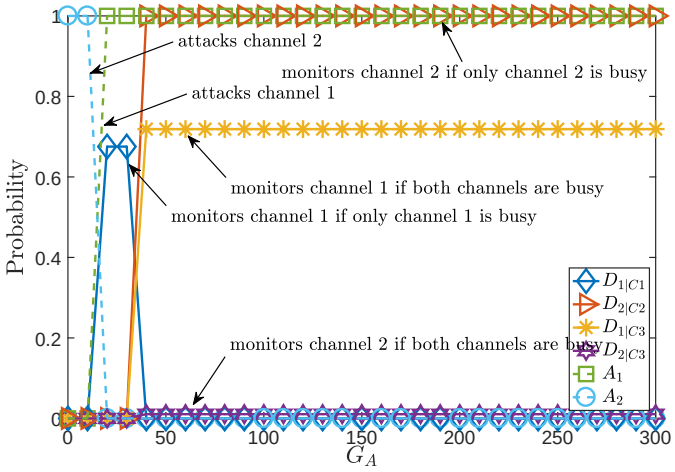


FIGURE 3.5 The SSE strategies of the attacker and the defender for the low attack gain ($G_A = 100$) when the attacker conducts a selfish PUEA.

$C_S^t < G_S^t, C_M^t < G_M^t, C_A^t < G_A^t$. This assumption guarantees that the attacker has the incentive to attack the CRN.

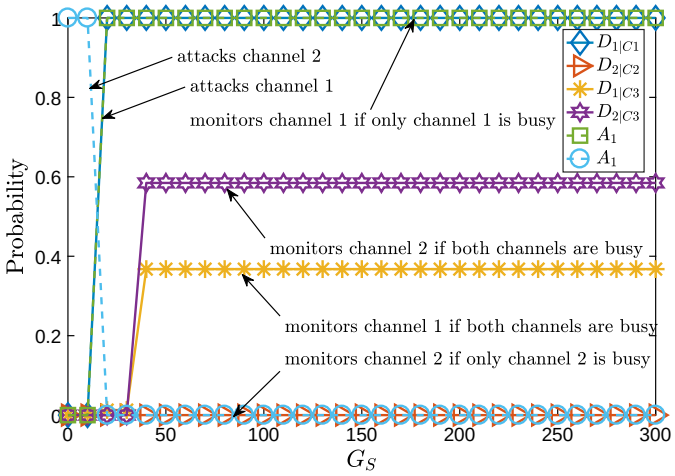


FIGURE 3.6 The SSE strategies of the attacker and the defender for the high attack gain ($G_A = 300$) when the attacker conducts a selfish PUEA.

3.6.1 The Selfish Primary Emulated Attack

When the attacker is captured, its punishment (penalty) consists of banning it from accessing the radio resources. Consequently, the saved radio resources will be beneficial for the rest of the network. In general, the gain of attack (G_A^t) and the gain of surveillance (G_S^t) depend on the being captured penalty (P_A^t). To simplify the problem, we assume that the cost/gain/penalty for the attack and the surveillance process are equal in all channels. To make the simulation results clear and easy to follow, we start with a CRN with two channels

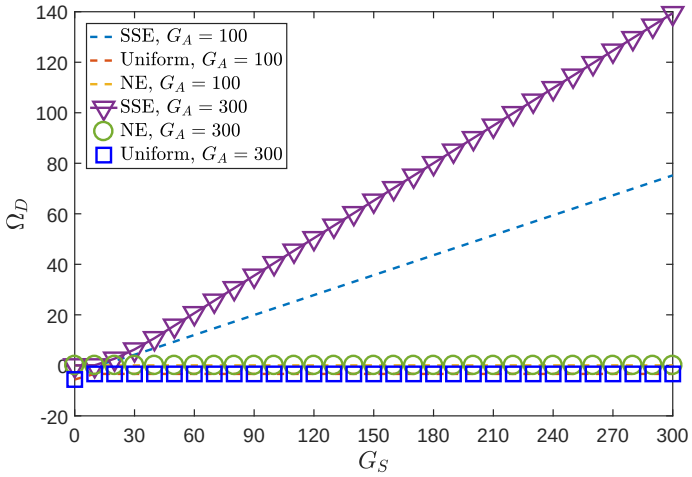


FIGURE 3.7 The expected payoff of the defender in three considered cases for $G_A = 100$ and $G_A = 300$ when the attacker conducts a selfish PUEA.

$(N = 2)$ with a capture penalty $P_A = 100$. We first consider the case where the attacker can attack up to $M = 1$ channel and the defender can monitor up to $L = 1$ channel at a time. Other parameters are $P_A = 100$, $C_A = 20$, $C_S = 10$, $\pi_1 = 0.2$ and $\pi_2 = 0.5$.

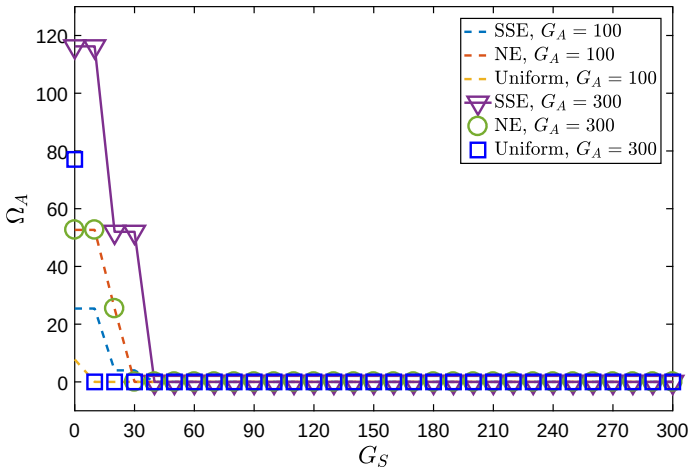


FIGURE 3.8 The expected payoff of the attacker in three considered cases for $G_A = 100$ and $G_A = 300$ when the attacker conducts a selfish PUEA.

Figure 3.5 and 3.6 presents the SSE strategies of the defender and the attacker in the commitment case with low attack gain ($G_A = 100$) and high attack gain ($G_A = 300$), respectively. We observe that, for a fixed captured penalty value, the SSE strategy of both players depends on G_A and G_S. For both cases, if G_S is low, the defender gives a low effort to implement the surveillance process on the occupied channels. The attacker, however, will implement the selfish PUEA on the CRN. If G_S is high, the defender will perform the following surveillance strategy on the occupied channel. We observed that for low G_A, the

defender monitors *channel* 2 if only channel 2 is busy. If both channels are busy, the defender then monitors *channel* 1. Conversely, for the high G_A, the defender monitors *channel* 1 if only channel 1 is busy and *channel* 1 with a probability 0.58 and *channel* 2 with a probability 0.36 if both channels are busy. Consequently, given any strategy of the defender, the best response of the attacker is to attack channel 1 since the presence probability of PU in channel 1 is smaller than in channel 2 ($\pi_1 = 0.2 < \pi_2 = 0.5$). This is based on the assumption that if the attacker has the choice of best response, then it advantages the defender.

To validate the benefits of the SSE strategy in the commitment model, we take into account the comparison between the expected payoffs of the defender and the attacker in three cases: 1) the commitment case where the defender and the attacker play their SSE strategy, 2) the non-commitment case where the defender and the attacker play their NE strategy, and 3) the commitment case where the defender plays the uniform strategy (*i.e.*, the defender performs the same probability for every possible strategy) and the attacker plays its best response to the defender's strategy.

Figure 3.7 shows the influence of the surveillance gain G_S on the expected payoffs of two players. We observe that, with the SSE strategy, the expected payoff of the defender is much higher than with the uniform strategy or the NE strategy. Similarly, Figure 3.8 shows the expected payoffs of the attacker when $G_A = 100$ and $G_A = 300$, respectively. We observe that, for most G_S, the expected payoff of the attacker obtained with the SSE strategy is approximately the one with the NE strategy. For the low surveillance gain (G_S), the defender will not perform the monitoring on the occupied channel due to the low gain, then the attacker will implement the selfish PUEA and achieve a positive expected payoff. In contrast, for the high surveillance gain (G_S), the expected payoff of the attacker in all considered cases will degrade to 0.

Figure 3.9 then shows the influence of the attack gain (G_A) on the expected payoffs of two players. We observe that, for a given surveillance gain (G_S), the expected payoff of the defender obtained with the SSE strategy is much higher than in the other cases. Similarly, Figure 3.10 shows the obtained expected payoff of the attacker when the surveillance gain $G_S = 30$ and $G_S = 300$, respectively. We observe that, for a given G_S, the expected payoff of the attacker when both players play their SSE strategy is approximately 0 when G_A is small ($G_A < 60$ for $G_S = 30$ and $G_A < 330$ for $G_S = 300$) and increases linearly as G_A increases. In summary, we conclude that by exploiting the leader position by committing the surveillance strategy and forcing the attacker as the follower, the defender significantly improves its utility with respect to playing a SSE strategy, hence obtains a better protection against selfish PUEAs.

Table 3.7 shows the average computation time (through the Monte-Carlo simulation) to determine the SSE point by using the MLP and the NE point by the sequence-form representation method. In these simulations, we assume that the attacker/defender can attack/monitor $M = L = 1$ channel at most. The results show that the MLP method

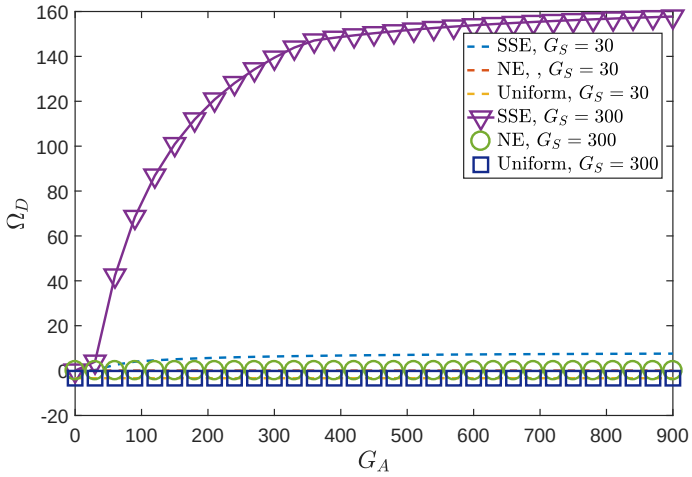


FIGURE 3.9 The expected payoff of the defender in three considered cases for $G_S = 30$ and $G_S = 300$ when the attacker conducts a selfish PUEA to attack the CR network.

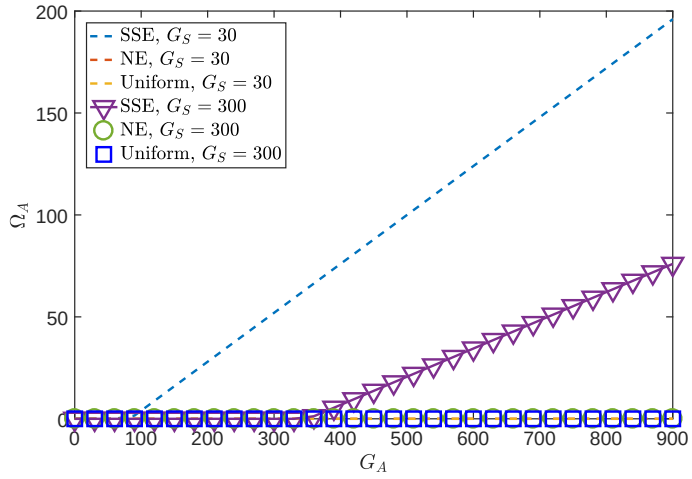


FIGURE 3.10 The expected payoff of the attacker in three considered cases for $G_S = 30$ and $G_S = 300$ when the attacker conducts a selfish PUEA to attack the CR network.

to determine the equilibrium point in the commitment model is much faster than the sequential representation method to determine the NE strategy in the non-commitment model. Consequently, the MLP method can provide the solution for a large game, which is infeasible by using the sequence-form representation method.

Figure 3.11 and 3.12 present the effectiveness of our proposed commitment model on reducing the number of collisions to PU due to PUEAs through the following simulation. We consider a CRN with $N = 3$ channels, where the attacker/defender can attack/monitor one channel at most, *i.e.*, $M = L = 1$. The common knowledge are the probability of PU activity at each channel $\pi_1 = 0.1$, $\pi_2 = 0.2$ and $\pi_3 = 0.3$, the probability of detection $P_d = 0.9$ and the probability of false alarm $P_f = 0.1$. A collision between the attacker and the PU happens

TABLE 3.7 The average computation time required to determine the equilibrium point in the non-commitment case (sequence-form representation method) and commitment case (MLP method).

	$N = 2$	$N = 4$	$N = 6$	$N = 8$	$N = 10$
Sequence-form	2s	11564s	>12h	–	–
MLP	0.17 s	7.8s	84.05s	20min	2h

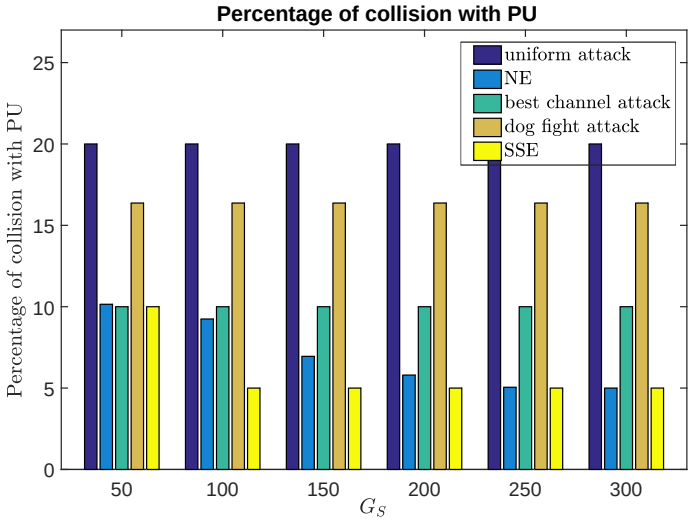


FIGURE 3.11 The percentage of collision with the primary user of the attacker for different values of G_S when the attacker conducts a selfish PUEA and $G_A = 100$.

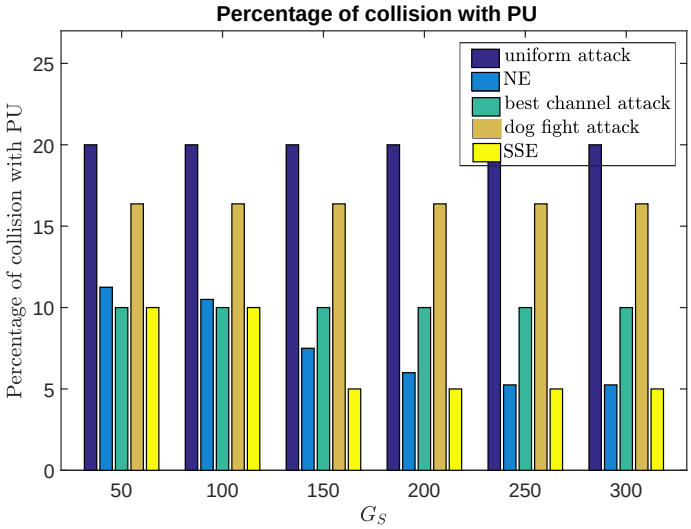


FIGURE 3.12 The percentage of collision with the primary user of the attacker for different values of G_S when the attacker conducts a selfish PUEA and $G_A = 300$.

if the sensing results show that an attacked channel, where the PU is actually transmitting, is occupied (then is used by the attacker). The Monte-Carlo simulations with 10^6 samples

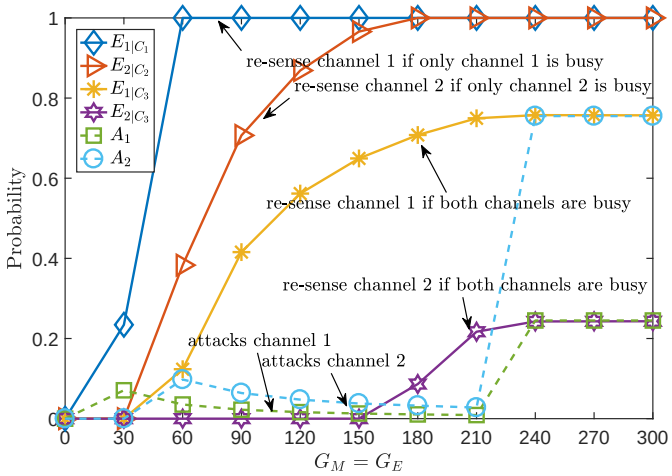


FIGURE 3.13 The NE strategy of the attacker and the defender when the attacker conducts a malicious PUEA.

is adopted to observe the collision between the attacker and the PU. Five scenarios are considered: i) the attacker follows its SSE strategy, ii) the attacker follows its NE strategy, iii) the attacker follows a uniform strategy (*i.e.*, the attack probability is the same for all channels), iv) the attacker conducts attack on the channel with the lowest probability of PU activity (*i.e.*, channel 1), and v) the attacker conducts attack as in the dog fight attack [51] (*i.e.*, the attacker attack channel t with a probability $\frac{1}{\pi_t}/\sum_{i=1}^{N}\frac{1}{\pi_i}$). From the simulation results, if the attacker follows the SSE strategy, the percentage of collision with primary users of the attacker is smallest. This conclusion confirms the added value of our proposed approach in order to mitigate the selfish PUEA in CRNs.

3.6.2 The Malicious Primary Emulated Attack

For the malicious PUEA, we also assume that the cost/gain for the attack and the surveillance process are equal in all channels. We start with a CR network with two channels ($N = 2$) in which the attacker can attack up to $M = 1$ channel and the defender can monitor up to $L = 1$ channel at a time. In general, the gain of attack (G_M^t) and the gain of extra-sensing (G_E^t) are equivalent to the benefit of obtaining the available channel. Thus, in order to simplify the problem, we assume that $G_M^t = G_E^t$. Other parameters are $P_A = 100$, $C_M = 10$, $C_E = 5$, $\pi_1 = 0.2$ and $\pi_2 = 0.5$.

Figure **??** presents the NE and the SSE strategy of the defender and the attacker in the non-commitment and the commitment case with various values of G_M, G_E, respectively. We observe that both strategies depend on the benefit of obtaining the available channels (*i.e.*, G_M, G_E). For the non-commitment case (Figure 3.13), if G_E, G_M are low, the attacker and the defender will give a low effort to implement the malicious PUEA and the extra-sensing process. In contrast, if G_E, G_M are high, the defender will re-sense the occupied-declared

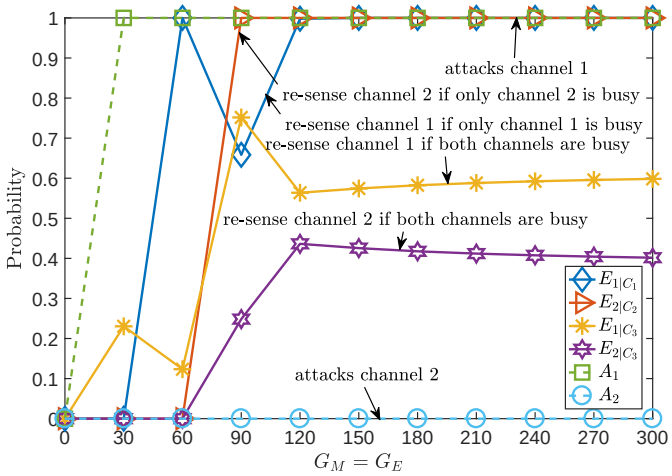


FIGURE 3.14 The SSE strategy of the attacker and the defender when the attacker conducts a malicious PUEA.

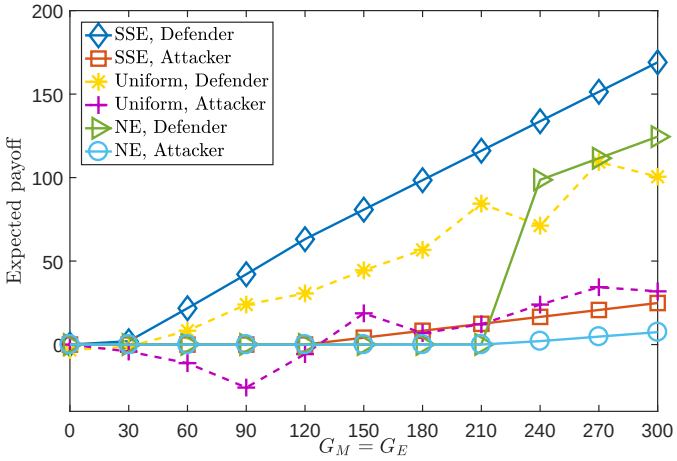


FIGURE 3.15 The expected payoffs of two players in the non-commitment and the commitment case when the attacker conducts a malicious PUEA.

channel if only one channel is busy. If both channels are busy, the defender will re-sense *channel* 1 with a higher probability. Similarly, for a high G_M, the attacker will perform the malicious PUEA in the channel 1 with a higher probability. In contrast, for the commitment case (Figure 3.14), the attacker will perform the malicious PUEA in the channel 1 in order to adapt to the extra-sensing strategy of the defender.

Figure 3.15 displays the expected payoffs of two players in: non-commitment, commitment and uniform cases. We observed that the expected payoffs of two players obtained with the SSE strategy are higher than the other ones with the NE (in the non-commitment case) and the uniform strategies. The reason is that there is no penalty for the attacker with the malicious PUEA, hence the attacker and the defender will choose the best response strategies

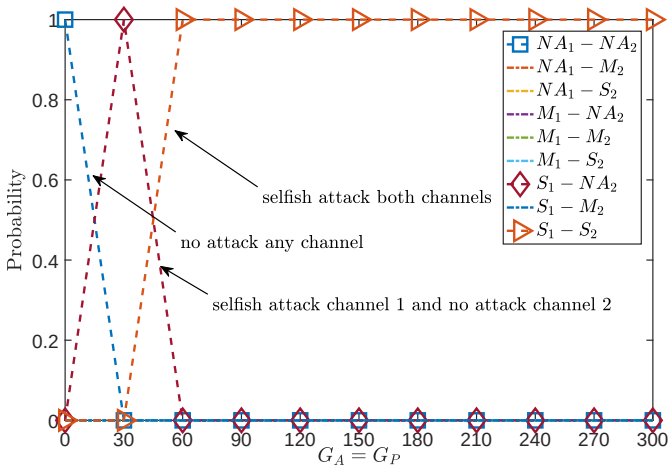


FIGURE 3.16 The SSE strategy of the attacker when the attacker conducts a general PUEA.

with higher expected payoffs by performing the SSE strategy. It means that, by employing the leader position by committing the extra-sensing strategy and forcing the attacker as the follower, the defender significantly improves its utility with respect to playing a NE strategy, hence obtains a better protection against the malicious PUEA.

3.6.3 The General Primary Emulated Attack

For the general PUEA, we also assume that the cost/gain for the attack and the surveillance process are equal in all channels. We start with a CR network with two channels ($N = 2$) in which the attacker can attack up to $M = 2$ channel and the defender can monitor up to $L = 1$ channel at a time. We suppose that the gain of attack and the gain of surveillance are equivalent to the benefit of obtaining the available channel, *i.e.*, $G_A^t = G_S^t$. Other parameters are $P_A = 100$, $C_A = 20$, $C_S = 10$, $\pi_1 = 0.2$ and $\pi_2 = 0.5$.

Figure 3.16 and 3.17 display the SSE strategy of the attacker and the defender in the commitment case with various values of G_A, G_S. We observed that the attacker will choose to implement the selfish PUEA on channel 1 or on both channels or not to implement the PUEA. The other actions, *e.g.*, the malicious attack on both channels, is not considered. The reason is that the attack and used the attacked channel if it is occupied-declared (*i.e.*, selfish PUEA) or not to attack any channels are the dominant strategies in that game. If the benefit of obtaining the available channel (*i.e.*, G_A^t, G_S^t) are small, the attacker will perform not to attack or selfish attack channel 1 and not to attack channel 2. If the benefit of obtaining the available channel is high, the attacker will perform selfish attack both channels. Similarly, if G_A^t, G_S^t are low, the defender will give a low effort to implement the surveillance process. However, if G_A^t, G_S^t are high, the defender will perform the surveillance process on the occupied-declared channel to force the attacker follows the strategy of the defender, hence mitigate the influence of the PUEA in the CR network.

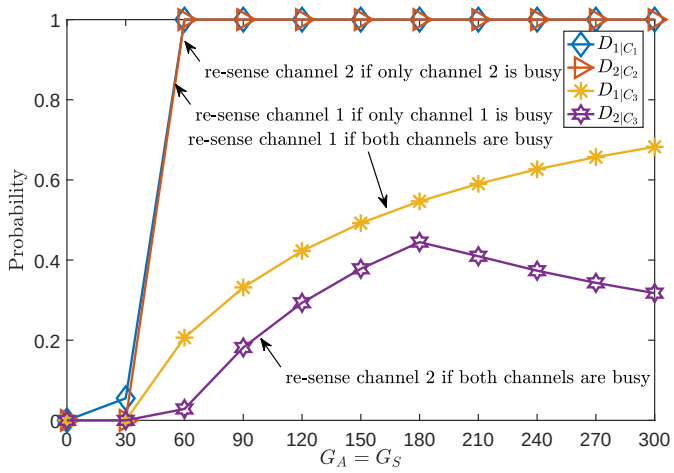


FIGURE 3.17 The SSE strategy of the defender when the attacker conducts a general PUEA.

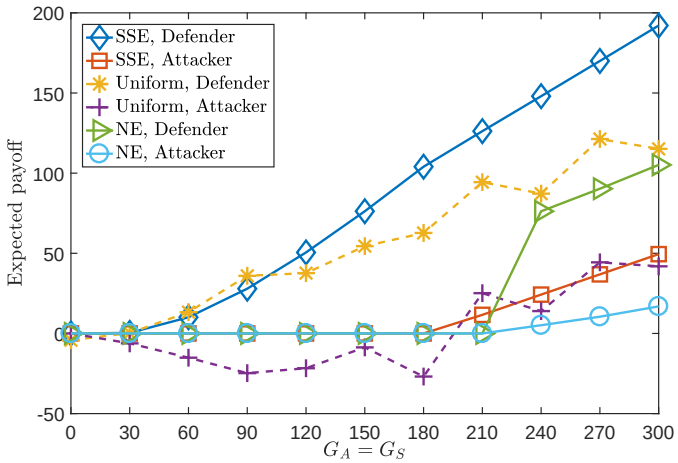


FIGURE 3.18 The expected payoffs of two players in the non-commitment and the commitment case when the attacker conducts a general PUEA.

Figure 3.18 presents the comparison in term of the expected payoff of the attacker and defender by performing the SSE, the NE, and the uniform strategy, respectively. We observe that the expected payoff of the attacker and the defender obtained with the SSE strategy outperform the ones with the NE strategy and the uniform strategy. We conclude that for the general PUEA, by exploiting the leader position in the game by committing to a surveillance strategy and forcing the attacker to act as the follower by playing the best response regarding the observed surveillance strategy, the network coordinator significantly improves its utility with respect to playing the other strategies, hence obtains a better protection against PUEAs.

3.7 Concluding Remarks

This chapter studied the surveillance process to mitigate the influence of the misbehaving user in the spectrum-sensing based CR networks. Due to the nature of the spectrum sensing-based CR systems, a misbehaving user can emit the emulated primary user signal for ruining the operation of the network, for occupying more channels for selfish purpose or for both purposes. Depends on the behavior of the PUEA attacker, selfish, malicious, or general PUEA, the corresponding surveillance process is proposed. By adopting the game theory framework, the relationship between the PUEA attacker and the surveillance process is analyzed in the multi-channel PUEA scenario. Through appropriate modeling of the strategic interaction between the network coordinator and the attacker, we formulate the commitment game in which the network coordinator takes the lead by committing to a surveillance strategy. To maximize the expected payoff, the rational attacker is forced to become a follower responding to the strategy used by the network coordinator. Relevant strategies of the surveillance process are invested through the SSE. Analytical and numerical results show that the defender's expected payoff is significantly improved when the defender commits to a surveillance strategy. Moreover, the computation time required to find the equilibrium point is lower in the commitment case than in the non-commitment case. We conclude that the defender should exploit the leader position in the game by committing to a defense strategy.

Chapter 4

Self-Coexistence in Database Driven-based CR Networks: Surveillance Strategy for Spoofing Attacks

4.1 Introduction

In Chapter 3, we investigated the surveillance process to mitigate the selfish and malicious PUE attack in the spectrum-sensing based CR networks with centralized infrastructure. In this chapter, we consider the mitigation methods to deal with the spoofing attack in the database-driven based CR networks. In cognitive radio, secondary users must be able to adapt their transmission parameters to exploit the spectrum utilities. Determining accurate and reliable spectrum opportunities is, therefore, essential and still a very challenging problem. In the spectrum sensing-based method, primary system's activity is explored by measuring the radio environment spectrum. However, the rapid change and complexity of radio propagation environment due to shadowing and fading bring in too many uncertainties, leading to low sensing accuracy [24]. Therefore, the geo-location database-driven based approach is proposed to ensure the coexistence between primary systems and secondary systems [25]. In the database driven-based CR networks, a network coordinator, which is essentially a database server, is responsible for managing the spectrum allocation to secondary networks according to the cognitive user's location and an online geo-location map of spectrum usage. Whenever a secondary user demands to use spectrum, it will send to the resource coordinator a request which contains its' location information. The spectrum coordinator optimizes the allocation as well as the corresponding transmission parameters of the available spectrum bands and

The materials presented in Chapter 4 have been submitted to the IET Communications [95].

provides the detailed configuration to the requester. Compared to the spectrum sensing based approach, the database driven-based approach is more accurate and reliable [25]. Therefore, in 2012, FCC enforces to adopt the database driven-based approach for implementing the secondary accessing in the TV White Space and the 3.5 GHz CR systems [26].

The key point for implementing the geo-location database driven-based approach is the availability and the accuracy of the information of SU's location. Considerable interference on both primary and secondary systems will appear if the location information of the users is inaccurate. Moreover, unfair spectrum allocation will happen if adversaries intentionally spoof request messages with either faked identification (ID) or faked location information. Therefore, spoofing attack is a critical vulnerability of the GDB driven-based DSA system. However, to the best of our knowledge, there is no work systematically examining the impacts of spoofing attacks in database driven-based CRBs. The most relevant related work which considers the GPS spoofing attacks in a database-driven cognitive radio (CR) network is presented in [17] but limited due to the impact of false localization from the attacked GPS signals. Other studies on the security problem in database-driven systems mostly focus on location privacy [18, 28, 29] or the incumbent system privacy issues [30] by proposing an encryption technique to protect sensitive incumbents' operational privacy without affecting database's accessibility and spectrum utilization efficiency.

Different from the studies in [17, 18, 28–30], this chapter investigates a general view of spoofing attack in the database driven-based CR networks. Specifically, we consider the spoofing attacks, which occur in the ID and the location information of the cognitive user's request messages. Based on the behaving of the attacker, we classify the request messages consisting of spoofing information into accidental, malicious and selfish categories. An *accidental spoofing request* occurs when the sender is not aware of the incorrectness of its location information due to either a malfunctioning or an attacking problem (similar to [17]). A *malicious spoofing request* comes when the sender intentionally provides false location information for causing more interference to the whole system. Finally, a *selfish spoofing request* appears when the sender abusively queries for more spectrum resources under faked ID. In order to counteract these spoofing attacks, we then consider two surveillance processes corresponding to the ID and the location information in the request messages and investigate the key question on when to implement the above surveillance processes.

Under the identification spoofing attack, the attacker uses a faked ID for registering and querying for spectrum. It is similar to the case of the TCP/IP or the VoIP, where the attacker can forge ID information and present false names and numbers [59, 60] due to the lack of a mechanism for authenticating the source or destination of a message. The consideration in this chapter is to proposed a data traffic identification process, which allows us to detect the ID spoofing attack in the database driven-based CR network. In order to investigate the traffic identification process, we first formulate the problem as an extensive form game. This

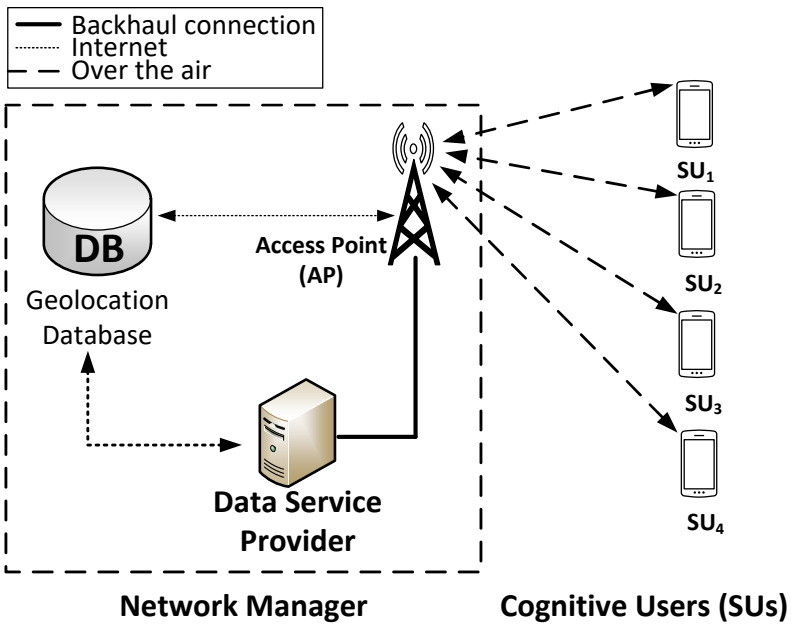


FIGURE 4.1 Example of database driven-based CR networks.

formulation allows us to investigate the surveillance strategies for detecting spoofing attacks through studying the existence and the computation of the game's NE.

Under the location spoofing attack, the attacker uses a faked location for registering and querying for spectrum. Consequently, such kind of attack can reduce spectrum resource opportunity at a specific location. Thus, our focus is on proposing a location verification process to detect the location spoofing attack. The verification strategy is investigated through the corresponding NE of the location verification game. We first present the NE of the game in a closed-form and show that the network coordinator can enforce attacker to reduce the number of spoofing attacks by performing surveillance processes according to NE at an appropriate penalty.

4.2 System Model

4.2.1 Database Driven-based Cognitive Radio Systems

We consider a database driven-based cognitive radio network which provides the wireless access services to the cognitive radio users in the incumbent spectrum bands, such as the IEEE 802.19.1 standard-based CR networks [58] or the IEEE 802.11 af standard-based CR networks [9] in TV White Space. In such a network, the spectrum accesses are performed by using geo-location awareness and maintaining information databases from cognitive user to establish the geo-location map of spectrum usage. Generally, the considered system consists two separating sets: the network coordinator set which are entities being responsible

to manage the accesses to the spectrum bands and the cognitive user set which are users exploiting the service of the network coordinator set. To control the spectrum assesses, the network coordinator is responsible for i.) collecting spectrum usage information of the primary networks and the CR networks to establish a geo-location map of spectrum usage, ii.) gathering registrations, geo-location information and requests for accessing of SUs, iii.) managing and allocating spectrum bands and the transmitting configurations to SUs, and iv.) monitoring and controlling to ensure the correctness of the system operation. In contrast, each cognitive user queries the network coordinator with its current location to retrieve the spectrum allocation. It means each cognitive user must be a location awareness device, *i.e.*, a fixed device which is location-aware or a portable device which has an internal geo-location capability. After receiving SUs' requests, the network coordinator will optimize and assign the spectrum bands and the corresponding transmitting configurations for SUs. In this chapter, we aim at a database driven-based CR network, which supports mobile SUs. Therefore, the registering, location updating and spectrum band querying requests are performed frequently through wireless connections. In summary, the model of database driven-based cognitive radio systems is illustrated in Figure 4.1.

4.2.2 Spoofing Attacks

In the database driven-based CR network, a cognitive user must send a request to the network coordinator in order to register for operation or to update new location or to query for spectrum bands. Usually, the request messages contain the physical ID, such as the media access control address, and the geolocation of the user. The general format for a request message is presented in Figure 4.2.

Due to the flexibility of the software-defined radio, either ID or location information could be spoofed by the misbehaving user. For example, the attacker can use the fake location to require the spectrum access for data transmission or to ruin the network operation. In addition, the attacker can spoof the ID (*i.e.*, by using a fake ID or using the ID of other users) to attack the network. According to spoofed contents, we categorize the spoofing requests into five types as follows.

— *Type 1: Attacker's ID and wrong location*
The spoofing request type 1 occurs when a user has a localizing malfunction or suffers from an outside adversary localizing attack, *e.g.*, the spoofing attack on GPS signals [17]. In these cases, it is an *accidental spoofing request*. The spoofing request type 1 also appears when an adversary wants to reduce the probability of receiving spectrum allocation at the attacked location. In this case, it belongs to the *malicious spoofing request* category. Otherwise, if the spoofing request type 1 comes when a registered user intentionally queries spectrum bands at a specific location for using in future, it is a *selfish attacking request.*

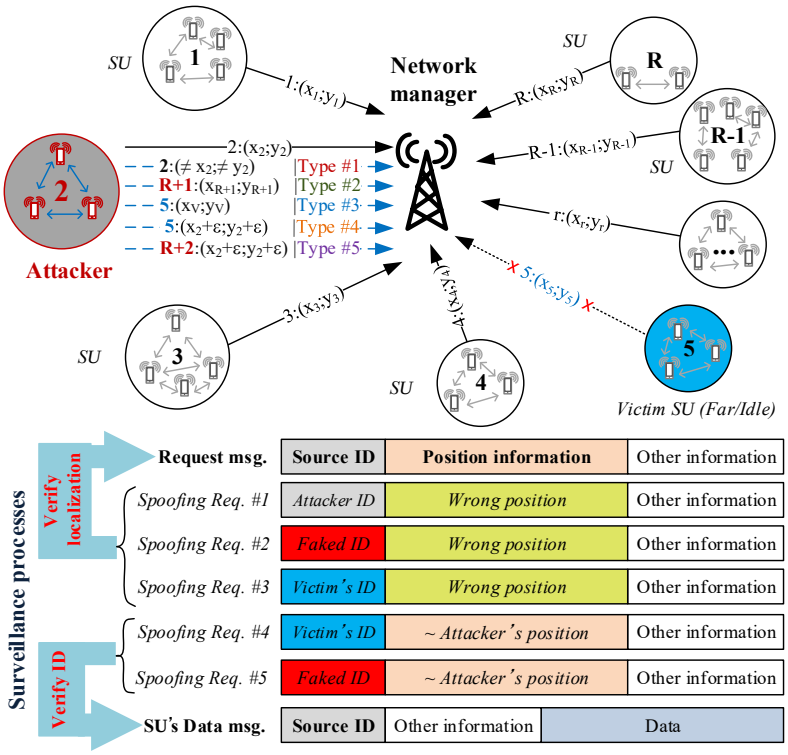


FIGURE 4.2 Types of spoofing attack in database driven-based cognitive radio networks.

— *Type 2: Faked ID and wrong location*

The spoofing request type 2 occurs when an adversary spoofs a registration for a new ID at an arbitrary location. Thus, similar to the spoofing request type 1, this request type can be used for reducing spectrum resource opportunity at a specific location, and we call it a *malicious attacking request*. In addition, an adversary also uses this type of attack for illegally occupying spectrum resource if the wrong location is close to its real location. In this case, we call it a *selfish attacking request*.

— *Type 3: Victim's ID and wrong location*

The spoofing request type 3 occurs when an attacker overlaps and replaces the request of a victim by a spoofed location one. If the victim is a far user, updating the wrong location can cause strong interference. Hence it is *maliciously attacked request*. Otherwise, if the victim is a neighbor of an attacker, spoofing an updating request with the wrong location can virtually move the position of the victim in the database to a position outside the area of the attacker. Such an attack hence increases the spectrum opportunity for the attacker. So we call it a *selfishly attacking request*. However, this spoofing could be detected by the victim rapidly.

— *Type 4: Victim's ID and attacker's location*

The spoofing request type 4 occurs in the same way as the type 3. However, in this type, the attacker aims at thieving spectrum resource of a victim user who can be

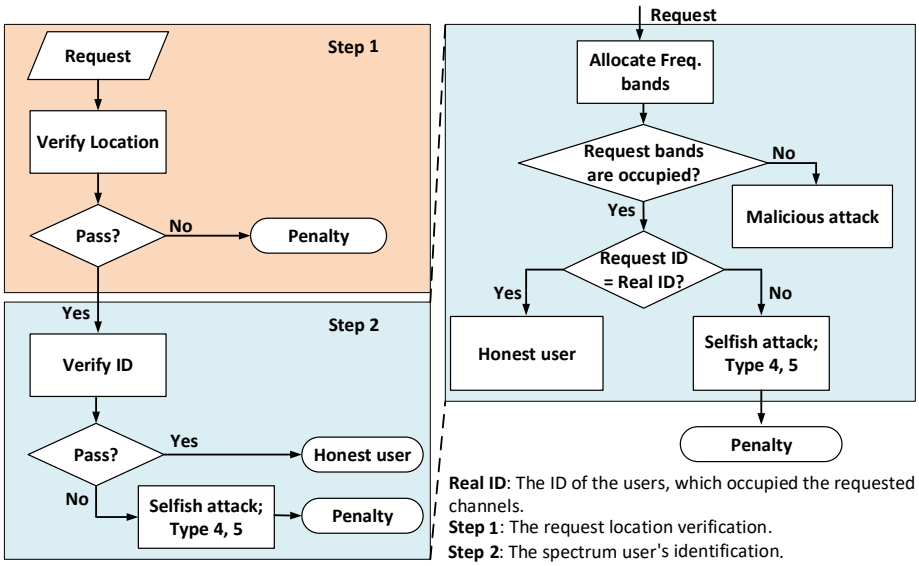


FIGURE 4.3 The 2-steps verification process to deal with the location and ID spoofing attacks on the GDB spectrum sharing system.

either a far (outside the area of the attacker) or an idle (inactive) user. By using the ID of a victim to query for a spectrum band at the location of the attacker, the attacker steals the spectrum resource for its use. Therefore, it is a *selfishly attacking request*.

— *Type 5: Faked ID and attacker's location*
The spoofing request type 5 is employed for increasing spectrum resource opportunity at the located area of the attacker. Using faked IDs, registering and querying for spectrum bands could help the attacker occupy more resources. Hence, the spoofing type 5 is a *selfishly attacking request*.

4.2.3 Verification Processes

Based on the variety of purposes and contents of spoofing request, there are possibly several mitigation methods to deal with the spoofing attacks. In order to systematize these methods, we remark that a spoofing attack only locates at the location or the ID information of the request message. Consequently, by performing a surveillance process to verify the location or the ID of the cognitive user who sends the request, the network coordinator can detect the wrong location or the illegal occupation. Therefore, we propose a surveillance process which includes two complementing steps: the *request location verification* and the *spectrum user's identification* to deal with the location and ID spoofing attacks, respectively (Fig. 4.3). The 2-steps verification process is issued in details as follows:

— **Request location verification**: for the location spoofing attack, we propose to implement a location verification process. Positioning methods based on receive signal

strength, time of arrival, added sensor networks, etc., can be used to determine the deriving position of the request. If there is a mismatch between the estimated location and the location information in the request message, the location spoofing attack is detected. The request will be ignored and a further penalty is imposed on the attacker. In practice, because of the variation of radio environment and the characteristic of positioning methods, there is always a limitation on localization accuracy. Hence, the efficiency of this surveillance step is limited to a distance, called an *undetectable radius*. Any difference distance between the real position and the location information in the request smaller than the undetectable radius cannot be discovered.

— **Spectrum user's identification**: in order to provide complementing counteractions for the above step, we propose to perform a second surveillance process. The extra surveillance at a small area inside an undetectable radius is conducted by scanning allocated spectrum bands to determine who is using the resource. The reason is that the user must reveal it physical ID to transmit its own data through any communication links. If the spectrum bands are not occupied, then the attack is malicious and the frequency resource is rearranged for other requests. If the spectrum bands are occupied by mismatching users, the selfishly spoofing attack (*i.e.*, type 4 and 5), therefore, can be detected and punished accordingly.

Due to the trade-off between the gain and the loss of the attacker and the network coordinator, game theory, which mathematically studies the interaction among independent, self-interested players, helps to formulate our problem. In the next two sections, we formulate two surveillance games that describe the interaction of the two surveillance methods with attacking strategies.

4.3 Request Location Verification Strategies

In the database driven-based CR network, each cognitive user sends the request messages to the network coordinator over the wireless connections. Hence, it is possible to localize sending locations of requests, and uses the estimated location to verify the request is location spoofing (*i.e.*, type 1, 2 and 3) or not by comparing it with the location information in the request message. Since the number of active SUs and their locations can be recorded in the history data, we assume that it is a common knowledge, which can be accessed by both the network manager and attacker. The attacker then can send multiple requests to implement the location spoofing. Similarly, the network coordinator can perform multiple verification processes. The question here is that, for both the attacker and the network coordinator, what is the optimal number of attacking requests and verification processes?

4.3.1 Game formulation

To analyze the interaction between the location verification process and the location spoofing, we formulate a 2-players game between a defender and an attacker as follows.

Players

— **Attacker**, who also is a cognitive user, implement the location spoofing attack by sending up to N location spoofing requests.
— **Defender**, who represents the network coordinator, can perform surveillance up to M locations/request slots (depending on the supporting infrastructure).

Strategies

Let A be the pure strategy set of the attacker. Then, A is defined by

$$A = \{n, n = 0, 1, ..., N\}, \tag{4.1}$$

where n denotes the number of spoofing attacks. If $n = 0$, the attacker does not perform to attack the CR network.

Similarly, let D be the pure strategy set of the defender. Then, D is defined by

$$D = \{m, m = 0, 1, ..., M\}, \tag{4.2}$$

where m denotes the number of verification. If $m = 0$, the defender does not perform to defend the CR network.

Payoffs

Let r denote the number of active SUs in the verified area. For each pair of (m, n) given r, the corresponding payoff of the attacker Π^A and the defender Π^D are calculated by:

$$\Pi^A_{m,n,r} = n\,(G - C_A) - \pi_{m,n,r} \tag{4.3a}$$
$$\Pi^D_{m,n,r} = -mC_S + \pi_{m,n,r} \tag{4.3b}$$

where G is the benefit of using an allocated band, C_S and C_A are the costs of implementing the surveillance process and the spoofing attack on one band, and $\pi_{m,n,r}$ represents the expected penalty.

In practice, instead of keeping one pure strategy, attacker and defender could choose their strategy randomly. This forms a mixed strategy for each player. The mixed strategy sets of the attacker and defender are defined by $\{\alpha_n\}$ and $\{\delta_m\}$ where α_n and δ_m are the probabilities of spoofing n users and monitoring m locations. The game between the spoofing

attacker and the defender is now equivalent to a strategic bi-matrix form game with size $N \times M$ as shown in Table 4.1.

TABLE 4.1 Strategic bi-matrix game

		Defender			
		0	***1***	...	***M***
Attacker	***0***	$\left[\Pi^A_{0,0,r}, \Pi^D_{0,0,r}\right]$	$\left[\Pi^A_{1,0,r}, \Pi^D_{1,0,r}\right]$	...	$\left[\Pi^A_{M,0,r}, \Pi^D_{M,0,r}\right]$
	1	$\left[\Pi^A_{0,1,r}, \Pi^D_{0,1,r}\right]$	$\left[\Pi^A_{1,1,r}, \Pi^D_{1,1,r}\right]$	...	$\left[\Pi^A_{M,1,r}, \Pi^D_{M,1,r}\right]$
	...	...	...	...	...
	N	$\left[\Pi^A_{0,N,r}, \Pi^D_{0,N,r}\right]$	$\left[\Pi^A_{1,N,r}, \Pi^D_{1,N,r}\right]$	...	$\left[\Pi^A_{M,N,r}, \Pi^D_{M,N,r}\right]$

The expected payoffs of players are given by:

$$U_A = \boldsymbol{\alpha}^T \boldsymbol{\Pi}_A \boldsymbol{\delta} = \sum_n \alpha_n U_{A|n} = \sum_n \alpha_n \left(\sum_m \delta_m \Pi^A_{m,n,r} \right) \tag{4.4a}$$

$$U_D = \boldsymbol{\alpha}^T \boldsymbol{\Pi}_D \boldsymbol{\delta} = \sum_m \delta_m U_{D|m} = \sum_m \delta_m \left(\sum_n \alpha_n \Pi^D_{m,n,r} \right) \tag{4.4b}$$

Obviously, the attacker's payoffs depend not only on its own strategy but also on the defender's strategy, and vice versa. The presence and interaction of the defender strongly affect the selection of the attacker to optimize its outcome. In turn, the adjustment of the attacker's strategies leads to the corresponding reaction of the defender's ones. The reasoning of these interactions introduces the equilibrium point which is the intersection of both best response functions of the players. Therefore, NE of the game will be investigated in the next subsection. Also, since the main impact of the network coordinator on the attackers is the punishment for the captured spoofing attack, penalty policies will be considered as well.

4.3.2 Penalty policy and Nash equilibrium

Penalty policy

After performing location verification process for a request message, if there is a mismatch between the (estimated) localized position of the sender and the indicated location of the request message, the defender then considers the request as a spoofing one and ignore it. A further penalty time P, called the location-based penalty, that is a ban on spectrum resource allocation for a penalty time P is imposed to the localized area of the spoofing request. Authentication steps could be run at this penalty time to confirm the existence of real SU and remove all possible virtual or victim SU.

For the location-based penalty, apparently, the defender always ensures that the attacker sending the detected spoofing request must be suffered from a punishment regardless its attack in type 1, or type 2, or type 3. Since there are many possibilities to consider a request

message as a spoofing one, selecting penalty policies is an issue. A request message in the spoofing type 1, shown in Figure 4.2, could derive from attackers who want either to get the spectrum of vicinity area or to let down the operation of SUs at the attacked position, but it could be generated by a positioning-malfunction user as well. We can impose a penalty P in this case because, with either the intentionally attacking purpose or the accidentally malfunctioning problem, the issue is quite serious and can affect the operation of the network. Unfortunately, since an attacker could generate several spoofing requests with different IDs (type 2 and type 3) at one requesting period, it is difficult to distinguish between spoofing IDs and honest IDs. In such a case, the network coordinator should enforce a penalty time P in the localized area deriving spoofing requests instead. This punishment will not affect other normal SUs located inside the area if they have a legal request with good historical records on their compliance with the previous spectrum allocations (*i.e.*, they have requests with registered IDs and matched location information.). Generally, the defender can select to impose a banning spectrum allocation time which is either a *constant penalty* (*i.e.*, a fixed P) or a *captured amount-related penalty* (*i.e.*, a kP, where k is the number of detected spoofing messages) for a detected area regardless the amount of the detected spoofing requests. However, since the other normal SUs located inside the penalized area would be affected, the penalty should not be too large. Therefore, for the location verification process, we propose to use a *constant penalty* for a detected area regardless the amount of the detected spoofing requests.

In order to determine the expected penalty $\pi_{m,n,r}$, we define $\gamma^{(k)}_{m,r,r}$ the probability of k detected spoofing messages $\left(0 \leq k \leq \min(m,n)\right)$ over n attacks. Since the number of combinations for monitoring m requests is $\begin{pmatrix} n+r \\ m \end{pmatrix}$, and the number of having k spoofing attacks in m surveillances is $\begin{pmatrix} n \\ k \end{pmatrix}\begin{pmatrix} r \\ m-k \end{pmatrix}$ for $r \geq m-k$, we have

$$\gamma^{(k)}_{m,n,r} = \begin{cases} 0, & \text{if } m = 0 \\ 1, & \text{if } m > r+k \\ \begin{pmatrix} n \\ k \end{pmatrix}\begin{pmatrix} r \\ m-k \end{pmatrix} \Big/ \begin{pmatrix} n+r \\ m \end{pmatrix}, & \text{otherwise} \end{cases} \tag{4.5}$$

The probability of capturing at least one attack is the complement of the probability of capturing nothing, *i.e.*, $1 - \gamma^{(0)}_{m,n,r}$. Since the constant penalty when capturing spoofing attacks is P and the amount-related penalty when capturing k attack is kP, the expected penalty is then given by:

$$\pi_{m,n,r} = \begin{cases} P\left(1 - \gamma^{(0)}_{m,n,r}\right), & \text{constant pentalty} \\ P \sum\limits_{k=1}^{\min(m,n)} k\gamma^{(k)}_{m,n,r}, & \text{amount-related penalty} \end{cases} \tag{4.6}$$

Nash Equilibrium

In order to find a solution for the best strategy of the attacker and the defender in such a game, we explore NE in which each player has selected the best response to opponents' strategies, and no player gains anything by solely changing their own strategy. The NE of the formulated game (α_n^*, δ_m^*), therefore, must satisfy the following conditions:

$$\begin{cases} U_A\left(\alpha_n^*, \delta_m^*\right) \geq U_A\left(\alpha_n, \delta_m^*\right) \\ U_D\left(\alpha_n^*, \delta_m^*\right) \geq U_D\left(\alpha_n^*, \delta_m\right) \end{cases} \tag{4.7}$$

And, the problem of finding NE is equivalent to a bi-optimization problem as follows.

$$\begin{array}{ll} \underset{\boldsymbol{\alpha}}{\text{maximize}} & \boldsymbol{\alpha}^T \boldsymbol{\Pi}_A \boldsymbol{\delta} \\ \underset{\boldsymbol{\delta}}{\text{maximize}} & \boldsymbol{\alpha}^T \boldsymbol{\Pi}_D \boldsymbol{\delta} \\ \text{subject to} & \mathbf{1}^T \boldsymbol{\alpha} = 1, \boldsymbol{\alpha} \geq 0 \\ & \mathbf{1}^T \boldsymbol{\delta} = 1, \boldsymbol{\delta} \geq 0 \end{array} \tag{4.8}$$

The optimization problem given in (4.8) can be solved by using the Lemke-Howson algorithm [86].

Proposition 4.1. *For constant penalty case, attacker only selects its attacking strategies from the two numbers of attack 0 and N.*

Proof. For constant penalty case, from (4.3a), (4.4a) and (4.6), the expected payoff of attacker corresponding to each selected number of attacks n is calculated by:

$$U_{A|n} = \sum_m \delta_m \Pi_{m,n,r}^A = \sum_m \delta_m \left[n\left(G - C_A\right) - \left(1 - \gamma_{m,n,r}^{(0)}\right) P \right] \tag{4.9}$$

Then, the second derivative $U_{A|n}$ is determined by

$$\Delta\Big(\Delta U_{A|n}\Big)_{|n} = \Delta U_{A|n+1} - \Delta U_{A|n} = \frac{P \sum\limits_m \delta_m \left(m^2 + m\right) \gamma_{m,n,r}^{(0)}}{\left(n + r + 1\right)\left(n + r + 2\right)} \tag{4.10}$$

where $\Delta F_{|n} = F_{|n+1} - F_{|n}$ denotes the derivative of a discrete function $F_{|n}$ of variable n. Since $\Delta\Big(\Delta U_{A|n}\Big)_{|n} \geq 0, \forall m$, $U_{A|n}$ is a convex function of n regardless m, and hence,

$$U_{A|n} \leq \left(1 - \frac{n}{N}\right) U_{A|0} + \frac{n}{N} U_{A|N}, \forall m \text{ and } 0 < n < N.$$

In the other word, the strategy n, $0 < n < N$, is dominated by either the strategy 0 or the strategy N. □

Corollary 4.2. *For constant penalty case, the formulated game given in Table 4.1 is equivalent to the $2 \times M$ bi-matrix game where attacker has only two strategies: not attack and attack with the full capacity of N spoofing requests.*

Proposition 4.3. *For constant penalty case,*

(i) $\exists\, m_{\max} \leq r : U_{D|m_{\max}} \geq U_{D|m}, \forall m > m_{\max}$.

(ii) $m_{\max}$ *is upper-bounded by*

$$m_0 = \max \left\{ \arg\max_m \left(\Pi^D_{m,n,r} \right) \right\}_{n=0}^{N} \tag{4.11}$$

(iii) the formulated game given in Table 4.1 reduces to a $2 \times (m_0 + 1)$ *bi-matrix game.*

Proof. (i) From (4.3b), (4.4b) and (4.6), the expected payoff of defender verifying m request in constant penalty case is computed by:

$$U_{D|m} = \sum_n \alpha_n \Pi^D_{m,n,r} = \sum_n \alpha_n \left(-mC_S + \left(1 - \gamma^{(0)}_{m,n,r} \right) P \right) \tag{4.12}$$

From (4.5), we have $\gamma^{(0)}_{m,n,r} = 0$ when $m > r$. Thus,

$$U_{D|r} \geq U_{D|m}, \forall m > r$$

This means that the feasible value of $m_{\max}$ is in $[0, r]$. Besides, the second derivative of $U_{D|m}$ is calculated by:

$$\begin{aligned} \Delta\Big(\Delta U_{D|m}\Big)_{|m} &= \Delta U_{D|m+1} - \Delta U_{D|n} \\ &= -P \sum_n \alpha_n \frac{n\,(n-1)\,\gamma^{(0)}_{m,n,r}}{(n+r-m-1)\,(n+r-m)} \end{aligned} \tag{4.13}$$

Obviously, $\Delta\Big(\Delta U_{D|m}\Big)_{|m} \leq 0$ for $0 \leq m \leq r$. Thus, $U_{D|m}$ is a concave function of m in $[0, r]$. This means $\exists\, m_{\max} \leq r$ so that $U_{D|m_{\max}} \geq U_{D|m}, \forall m > m_{\max}$.
(ii) One can easily check that $\Delta\Big(\Delta(\Pi^D_{m,n=k,r})_{|m}\Big)_{|m} \leq 0$, $\forall 0 \leq k \leq N$ and $0 \leq m \leq r$. Hence, $\Pi^D_{m,n=k,r}$ is a concave function of m in $[0, r]$, $\forall 0 \leq k \leq N$. This means

$$\Pi^D_{m_0,n=k,r} \geq \Pi^D_{m,n=k,r}, \text{ or } U_{D|m_0} \geq U_{D|m}, \forall m \geq m_0.$$

(iii), One can easily check from (ii) that the formulated game (Table 4.1) reduces to a $2 \times (m_0 + 1)$ bi-matrix game. □

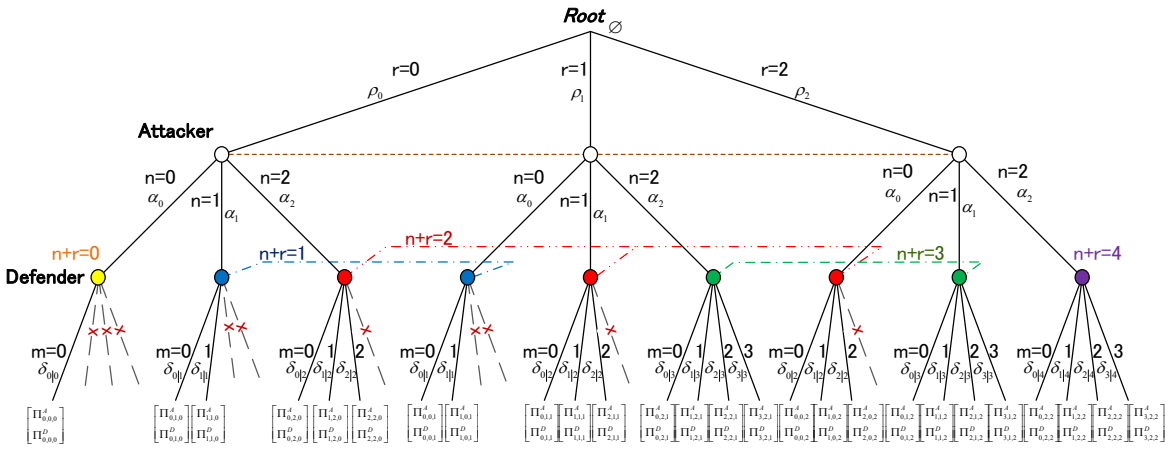


FIGURE 4.4 The identification surveillance game for mitigating spoofing attack when $N = 2, M = 3$ and $R = 2$.

4.4 Data Traffic Identification Strategies

If the request passes the location verification step, the network coordinator then allocates the spectrum resource for the user. However, the ID spoofing attacks and even the location spoofing attacks could pass through due to the imperfect localization. Therefore, it is necessary to conduct a further surveillance process to verify if the allocated spectrum resource is used by the right/registered SU or not. The proposed ID verification can be considered as an appropriate complement for the request location verification process. Similarly to, the location spoofing, the attacker can send multiple requests to implement the ID spoofing while the network coordinator can perform multiple verification processes. The question here is that, for both the attacker and the network coordinator, what is the optimal number of attacking requests and verification processes?

4.4.1 Game formulation

We formulate a non-cooperative extensive-form game to analyze the interaction between the ID spoofing attack and the ID surveillance process as follows.

Players

— **Attacker**, who also is a cognitive user, implement the ID spoofing attack by sending up to N ID spoofing requests.

— **Defender**, who represents the network coordinator, can perform ID verification process to detect the ID spoofing attack.

Strategies

— **Step 1**: the attacker performs the ID spoofing attack by sending n, $0 \leq n \leq N$ spoofing requests in either type 4 or type 5 for getting more spectrum resource, where N denotes the maximum spoofing attack capability.
— **Step 2**: The defender allocates $n+r$ spectrum bands for n requests from the attacker and r requests from honest users.
— **Step 3**: The defender scans m, $0 \leq m \leq \min(M, n+r)$ allocated spectrum bands to detect the spoofing attack and then penalize the attacker, where M represents the maximum surveillance capability.

In such a case, the attacker sends n ID spoofing requests without knowing the true value of r, while the defender scans m spectrum bands with the knowledge of the total allocated spectrum bands $n+r$. Hence, the pure behavioral strategy set of the attacker is defined by

$$\mathbf{S}_A = \{n, 0 \leq n \leq N\},$$

and the pure behavioral strategy set of the defender depending on $n+r$ is given by

$$\mathbf{S}_{D|n+r} = \{m|(n+r), 0 \leq m \leq \min(M, n+r)\}.$$

The corresponding mixed strategy sets of the attacker and the defender is defined by: $\boldsymbol{\alpha} = \{\alpha_n, 0 \leq n \leq N\}$ and $\boldsymbol{\delta}_{|n+r} = \{\delta_{m|n+r}, 0 \leq m \leq \min(M, n+r)\}$ where α_n is the probability of spoofing n requests and $\delta_{m|n+r}$ is the probability of monitoring m spectrum bands given that $n+r$ requests have been allocated.

Payoffs

Since both the attacker and the defender could have the historical records of the amount of the real SUs located in the attacked area, we assume that the distribution of the real requests number r is a common knowledge. Without loss of generality, we assume that r follows Poisson distribution. The probability mass function (pmf) of r is given by:

$$f_{\Re}(r, \lambda) = \frac{\lambda^r e^{-\lambda}}{r!}, \tag{4.14}$$

where λ is Poisson distribution parameter, which equals to the mean value of r. To simplify the game, we assume that r is truncated by a maximum value R where $Pr[r \leq R] \geq \theta$ (θ denotes a probability threshold, *e.g.*, $\theta = 0.99$). This assumption is acceptable because the game is formulated for a small area where the difference in locations of SUs is undetectable by the request senders' locations verification process (Section 4.3), and hence the number of

SUs could be limited. Then the probability of r is given by normalizing $f_R(r, \lambda)$ as follows.

$$\rho_r = \frac{f_{\Re}(r, \lambda)}{\sum_{r=0}^{R} f_{\Re}(r, \lambda)} \tag{4.15}$$

For providing a clear example, we depict the formulated game in a tree form when $M = 3$, $N = 2$ and $R = 2$ in Figure 4.4. It can be seen that, at each terminal node, *i.e.*, the leaf of the game tree corresponding to a certain set of m, n and r, there is a pair of payoffs for both attacker and defender $\left[\Pi^A_{m,n,r}, \Pi^D_{m,n,r}\right]$ which are calculated as similarly as (4.3a) and (4.3b). Notice that the expected penalty $\pi_{m,n,r}$ is also calculated by (4.6) for either constant or amount-related penalty policy.

In principle, the formulated game can be converted to a strategic-form game by adopting Harsanyi transformation [78]. This means the pure strategy set of defender can be built upon the combinations of all possible conditional pure strategy sets, *i.e.*, $\mathbf{S}_D = \mathbf{S}_{D|0} \times \mathbf{S}_{D|1} \times \cdots \times \mathbf{S}_{D|n+r} \times \cdots \times \mathbf{S}_{D|N+R}$. However the number of the elements of $\mathbf{S}_D$ increases exponentially with M, N, and R ($|\mathbf{S}_D| = M!(M+1)^{N+R-M+1}$). For example, $|\mathbf{S}_D| = 96$ with $M = 3$, $N = 2$ and $R = 2$ (Figure 4.4), but $|\mathbf{S}_D| = 24576$ with $M = 3$, $N = 2$ and $R = 6$. Therefore, it is too complicated to solve the game by Harsanyi transformation. Instead, we use the sequence-from representation approach [76] to express the formulated game.

4.4.2 Sequence-form representation and Nash equilibrium

In game theory, an extensive game can be represented through the sequence-form representation by following the tree-form of the game. Such kind of representation is similar to the strategic-form one except that pure strategies are replaced by sequence actions of players, but with the smaller strategy set [79, 89]. In general, a player with perfect recall has the same sequence σ_u of choices at all nodes in an information set u. Consequently, each choice c at u is the last choice of a unique sequence $c|\sigma_u$, and the set of sequence of a player is given by $\mathbf{\Sigma} = \{\emptyset\} \cup \{c|\sigma_u\}$. In our formulated game, since both players have perfect recall, the game can be described in the sequence-form representation, in which the sequence sets of attacker and defender are defined by:

$$\mathbf{\Sigma}_A = \{\emptyset\} \cup \{n, n = 0, 1, ..., N\} \tag{4.16}$$

$$\mathbf{\Sigma}_D = \{\emptyset\} \cup \{m|n + r, m = 0, 1, ..., \min(M, n + r)\} \tag{4.17}$$

When attacker plays a mixed strategy, *i.e.*, the probabilities for its sequences, is represented by a non-negative vector $\boldsymbol{\alpha}$,

$$\boldsymbol{\alpha} = [\alpha_\emptyset, \alpha_0, \alpha_1, ..., \alpha_n, ..., \alpha_N]^T,$$

where $\alpha_\emptyset = 1$ and $\sum_{n=0}^{N} \alpha_n = \alpha_\emptyset$.

Similarly, the corresponding mixed strategy of the defender is represented by a non-negative vector $\boldsymbol{\delta}$,

$$\boldsymbol{\delta} = \left[\delta_{\emptyset}, \delta_{0|0}, \delta_{0|1}, \delta_{1|1}, ..., \delta_{m|n+r}, ..., \delta_{\min(M,N+R)|N+R}\right]^T,$$

where $\delta_{\emptyset} = 1$ and $\sum_{m=0}^{\min(M,n+r)} \delta_{m|n+r} = \delta_{\emptyset} = 1, \forall n, r$.

The relationship between the mixed strategies of the attacker and the defender is characterized by its *realization plan*, respectively. Generally, these realization plans can be rewritten in matrix form by:

$$\begin{cases} \mathbf{E}\boldsymbol{\alpha} = \mathbf{e} \\ \boldsymbol{\alpha} \geq 0 \end{cases} \quad \text{and} \quad \begin{cases} \mathbf{F}\boldsymbol{\delta} = \mathbf{f} \\ \boldsymbol{\delta} \geq 0 \end{cases}, \tag{4.18}$$

where $\mathbf{e} = [1, 0]^T$, $\mathbf{f} = [1, 0, ..., 0]^T$, $\mathbf{E}$ and $\mathbf{F}$ are constraint matrices which are given by:

$$\mathbf{E} = \begin{bmatrix} 1 & 0 & ... & 0 \\ -1 & 1 & ... & 1 \end{bmatrix} \tag{4.19}$$

$$\mathbf{F} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & ... & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & ... & 0 \\ -1 & 0 & 1 & 1 & 0 & 0 & ... & 0 \\ ... & & & & ... & & ... & \\ -1 & 0 & 0 & 0 & 0 & 1 & ... & 1 \end{bmatrix} \tag{4.20}$$

In the sequence-form representation, the payoff of the attacker and the defender is represented by matrices $\boldsymbol{\Phi}_A$ and $\boldsymbol{\Phi}_D$, respectively. Each sequence of the attacker corresponds to a row while each sequence of the defender corresponds to a column. The payoff values for a pair of sequences defined by a leaf of the game tree (*i.e.*, the terminal node) are equal to the payoff values of the leaf. Otherwise, the payoff values are zero. For example, the payoffs of attacker and defender at $(\emptyset, m|n+r)$ are zero, and at $(n, m|n+r)$ are $\Pi^A_{m,n,r}$ and $\Pi^D_{m,n,r}$.

The expected utility of the attacker and the defender in the sequence-form representation are given by:

$$U_A = \boldsymbol{\alpha}^T \boldsymbol{\Phi}_A \boldsymbol{\delta} \tag{4.21a}$$

$$U_D = \boldsymbol{\alpha}^T \boldsymbol{\Phi}_D \boldsymbol{\delta} \tag{4.21b}$$

The problem for finding NE of the game is given by:

$$\begin{aligned} \max_{\boldsymbol{\alpha}} \quad & \boldsymbol{\alpha}^T \boldsymbol{\Phi}_A \boldsymbol{\delta} && \text{(4.22a)} \\ \text{s.t.} \quad & \mathbf{E}\boldsymbol{\alpha} = \mathbf{e}, \boldsymbol{\alpha} \geq \mathbf{0} \\ \max_{\boldsymbol{\delta}} \quad & \boldsymbol{\alpha}^T \boldsymbol{\Phi}_D \boldsymbol{\delta} && \text{(4.22b)} \\ \text{s.t.} \quad & \mathbf{F}\boldsymbol{\delta} = \mathbf{f}, \boldsymbol{\delta} \geq \mathbf{0} \end{aligned}$$

The duality problems of (4.22) are given by:

$$\begin{aligned} \min_{\mathbf{x}} \quad & \mathbf{e}^T \mathbf{x} && \text{(4.23a)} \\ \text{s.t.} \quad & \boldsymbol{\alpha}^{\mathbf{T}} \left(-\boldsymbol{\Phi}_A \boldsymbol{\delta} + \mathbf{E}^T \mathbf{x} \right) = 0, \mathbf{E}^T \mathbf{x} \geq \boldsymbol{\Phi}_A \boldsymbol{\delta} \\ \min_{\mathbf{y}} \quad & \mathbf{f}^T \mathbf{y} && \text{(4.23b)} \\ \text{s.t.} \quad & \boldsymbol{\delta}^{\mathbf{T}} \left(-\boldsymbol{\Phi}_D^T \boldsymbol{\alpha} + \mathbf{F}^T \mathbf{y} \right) = 0, \mathbf{F}^T \mathbf{y} \geq \boldsymbol{\Phi}_D^T \boldsymbol{\delta} \end{aligned}$$

The feasible solutions of $\boldsymbol{\alpha}$ of (4.22a) and $\boldsymbol{x}$ of (4.23a) are optimal if and only if the two objective function values are equal, *i.e.*, $\boldsymbol{\alpha}^T \boldsymbol{\Phi}_A \boldsymbol{\delta} = \mathbf{e}^T \mathbf{x}$. This means that $\boldsymbol{\alpha}^{\mathbf{T}} \left(-\boldsymbol{\Phi}_A \boldsymbol{\delta} + \mathbf{E}^T \mathbf{x} \right) = 0$. Similarly, $\boldsymbol{\delta}$ of (4.22b) and $\boldsymbol{y}$ of (4.23b) are optimal if and only if $\boldsymbol{\delta}^{\mathbf{T}} \left(-\boldsymbol{\Phi}_D^T \boldsymbol{\alpha} + \mathbf{F}^T \mathbf{y} \right) = 0$. In summary, the equilibrium $\{\boldsymbol{\alpha}, \boldsymbol{\delta}\}$ is determined through solving the problem:

$$\begin{aligned} \text{find} \quad & \boldsymbol{\alpha}, \boldsymbol{\delta}, \mathbf{x}, \mathbf{y} \\ \text{s.t.} \quad & \mathbf{E}^T \mathbf{x} \geq \boldsymbol{\Phi}_A \boldsymbol{\delta}, \mathbf{F}^T \mathbf{y} \geq \boldsymbol{\Phi}_D^T \boldsymbol{\delta} \\ & \boldsymbol{\alpha}^{\mathbf{T}} \left(-\boldsymbol{\Phi}_A \boldsymbol{\delta} + \mathbf{E}^T \mathbf{x} \right) = 0 \\ & \boldsymbol{\delta}^{\mathbf{T}} \left(-\boldsymbol{\Phi}_D^T \boldsymbol{\alpha} + \mathbf{F}^T \mathbf{y} \right) = 0 \\ & \boldsymbol{E}\boldsymbol{\alpha} = \mathbf{e} \\ & \boldsymbol{F}\boldsymbol{\delta} = \mathbf{f} \\ & \boldsymbol{\alpha} \geq 0, \boldsymbol{\delta} \geq 0 \end{aligned} \qquad \text{(4.24)}$$

We introduce a non-negative vector $\mathbf{z} = \left(\boldsymbol{\alpha}, \boldsymbol{\delta}, \mathbf{x}^{'}, \mathbf{x}^{''}, \mathbf{y}^{'}, \mathbf{y}^{''} \right)^T$ where $\mathbf{x}^{'}, \mathbf{x}^{''}$, $\mathbf{y}^{'}$, and $\mathbf{y}^{''}$ are also non-negative vectors with the same dimension so that $\mathbf{x} = \mathbf{x}^{'} - \mathbf{x}^{''}$ and $\mathbf{y} = \mathbf{y}^{'} - \mathbf{y}^{''}$. The values of $\mathbf{x}, \mathbf{y}, \boldsymbol{\alpha}$, and $\boldsymbol{\delta}$ which satisfy the constraints of (4.24) can be found by solving a standard Linear Complementary Programing (LCP) which is given by [88]:

$$\begin{aligned} \text{find} \quad & \mathbf{z} \\ \text{s.t} \quad & \mathbf{H}\mathbf{z} + \mathbf{b} \geq \mathbf{0} \\ & \mathbf{z}^{\mathbf{T}} (\mathbf{H}\mathbf{z} + \mathbf{b}) = 0 \\ & \mathbf{z} \geq 0 \end{aligned} \qquad \text{(4.25)}$$

where $\mathbf{b}^T = \begin{pmatrix} 0, & 0, & \mathbf{e}, & -\mathbf{e}, & \mathbf{f}, & -\mathbf{f} \end{pmatrix}^T$ and

$$\mathbf{H} = \begin{bmatrix} \mathbf{0} & -\mathbf{\Phi}_A^T & \mathbf{E^T} & -\mathbf{E^T} & \mathbf{0} & \mathbf{0} \\ -\mathbf{\Phi}_D^T & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{F^T} & -\mathbf{F^T} \\ -\mathbf{E} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{E} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & -\mathbf{F} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{F} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix} \tag{4.26}$$

Lemke algorithm [79, 88, 89], a general version of the Lemke-Howson algorithm, is an efficient method to solve the LCP problem (please refer to Appendix A). We adopt it for dealing with the problem (4.25). Feasible points achieved from Lemke algorithm is then used to find the optimal solution of (4.24), which is the NE point of the game. The existence of a feasible solution of the formulated game is provided in [79] by subtracting a constant from the payoffs of two players that these become negative. Although the sequence-form representation reduces the complexity, the formulated game could be unsolvable when M, N, and R are too large. However, as mentioned in above, the formulated game happen in a small area where the differences in locations of SUs are undetectable by the locations verification process. Therefore, the proposed solution based on numerical algorithms is valid.

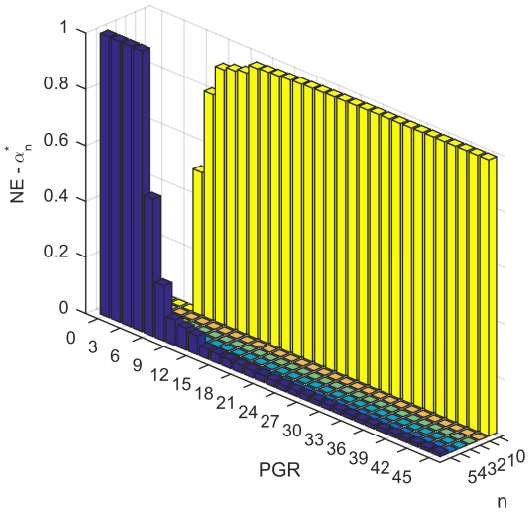
4.5 Simulation Results

This section presents the simulation results validating our studies on the verification processes to mitigate the influence of the location spoofing attacks and the ID spoofing attacks in the database driven-base CR networks. In order to analyze the NE of the game for the two penalty policy cases, we define the penalty-to-gain-ratio (PGR) which is equivalent to the number of banning time interval on a captured attacker. In particular, PGR is given by

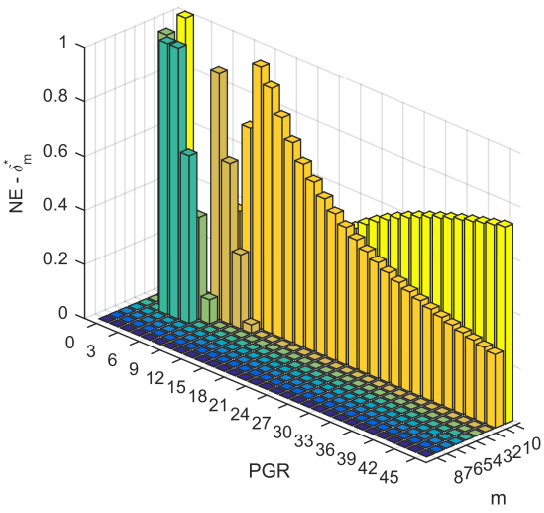
$$PGR = \frac{P}{G}, \tag{4.27}$$

where G is the gain of using a spectrum band in a requesting interval, *i.e.*, the interval between two adjacent requesting times.

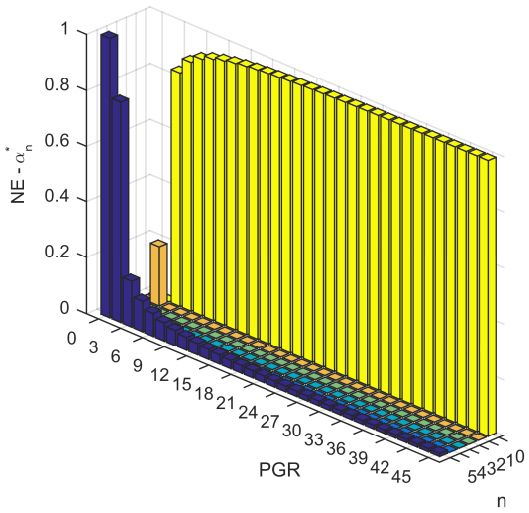
We first investigate the verification process to mitigate the location spoofing attack in CR networks. To make the simulation results clear and easy to follow, we start with a CRN with 6 actives SUs in the verified area (*i.e.*, $r = 6$) in which the attacker can send up to 5 spoofing request (*i.e.*, $N = 5$) and the defender can surveillance up to 8 request slot (*i.e.*, $M = 8$). Assume that $G = 10$, $C_S = 2$ and $C_A = 1$. Noted that C_A is the cost of sending a request to the network coordinator on a control channel, whereas C_S is the cost for localizing the request sender. Thus, it is reasonable to assume that $C_A \ll G$ and $C_A < C_S$. The results are



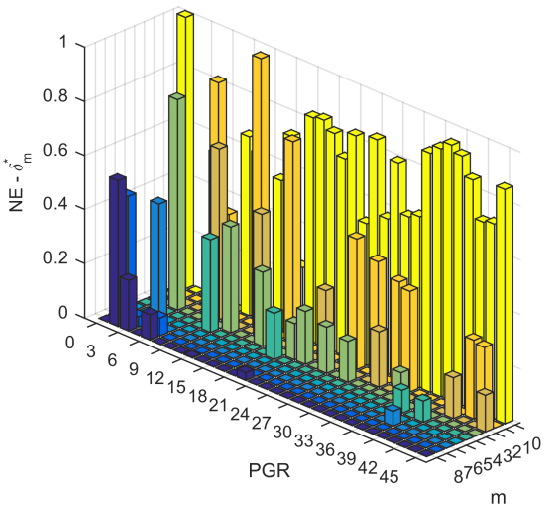
(A) Attacker – Constant penalty



(B) Defender – Constant penalty



(C) Attacker – Amount-related penalty



(D) Defender – Amount-related penalty

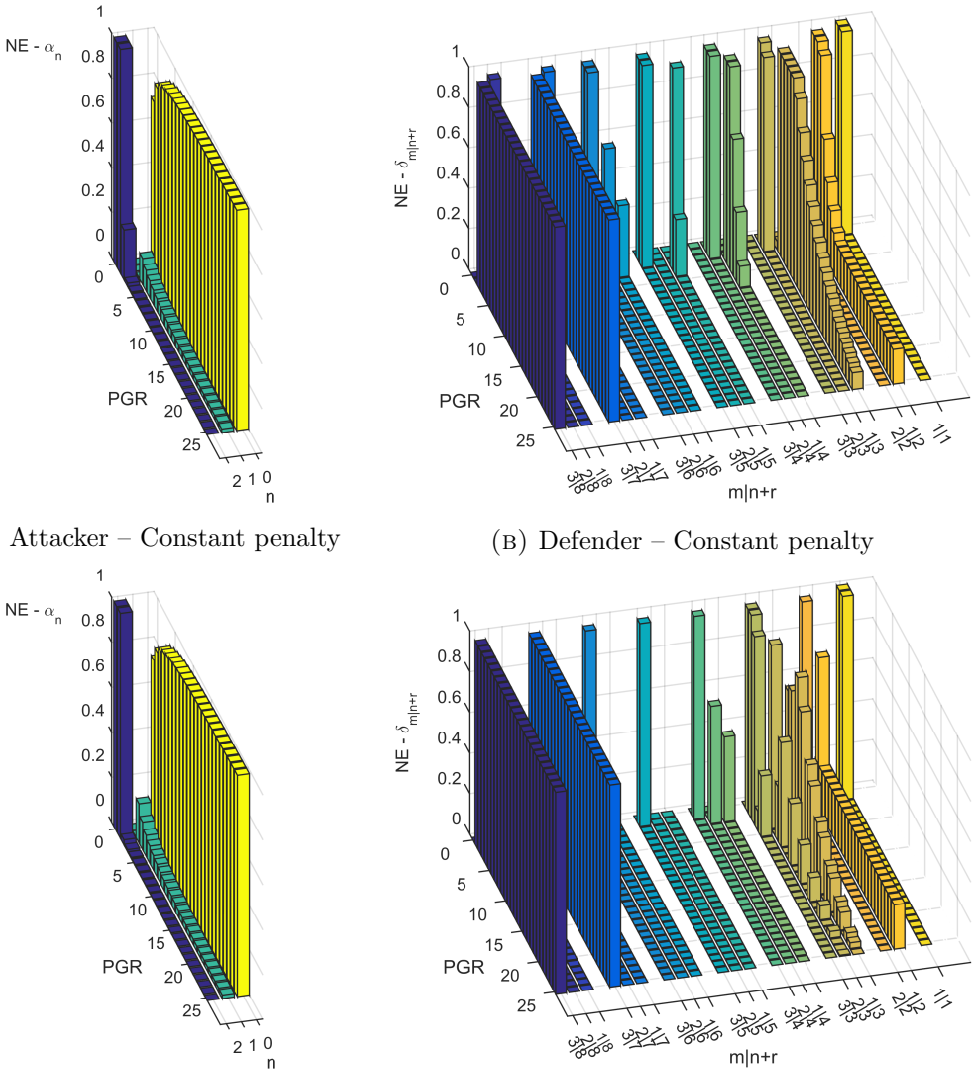
FIGURE 4.5 NE vs. PGR when $r = 6$, $N = 5$, and $M = 8$.

achieved by adopting Lemke-Howson algorithm on the original game with the size $N \times M$. Figure 4.5a and 4.5b present the strategy of the attacker and the defender in the constant penalty case while Figure 4.5c and 4.5d present the strategy of the attacker and the defender in the amount-related penalty cases with several values of PGR. We observe that, in the constant penalty case, the attacker only chooses no attack (*i.e.*, $n = 0$) or attack with the full capability (*i.e.*, $n = N$). The other attacking strategies are dominated. This result is in accordance with the statement in Proposition 4.1. In the amount-related penalty case, the attacker has almost the same behavior as an attacker in the constant penalty case, except for the small PGR case where strategies $n, n > 0$ appear. Complicated surveillance behaviors

of the defender, in this case, is the reason for this result. Also, there is a big difference between the NE of the defender in the two penalty cases. In the constant penalty case, in accordance with the state in Corollary 4.3, the defender does not select to verify more than the number of real users. However, in the amount-related case, the defender can select to verify more than the number of real users. The reason is that, in the amount-related case, the more the spoofing attacks has been captured, the more the benefit from penalties has been gained. Hence, the defender has to optimize the number of verification of request messages in its full range of monitoring capability, *i.e.*, $\min(M, r+n)$. In brief, these results mean that the penalty policies do affect the selection of the NE strategies of both players. For the effect of PGR, we observe that there is the same decreasing trend of both attacking and defending probabilities when PGR increases. With a large PGR, defender in constant penalty only needs to maintain a small monitoring probability in one location while defender in amount-related penalty may need to monitor many requesting locations. Consequently, for the formulated game between the spoofing attack and the requests' location verification, it is favorable to select the constant penalty policy with a large PGR. However, as analyzed in the penalty policy issue, the PGR should not be too large because of the possible influence on other normal NOs located inside the monitoring area. Therefore, a reasonable PGR should be selected, *e.g.*, $PGR = 15$ as in Figure 4.5a and 4.5b.

Next, we investigate the verification process to mitigate the ID spoofing attack in CR networks. Figure 4.6a, 4.6a, 4.6b,and 4.6d illustrate the NE of the surveillance game with different values of PGR for a CR network with $M = 3$, $N = 2$, $R = 4$ [1], and $\lambda = 2$. Other parameters are are the same as in the location verification case. Two penalty policies, the constant and the amount-related, are investigated. In order to provide a clear view of NE points, only the strategies of defender where $m \neq 0$ are depicted. Note that the probability $\delta_{0|n+r}$ at NE can be inferred from the others because $\sum_m \delta_{m|n+r} = 1$. From the simulation results, we observed that the NE points in two penalty cases are quite similar for the attacker. Specifically, the NE strategies of the attacker in the two penalty cases are implemented the spoofing attack with: i.) a high number of requests when PGR is low, and ii.) a low number of requests or not when PGR is high. It means that the penalty value does affect the attacking behavior of attacker. In contrast, the best behaviors of the defender depend on both PGR and the total number of request $n + r$: i.) at low PGRs, the defender performs to verify the spectrum bands in all $n + r$ because the probability of spoofing is very high in these points, ii.) at high PGRs, the defender only monitors spectrum bands at very low and very high $n + r$. The reason is that the probabilities of having a very low (or a very high) number of real requests are lower than the one in middle range, hence conducting verification process in these extreme cases will lead to a higher possibility of capturing the attacker.

1. We select a small value of R to provide a clearer presentation of the results



(A) Attacker – Constant penalty

(B) Defender – Constant penalty

(C) Attacker – Amount-related penalty

(D) Defender – Amount-related penalty

FIGURE 4.6 NE vs. PGR when $M = 3$, $N = 2$, $R = 4$, and $\lambda = 2$.

Figure 4.7 depicts the average delay penalty that the attacker has to suffer when it considers NE, uniform (*i.e.*, the attacker performs its pure strategies equally), and full attacking strategies (*i.e.*, the attacker always attacks with full capability). A Monte Carlo simulation with 10^6 samples is adopted, when $(M, N, R) = (3, 2, 6)$, and $\lambda = 2$. Two penalty policies are considered. From the simulation results, we observed that the attacker is severely delayed if it tries to increase their attacking rate and there is an optimal point for setting PGR for both penalty cases, *i.e.*, 8 for the constant penalty and 3 for the captured amount-related penalty, where the attacker suffers the highest delays. This means that, by using NE and setting the appropriate penalty, the defender could impose a stronger enforcement of reducing the selfish spoofing attack.

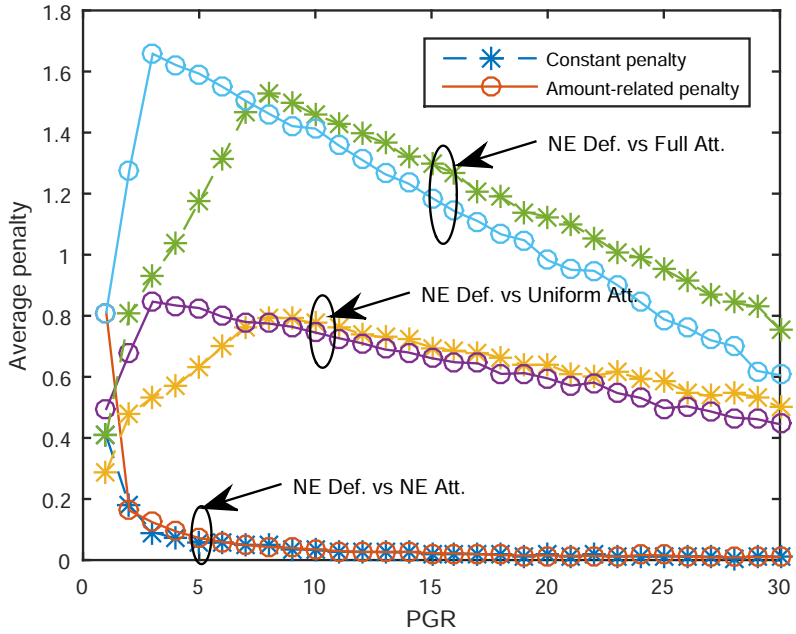


FIGURE 4.7 Average delay penalty vs. PGR.

4.6 Concluding Remarks

This chapter studied the verification processes to mitigate the influence of the location and the ID spoofing attack in the database driven-based CR networks. Depending on the structure of the spoofing request, an attacker could spoof either the location or the ID information or both. Under a location spoofing attack, the requests' location verification is proposed to counteract the spoofing attacks. Under an ID spoofing attack, the requests' data verification is the countermeasures for the spoofing attacks. A location/data verification game is formulated to modeling the interaction between the spoofing attack and the verification process. The surveillance game of the requests' location verification and the spoofing attack is expressed by the strategic-form while the game of the data identification and the spoofing attack is built upon by the sequence-form representation, where the NEs of the game are the best strategies for the attacker and the network coordinator. Simulation results confirm the analysis and show that a resource coordinator mitigates the spoofing attack by changing its penalty policy and surveillance strategies.

Chapter 5

Self-Coexistence in Distributed-based CR Networks: Collaborative Resource Allocation Framework

5.1 Introduction

In the centralized-based CR networks, the network coordinator manages the spectrum sharing process between users; hence, the coexistence mechanism between SUs, by performing the surveillance processes, mitigates the influence of attacks from misbehaving users. In Chapter 3 and 4, it has been shown that significant performance improvement can be obtained by such a surveillance process to deal with the PUE attacks in the spectrum sensing-based CR networks and the verification process to deal with the spoofing attacks in the database driven-based CR networks. In the distributed infrastructure-based CR networks, however, due to the lack of a network coordinator to control the spectrum sharing, ensuring the coexistence between the independent SUs with fair spectrum allocation and efficient spectrum utilization is a great challenge.

In this chapter, we examine a distributed-based CR network with multiple independent SUs in the licensed and the unlicensed spectrum bands. The considered network model is similar to a wireless communication system in which multiple transmitter-receiver pairs share a common frequency band and cause signal interference to other receivers [97]. In such a case, maintaining a harmonized coexistence between SUs is also key to optimize the CR network performance. Recently, the coexistence mechanism is considered by finding

The materials presented in Chapter 5 have been submitted to the EURASIP Journal on Wireless Communications and Networking [96].

a resource allocation strategy that allows SUs to simultaneously use the frequency band. Thus, the main interest of this chapter is to design an efficient resource allocation strategy between the cognitive users while maintaining a certain quality of service (QoS) requirements at the primary network. Since power control is an important aspect in the design of any communication system, especially in a mutual interference multiuser channel like the cognitive multiuser environment, this chapter focus on proposing a power allocation strategy between SUs. The proposed strategy is however not limited to adaptive power control. Other resource allocation aspects such as channel selection, user scheduling, beamforming or precoding design and MAC layer scheduling, can be investigated through this study.

In the distributed-based CR networks, due to the interaction between network users, recent work on power allocation mainly focuses on the two strategies: distributed strategy based on non-cooperative game framework [31–37] and centralized strategy based on joint optimization [38–43]. In the former, the power allocation among the users is considered as a non-cooperative game, where each user selfishly maximizes its own data rate [33, 62] or its packet transmission success rate [36] or its energy efficiency [37], or minimizes its transmit power while achieving a given target signal-to-interference-and-noise-ratio (SINR) [32]. In such games, pricing strategies [62] are added to encourage the users to adopt more socially optimal power control. As a result, the efficiency of the Nash Equilibrium is substantially enhanced if reasonable deviations from the target SINR are allowed. In the distributed approach, each user only needs the local information to make the independent and rational decision. This feature makes it possible to use low-complexity distributed algorithms to determine the power allocation. However, the global optimum may be less likely to be achieved and the system-level performance may be degraded. In the latter, the power allocation is coordinated by a joint optimization process, where all users aim to maximize a common utility function, such as the weighted sum-rate [38–41] or the total energy efficiency [37, 42, 43]. Mathematical frameworks, such as geometric programming [38–41] or the factional programing [37, 42, 43], are employed to establish the optimal power allocation. The joint optimization approach allows all the users to *coordinately optimize* their strategies and enables a dynamic allocation of the interference budget among users. However, this approach faces the problems of the *increased complexity* and *overhead* due to the demand for the channel information of all users and/or the requirement of a centralized unit. In addition, even when the global information is known, the optimization results show that users with poor channel conditions are allocated with much less power in order to optimize the performance of the whole network. It degrades the fairness between users in the network.

The main contribution of this chapter is the development of a collaborative power control framework, where the SUs use greater intelligence to avoid interference while optimizing the spectrum by collaborating with others to determine not just the best use of the spectrum for its own but the best use of spectrum for others. In particular, each user optimizes its power allocation strategy in a collaborative manner through a modified objective, which comprises

not only its own performance but also the others' performance. The proposed paradigm possesses the advantages of the distributed approach, which is the low-complexity and fast-converging algorithms with distributed implementation and overcomes the disadvantages of the centralized approach, which is the increased complexity, overhead and the requirement of a central unit. Specifically, we will formulate new games that will narrow the performance gap compared to the joint optimization, while maintaining the distributed implementation. Unlike the previous work, which mostly focused on utility maximization with power constraint [33, 35–38, 41, 43] or power minimization with quality constraint (*e.g.*, the minimum SINR at the receivers) [32, 34, 42, 62], we consider the power control problem with utility maximization under both power and SINR constraints. This allows us to maximize the network performance while maintaining a certain quality of transmission for each user.

Typically, the optimization problems for multiuser power control are non-concave (and/or non-quasi-concave). Obtaining a global solution is highly complex. In order to overcome this problem, we propose a low-complexity method for efficiently solving this issues by approximating the utility function of the game for each region of the SINR of the network: the high-SINR region (i.e., the users are far apart), and ii) the network in the low-SINR region (otherwise). By adopting the approximation process, we obtain a well-known game, such as the potential game [33] or the concave game [98], which is easier than the original game in order to find the NE strategy. The power allocation strategy is then analyzed through the NE of such game. The best response dynamic algorithm then prompts the study on the existence and uniqueness of the NE in the game. We supplement the theory with the numerical results, which show that the proposed paradigm provides better fairness between users, higher performance and lower convergence time, in comparison with the distributed-based and the joint optimization-based power allocation strategies. The simulations also confirm the convergence analysis of the proposed algorithms.

5.2 System Model and Problem Formulation

We consider the power allocation problem in a CR network with N independent SUs, each consists of a transmitter-receiver pair, sharing a common frequency band. Since the CR network exploits the spectrum opportunities in the licensed band owned by the primary network, the operation at the latter should not be affected by the former [99–101]. Thus, the considered network corresponds to a wireless communication system with N independent transmitter-receiver pairs, where the transmission from each transmitter causes interference at the reception of other receivers. The system model is illustrated in Figure 5.1.

We model this scenario as a Gaussian interference channel with flat fading, where each receiver perceives the transmitted signal with additive white Gaussian noise. Let $g_{j,i}$ be the channel power gain from the transmitter j to the receiver i of the CR network and σ_i^2 be the noise power at receiver i. Consequently, $g_{i,i}$ is the channel power gain between the

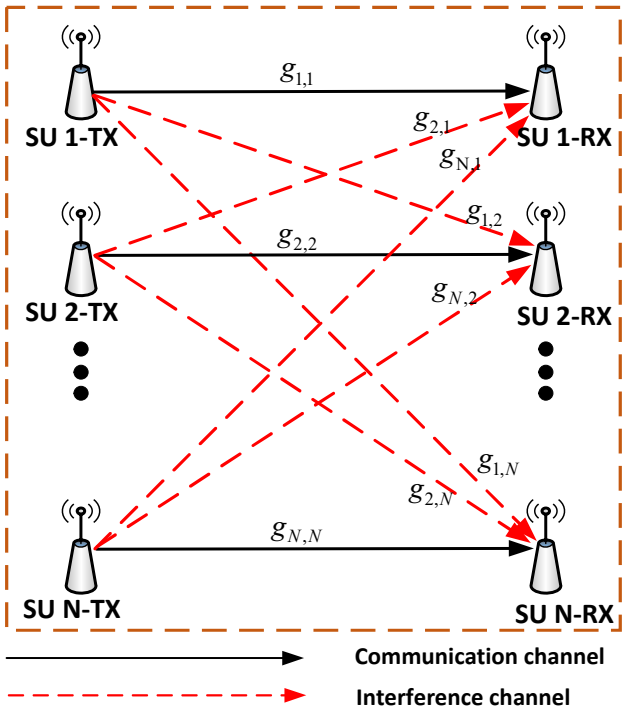


FIGURE 5.1 The system model of the power allocation problem between multiple SUs in a cognitive radio network.

transmitter and the receiver of user i. Denote by $\mathbf{p} = \{p_1, p_2, \ldots, p_N\}$ the vector comprising the *allocated power* of all SUs and $\mathbf{p}_{-i}$ the power vector of all SUs except i. The SINR at the receiver i, denoted by γ_i, is given by

$$\gamma_i(p_i, \mathbf{p}_{-i}) = \frac{g_{i,i}p_i}{\sigma_i^2 + \sum\limits_{j \neq i} g_{j,i}p_j}. \tag{5.1}$$

Suppose that each user can adjust its transmit power within a bounded region ($[0, p_i^{\max}]$) to meet a given *target SINR constraint*. For user i, it means that

$$\gamma_i \geq \gamma_i^{tar}, \tag{5.2}$$

where γ_i^{tar} is the given *target SINR* of user i.

Over the time-period of interest, we assume that the channel gains are fixed (*i.e.*, fading effects take place at a much slower time-scale). Let $r_i(p_i, \mathbf{p}_{-i})$ be the rate of user i. Then,

$$r_i(p_i, \mathbf{p}_{-i}) = \log_2(1 + \gamma_i(p_i, \mathbf{p}_{-i})) \tag{5.3}$$

For each user i, we defined the *performance metric* $f_i(p_i, \mathbf{p}_{-i})$ that capture a trade-off between the obtained transmission rate and the power cost for the data transmission process.

These metrics are then given by

$$f_i\left(p_i, \mathbf{p}_{-i}\right) = r_i\left(p_i, \mathbf{p}_{-i}\right) - c_i p_i, \tag{5.4}$$

where c_i is the pricing factor of user i [62].

In the distributed strategy based on non-cooperative game approach [32–36], each cognitive user acts in a selfish manner by optimizing its own performance. It means the utility of each user is its performance metric. However, in the centralized strategy based on joint optimization approach [37–43], network users share a *common utility function* which is typically the total performance of the network. In this chapter, we consider the collaboration between cognitive users by proposing the *collaborative utility function*. Instead of considering its own performance or the common utility function, each user optimizes its collaborative utility function which comprises not only its own performance but also the others' performances. For simplicity, we suppose that the collaborative utility function of each user in the licensed spectrum band case is

$$U_i^{col}\left(p_i, \mathbf{p}_{-i}\right) = \underbrace{f_i\left(p_i, \mathbf{p}_{-i}\right)}_{\text{performance metric}} + \underbrace{g_i\left(p_i, \mathbf{p}_{-i}\right)}_{\text{collaboration metric}}, \tag{5.5}$$

where the *collaboration metric* $g_i\left(p_i, \mathbf{p}_{-i}\right)$ is assumed to be the partial sum of the others' performances, *i.e.*,

$$g_i\left(p_i, \mathbf{p}_{-i}\right) = \sum_{j \neq i} \alpha_j f_j\left(p_j, \mathbf{p}_{-j}\right), \tag{5.6}$$

and $\alpha_j \geq 0$ is the *collaboration factor* for user j.

The collaboration between SUs is designated through a collaboration channel, which provides a direct means for network users to share potentially valuable information and to strategize with their peers. Example of the collaboration protocol is presented in the system specifications of [102]. The collaboration factors are determined by each user based on its demand.

In the collaborative power allocation, each user aims to *maximize* its collaborative utility function, *i.e.*,

$$\begin{aligned} \max_{p_i} \quad & U_i^{col}(p_i, \mathbf{p}_{-i}) \quad \forall i = 1, \ldots, N \\ \text{s.t.} \quad & p_i \in [0, p_{\max}^i] \\ & \gamma_i \geq \gamma_i^{tar} \end{aligned} \tag{5.7}$$

5.2.1 Game Formulation

Due to the conflict and trade-off between the objectives of network users, the game-theoretic approach is employed to model the relationship between network users. We deemed

this game as the *collaborative power control game*

$$\mathcal{G} \triangleq \{\mathcal{N}, \{\mathcal{P}_i(\mathbf{p}_{-i})\}_i, \{U_i^{col}(p_i, \mathbf{p}_{-i})\}_i\}, \tag{5.8}$$

where $\mathcal{N} = \{1, 2, \ldots, N\}$ is the set of players, $\mathcal{P}_i(\mathbf{p}_{-i})$ is the player i's strategy set such that $\gamma_i \geq \gamma_i^{tar}$.

The game $\mathcal{G}$ is a continuous game since each strategy set of the game is a continuous interval of real numbers, i.e., $\mathcal{P}_i \subseteq \mathbb{R}$ and the utility function U_i^{col} is continuous and differentiable everywhere on $\mathcal{P}_i$.

Generally, a Nash Equilibrium (NE) of a game is a feasible strategy from which players cannot gain by independently adjusting their strategy. For $\mathcal{G}$, $(p_i^*, \mathbf{p}_{-i}^*)$ is a NE if and only if

$$U_i^{col}(p_i^*, \mathbf{p}_{-i}^*) \geq U_i^{col}(p_i, \mathbf{p}_{-i}^*)\ \forall p_i \in \{\mathcal{P}_i(\mathbf{p}_{-i})\}_i. \tag{5.9}$$

In a game, the existence of a NE is guaranteed under the following assumptions [98, 103]:

— The users' feasible action sets $\mathcal{P}_i(\mathbf{p}_{-i})$ are non empty, closed, convex, and contained in some compact set $\mathcal{C}_i$ for all $\mathbf{p}_{-i} \in \mathcal{P}_i(\mathbf{p}_{-i}) = \prod_{j \neq i} \mathcal{P}_j$.

— The set $\mathcal{P}_i(\mathbf{p}_{-i})$ vary continuously with p_i.

— Each user's payoff function $U_i^{col}(p_i, \mathbf{p}_{-i})$ is quasi-concave in $p_i\ \forall \mathbf{p}_{-i} \in \mathcal{P}_{-i}$.

To determine the NE of the game, the iterative process by iteratively solving N coupled problems in (5.7) can be used. In such a process, each user iteratively selects the best response (BR) (or one of the BRs) to the others' strategies. Specifically, given the other's powers $\mathbf{p}_{-i}$, the BR of player i in $\mathcal{G}$ is defined as

$$\mathcal{B}_i(\mathbf{p}_{-i}) \triangleq \underset{p_i \in \mathcal{P}_i(\mathbf{p}_{-i})}{\arg\max}\ U_i^{col}(p_i, \mathbf{p}_{-i}), \tag{5.10}$$

Such a process is called the best-response dynamics (BRD), where any fixed point of BRD is a NE of the game [33, 43].

5.2.2 Approximation

The important questions in the analysis of a non-cooperative game are to investigate the existence and uniqueness of an equilibrium, and whether implementing the BRD eventually yields an equilibrium. In our game, however, the question is more challenging since

— the objective function in (5.7) is non-concave and non-quasi-concave, and

— not only the utility function, but also the strategy set of each player are mutual coupling, depending on other players' actions due to the SINR constraints.

To this end, we propose low-complexity methods for efficiently solving these problems by approximating the utility function of the game for each region on the SINR network thanks to the following features:

— for high SINR region (i.e., the users are far apart or $\gamma_i \gg 1$), the rate $\log_2(1+\gamma_i)$ and $\log_2(1+\gamma_i)$ can be approximated by $\log_2(\gamma_i)$, *i.e.*, $\log_2(1+\gamma_i) \approx \log_2(\gamma_i)$,
— for the low SINR region (i.e., otherwise), since the utility function is continuous and differentiable, it hence can be approximated by a linear function through the first-order Taylor approximation.

The aim is to overcome the non-concave issues of the utility function; hence, we can obtain a well-known game, such as the potential game and the concave game, which is easier than the original game in order to find the NE strategy. Specifically, consider the game $\mathcal{G}$, we have:

Definition 5.1. The continuous game $\mathcal{G}$ is an exact continuous potential game if exists a potential function $\Phi(\mathbf{p})$ such that

$$\frac{\partial \Phi(\mathbf{p})}{\partial p_i} = \frac{\partial U_i^{col}(p_i, \mathbf{p}_{-i})}{\partial p_i}, \forall i \in \mathcal{N}$$

If the potential function if strictly concave, from [28] (Definition 2.3), the game $\mathcal{G}$ is a strictly concave potential game.

Definition 5.2. The continuous game $\mathcal{G}$ is a continuous concave game if the utility function of player i, i.e., U_i^{col} is continuous in $\mathbf{p}$ and concave in p_i for $\{\mathcal{P}_i(\mathbf{p}_{-i})\}_i$.

The approximation methods, the difference between these approximated games, and how each game is applicable to certain scenarios are shown in Figure 5.2. The analysis of these games will be presented in next Sections.

5.3 The Potential Game Approximation

We first do the approximation of the utility function of $\mathcal{G}$ for the CR network with high SINR region, *i.e.*, the network users and the PU are far apart. For such scenario, the performance metric and the collaboration metric of each user can be approximated as

$$\hat{f}_i(p_i, \mathbf{p}_{-i}) = \log_2(\gamma_i) - c_i p_i, i = 1, \ldots, N \tag{5.11a}$$

$$\hat{g}_i(p_i, \mathbf{p}_{-i}) = \sum_{j \neq i} \alpha_j \hat{f}_j(p_j, \mathbf{p}_{-j}). \tag{5.11b}$$

Consequently, the *modified* utilities of player i is given by

$$\hat{U}_i^{col}(p_i, \mathbf{p}_{-i}) = \hat{f}_i(p_i, \mathbf{p}_{-i}) + \hat{g}_i(p_i, \mathbf{p}_{-i}), \tag{5.12}$$

We formulate the new games with the modified utilities, which is referred to the *potentialized game*, and denote it by

$$\mathcal{G}_1 \triangleq \{\mathcal{N}, \{\mathcal{P}_i(\mathbf{p}_{-i})\}_i, \{\hat{U}_i^{col}(p_i, \mathbf{p}_{-i})\}_i\}, \tag{5.13}$$

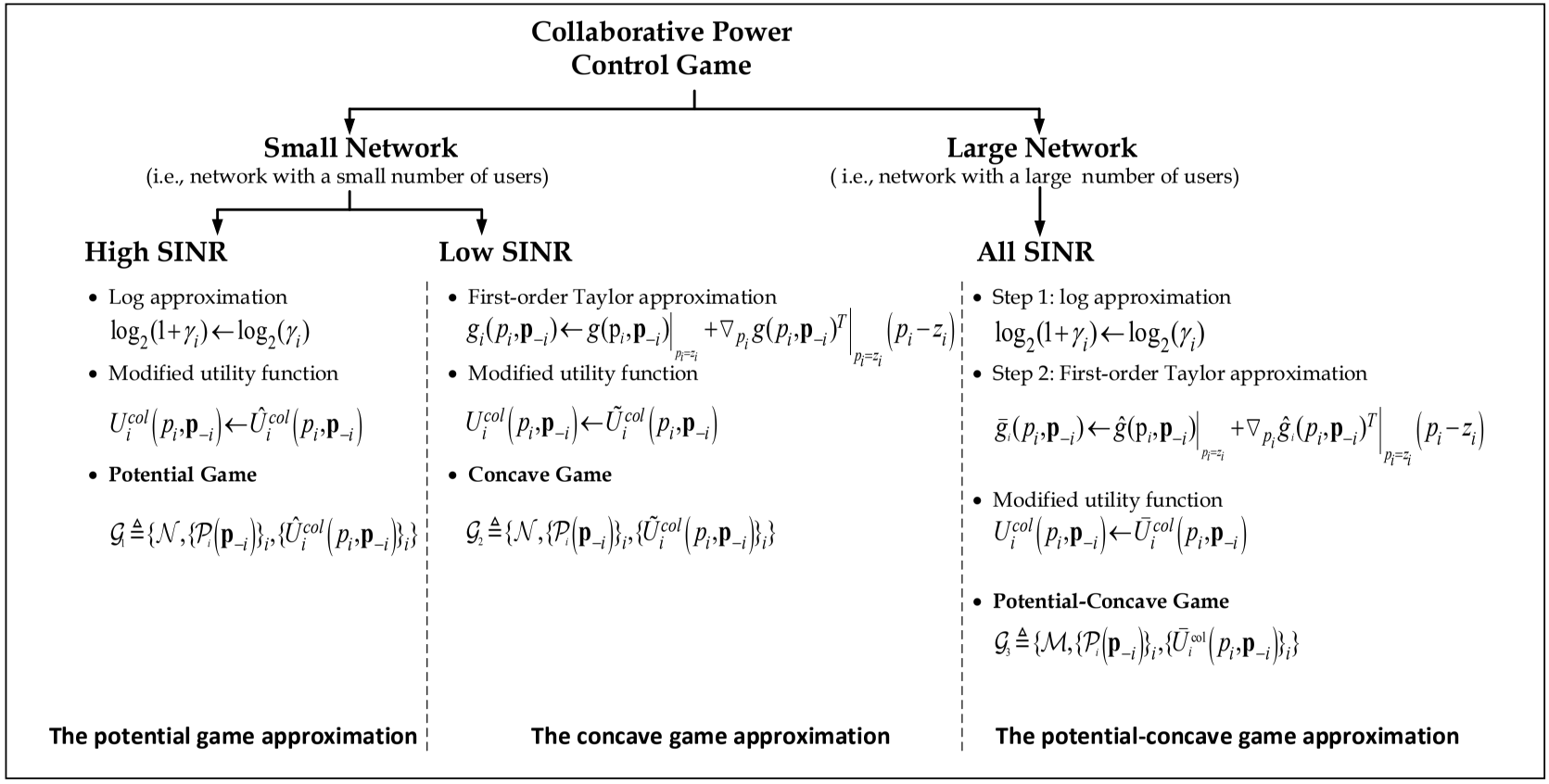


FIGURE 5.2 The approximated games for each region on SINR and network size.

In game $\mathcal{G}_1$, given $\mathbf{p}_{-i}$, we define the best response $\hat{\mathcal{B}}_i(\mathbf{p}_{-i})$ of player i as

$$\hat{\mathcal{B}}_i(\mathbf{p}_{-i}) \triangleq \underset{p_i \in \{\mathcal{P}_i(\mathbf{p}_{-i})\}_i}{\arg\max} \hat{U}_i^{col}(p_i, \mathbf{p}_{-i}). \tag{5.14}$$

5.3.1 Properties of the Potentialized Game

Hereafter, we obtain some basic properties of the game $\mathcal{G}_1$. First, we prove that the game is an exact potential game.

Proposition 5.3. *The game $\mathcal{G}_1$ is an exact continuous potential game. The corresponding potential function $\Phi(\mathbf{p})$ is given by*

$$\Phi(\mathbf{p}) = \sum_i \left(\log_2(g_{i,i}p_i) - c_i p_i - \frac{1}{N-1} \sum_{j \neq i} \alpha_j \log_2 \left(\sum_{k \neq j} g_{k,j}p_k + \sigma_j^2 \right) \right) \tag{5.15}$$

Proof. For user $i \in \mathcal{N}$, we have

$$\frac{\partial \hat{U}_i^{col}}{\partial p_i} = \frac{1}{\ln(2)} \left[\frac{1}{p_i} - c_i - \sum_{j \neq i} \alpha_j \frac{g_{i,j}}{g_{i,j}p_i + \sum\limits_{k \neq i,j} g_{k,j}p_k + \sigma_j^2} \right], \tag{5.16}$$

Next, since we have

$$\Phi(\mathbf{p}) = \sum_i (\log_2(g_{i,i}p_i) - c_i p_i) - \frac{1}{N-1} \sum_i \Big(\sum_{j \neq i} \alpha_j \log_2 \Big(\sum_{k \neq j} g_{k,j}p_k + \sigma_j^2 \Big) \Big) \tag{5.17}$$

then

$$\frac{\partial \Phi(\mathbf{p})}{\partial p_i} = \frac{1}{\ln(2)} \left[\frac{1}{p_i} - c_i - \sum_{j \neq i} \alpha_j \frac{g_{i,j}}{g_{i,j}p_i + \sum\limits_{k \neq i,j} g_{k,j}p_k + \sigma_j^2} \right] \tag{5.18}$$

According to Definition 5.1 of (exact) potential game, we therefore conclude that the game $\mathcal{G}_1$ is an exact potential games with potential function $\Phi(\mathbf{p})$. □

5.3.2 Analysis of the Equilibria

The existence and uniqueness of the NE points of the game $\mathcal{G}_1$ are now studied by exploiting the utility function and the potential function (5.15) as following.

Proposition 5.4. *If $\sum\limits_{j \neq i} \alpha_j \leq 1, \forall j \in \mathcal{N}$, the game $\mathcal{G}_1$ admits a unique NE point.*

Proof. According to [98], in game $\mathcal{G}_1$, if the utility function $\hat{U}_i^{col}(p_i, \mathbf{p}_{-i})$ is strictly concave w.r.t (i.e., with regard to) $\{\mathcal{P}_i(\mathbf{p}_{-i})\}_i \ \forall i \in \mathcal{N}$ and continuous w.r.t $\{\mathcal{P}_j(\mathbf{p}_{-i})\}_j \ \forall j$ different from $i \in \mathcal{N}$, hence a pure NE exists and it is unique.

We observed that:

— the approximated utility function $\hat{U}_i^{col}(p_i, \mathbf{p}_{-i})$ is continuously differentiable w.r.t $\{\mathcal{P}_i(\mathbf{p}_{-i})\}_j \ \forall i \in \mathcal{N}$, and

$$\ln(2)\frac{\partial^2 \hat{U}_i^{col}(p_i, \mathbf{p}_{-i})}{(\partial p_i)^2} = \frac{-1}{p_i^2} + \sum_{j\neq i} \alpha_j \left(p_i + \sum_{k\neq j,i} \frac{g_{k,j}}{g_{i,j}} p_k + \frac{\sigma_j^2}{g_{i,j}} \right)^{-2},$$

— the approximated utility function $\hat{U}_i^{col}(p_i, \mathbf{p}_{-i})$ is continuously differentiable w.r.t $\{\mathcal{P}_j(\mathbf{p}_{-i})\}_j \ \forall j$ different from $i \in \mathcal{N}$, and
— the SINR constraint is linear w.r.t $\{\mathcal{P}_i(\mathbf{p}_{-i})\}_i \ \forall i \in \mathcal{N}$ since

$$\gamma_i - \gamma_i^{tar} = \frac{g_{i,i}p_i}{\sum\limits_{j\neq i} g_{j,i}p_j + \sigma_i^2} - \gamma_i^{tar} \geq 0, \forall i \in \mathcal{N}. \tag{5.19}$$

Thus, if

$$\sum_{j\neq i} \alpha_j \leq 1, \forall i, j \in \mathcal{N} \tag{5.20}$$

is satisfied then the second-order derivatives of the utility function $\hat{U}_i^{col}(p_i, \mathbf{p}_{-i}) < 0$ w.r.t $\{\mathcal{P}_i(\mathbf{p}_{-i})\}_i \ \forall i \in \mathcal{N}$, or the utility function $\hat{U}_i^{col}(p_i, \mathbf{p}_{-i})$ is strictly concave with p_i.

Therefore, if the condition (5.20) holds then the game $\mathcal{G}_1$ admits a unique NE point. □

Next, given the power vector $\mathbf{p}_{-i}$, the BR of the user $i \in \mathcal{N}$ in (5.14) is determined as follows:

Lemma 5.5. *If*

$$p_i^{\max} \geq \frac{\gamma_i^{tar}}{g_{i,i}} \left(\sum_{j\neq i} g_{j,i} p_j^{\max} + \sigma_i^2 \right) \tag{5.21}$$

then $\hat{\mathcal{B}}_i(\mathbf{p}_{-i})$ *takes the form*

$$\hat{\mathcal{B}}_i(\mathbf{p}_{-i}) = \min\{p_i^{\max}, \max\{p_i^*, p_i^{tar}\}\} \tag{5.22}$$

wherein

$$p_i^{tar}(\mathbf{p}_{-i}) \triangleq \frac{\gamma_i^{tar}}{g_{i,i}} \left(\sum_{j\neq i} g_{j,i} p_j + \sigma_i^2 \right) \tag{5.23}$$

and

$$p_i^* \triangleq \underset{p_i \in \mathbb{R}^+}{\operatorname{argmax}} \Phi(\mathbf{p}). \tag{5.24}$$

Proof. The first part of the Lemma easily follows from the SINR constraints ($\gamma_i \geq \gamma_i^{tar}$) as

$$p_i \geq \frac{\gamma_i^{tar}}{g_{i,i}} \left(\sum_{j\neq i} g_{j,i} p_j + \sigma_i^2 \right) \tag{5.25}$$

Since $p_i \leq p_i^{\max}$ for all $i \in \mathcal{N}$, then

$$\frac{\gamma_i^{tar}}{g_{i,i}} \left(\sum_{j \neq i} g_{j,i} p_j^{\max} + \sigma_i^2 \right) \geq \frac{\gamma_i^{tar}}{g_{i,i}} \left(\sum_{j \neq i} g_{j,i} p_j + \sigma_i^2 \right) \tag{5.26}$$

Hence, if $\forall i \in \mathcal{N}$, (5.21) holds, then there always exists a power $p_i \in [0, p_i^{\max}]$ such that $\gamma_i \geq \gamma_i^{tar}$ is fulfilled.

Next, since the game is a potential game with strictly concave potential function, it admits a unique maximizer $p_i \in \mathbb{R}^+$. Accounting for the SINR constraint (5.2) and imposing (5.24) eventually yields (5.22). □

5.3.3 Distributed Implementation

To determine the NE strategy of the game, we employ the Best Response Dynamic (BRD) algorithm by iteratively finding the BR of each player given others' power profile until reaching the NE point [33]. Since the game $\mathcal{G}_1$ is an exact potential game with an unique NE, the global convergence of the BRD algorithm holds. The BRD algorithm and the information exchange process for the cooperative power allocation are as follows.

To implement Algorithm 2, information is exchanged between users through a *collaboration paradigm*. Specifically, the network users using a *collaboration channel* to distribute the information to be shared and the resulting decisions. For each user i, the direct channel (*i.e.*, $g_{i,i}$) can be estimated at its receiver and sent back to its transmitter through a feedback channel. Since the power (p_i) is locally available at the transmitter, the interference plus noise (*i.e.*, $\sum_{j \neq i} g_{j,i} p_j + \sigma_i^2$) can be observed. Then, the computation of (5.23) is available. For user i, we observe that the computation of best response does not depend on the other's direct channel and power (*i.e.*, $g_{j,j}$ and p_j, $\forall j \neq i$) and only requires

— knowledge of its direct channels,
— knowledge of its cross-channel (*i.e.*, $g_{i,j}, j \neq i$), and
— knowledge of other users' interference plus noise.

Since the cross-channel can be estimated through the other users' interference plus noise and its locally available power (p_i), we can obtain the best response by exchanging the information about the interference plus noise of each user. Therefore, the distributed implementation can be adopted to solve (5.22). We conclude that Algorithm 2 not only guarantees the convergence to a unique NE but can also be implemented in a distributed manner.

5.4 The Concave Game Approximation

The *potentialized game* approach in Section 5.3 only serves as a good approximation for the true rate when the users operate in the high SINR region (i.e., the users are far apart).

Algorithm 2 Best Response Dynamic (BRD)

Initialize: $k = 1$ and $\forall i : p_i[0] \in \mathbb{R}^+$ in the feasible set
repeat
  for $i = 1$ to N **do**
    Compute p_i^{tar} from (5.20)
    for $i = 1$ to N **do**
      Estimate h_{ii} from the received power and p_i.
      Compute the interference plus noise: $\sum_{j \neq i} g_{j,i} p_j + \sigma_i^2$.
      Set up the collaboration channel
      Broadcast the interference plus noise on the collaboration channel
    Update the potential function as (5.26)
    Compute $p_i^*[k]$ from (5.24)
    Update the power as (5.22)
  Update $k = k + 1$
until convergence

$$\tilde{U}_i^{col}(p_i, \mathbf{p}_{-i}, z_i) = \log_2(1+\gamma_i) + \sum_{j \neq i} \alpha_j \left(\log_2 \left(1 + \frac{g_{j,j} p_j}{g_{i,j} z_i + \sum\limits_{k \neq i,j} g_{k,j} p_k + \sigma_i^2} \right) - c_j p_j \right)$$
$$+ \sum_{j \neq i} \frac{\alpha_j}{\ln(2)} (z_i - p_i) \frac{g_{i,j} g_{j,j} p_j}{\left(g_{i,j} z_i + \sum\limits_{k \neq i,j} g_{k,j} p_k + \sigma_i^2 \right) \left(g_{i,j} z_i + \sum\limits_{k \neq i} g_{k,j} p_k + \sigma_2^2 \right)} - c_i p_i \tag{5.29}$$

Hereafter, we do the approximation the utility function of the games for the CR network with low SINR region (i.e., the otherwise). For such scenario, the origin utility functions are approximated by *linearizing* the convex part (i.e., the collaborative metric $g_i(p_i, \mathbf{p}_{-i})$) as in follows:

$$\tilde{g}_i(p_i, \mathbf{p}_{-i}, z_i) \approx g(z_i, \mathbf{p}_{-i}) + \bigtriangledown_{p_i} g(p_i, \mathbf{p}_{-i})^T |_{p_i = z_i} (p_i - z_i), \tag{5.27}$$

where $z_i \in [0, p_i^{\max}]$ is the initial point of user i for the approximation process.

The *modified utility function* then is given by

$$\tilde{U}_i^{col}(p_i, \mathbf{p}_{-i}, z_i) = f(p_i, \mathbf{p}_{-i}) + \tilde{g}_i(p_i, \mathbf{p}_{-i}, z_i) \tag{5.28}$$

or can be expanded as in (5.29).

Obviously, the approximated collaborative metric $\tilde{g}_i(p_i, \mathbf{p}_{-i}, z_i)$ is a linear function; hence the approximated utility function is concave. We then formulate a non-cooperative game

with modified utility function as follows

$$\mathcal{G}_2 \triangleq \{\mathcal{N}, \{\mathcal{P}_i(\mathbf{p}_{-i})\}_i, \{\tilde{U}_i^{col}(p_i, \mathbf{p}_{-i})\}_i\}. \tag{5.30}$$

In such a game, the players' feasible action sets are non-empty, closed, and convex. Since the modified utility function is concave, from Definition 5.2, the game hence is referred as the *concave game*.

The best response of user i for the given strategy $\mathbf{p}_{-i}$ are defined as

$$\tilde{\mathcal{B}}_i(\mathbf{p}_{-i}) \triangleq \underset{p_i \in \mathcal{P}_i(\mathbf{p}_{-i})}{\arg\max}\, \tilde{U}_i^{col}(p_i, \mathbf{p}_{-i}) \tag{5.31}$$

5.4.1 Properties of the Concave Game

Some properties of the game $\mathcal{G}_2$ are as follows:

Lemma 5.6. *If condition* (5.21) *holds then* $\tilde{\mathcal{B}}_i(\mathbf{p}_{-i})$ *takes the form*

$$\tilde{\mathcal{B}}_i(\mathbf{p}_{-i}) = \min\{p_i^{\max}, \max\{p_i^{+}, p_i^{tar}\}\} \tag{5.32}$$

wherein $p_i^{tar}(\mathbf{p}_{-i})$ *is defined as in* (5.23) *and*

$$p_i^{+} \triangleq \underset{p_i \in \mathbb{R}^+}{\arg\max}\, \tilde{U}_i^{col}(p_i, \mathbf{p}_{-i}) \tag{5.33}$$

Proof. The first part of the Lemma easily follows from the SINR constraints ($\gamma_i \geq \gamma_i^{tar}$).

Next, since the modified utility function (5.28) is a concave function (*i.e.*, sum of a concave function and a linear function), hence it admits a maximizer $p_i^{+} \in \mathbb{R}^+$. Accounting for the SINR constraint and imposing (5.33) eventually yields (5.32). □

Lemma 5.7. *For any given* $\mathbf{p}_{-i}$*, the solution to* (5.33) *is founded to be*

$$p_i^{+} = \frac{1}{c_i + \sum\limits_{j \neq i} \alpha_j \varphi_i(z_i)} - \sum_{j \neq i} \frac{g_{j,i}}{g_{i,i}} p_j - \frac{\sigma_i^2}{g_{i,i}}, \tag{5.34}$$

where

$$\varphi_i(z_i) = \frac{1}{\ln(2)} \frac{g_{j,j} g_{i,j} p_j}{\left(g_{i,j} z_i + \sum\limits_{k \neq i,j} g_{k,j} p_k + \sigma_j^2\right)\left(g_{i,j} z_i + \sum\limits_{t \neq i} g_{t,j} p_t + \sigma_j^2\right)} \tag{5.35}$$

Proof. For the game $\mathcal{G}_2$, the utility function of player i is given by

$$\begin{aligned}\tilde{U}_i^{col}(p_i, \mathbf{p}_{-i}, z_i) &= f_i(p_i, \mathbf{p}_{-i}) + \tilde{g}_i(p_i, \mathbf{p}_{-i}, z_i) \\ &= \log_2\left(1 + \frac{g_{i,i}p_i}{\sum\limits_{j\neq i} g_{j,i}p_j + \sigma^2}\right) - c_i p_i + \tilde{g}(p_i, \mathbf{p}_{-i})_{p_i=z_i} \\ &+ \sum_{j\neq i} \alpha_j \left[\varphi_i\left(z_i\right)\left(p_i - z_i\right)\right],\end{aligned} \tag{5.36}$$

Since $\tilde{U}_i(p_i, z_i)$ is a concave function w.r.t p_i, there are unique maximizer point p_i^+ which is determined by

$$p_i^+ \triangleq \arg\max_{p_k \in +} \tilde{U}_i^{col}\left(p_i, \mathbf{p}_{-i}\right) \tag{5.37}$$

Thus, we have:

$$\begin{aligned}&\left.\frac{\partial \tilde{U}_i^{col}\left(p_i, z_i\right)}{\partial p_i}\right|_{p_i=p_i^+} = 0 \\ &\Rightarrow \frac{g_{i,i}}{g_{i,i}p_i^+ + \sum\limits_{j\neq i} g_{j,i}p_j + \sigma_i^2} - c_i + \sum_{j\neq i} \alpha_j \varphi_i\left(z_i\right) = 0 \\ &\Rightarrow p_i^+ = \frac{1}{g_{i,i}}\left(\frac{g_{i,i}}{c_i - \sum\limits_{j\neq i} \alpha_j \varphi_i\left(z_i\right)} - \sum_{j\neq i} g_{j,i}p_j - \sigma_i^2\right) \\ &\Rightarrow p_i^+ = \frac{1}{c_i - \sum\limits_{j\neq i} \alpha_j \varphi_i\left(z_i\right)} - \sum_{j\neq i} \frac{g_{j,i}}{g_{i,i}} p_j - \frac{\sigma_i^2}{g_{i,i}}\end{aligned}$$

□

5.4.2 Analysis of the Equilibria

The existence of equilibria are now studied under the assumption that condition (5.21) holds.

Proposition 5.8. *The game $\mathcal{G}_2$ admits a nonempty set of NE points. If $\exists\ \alpha_i\ (\forall i \in \mathcal{N})$ such that*

$$-\frac{\partial^2 \tilde{U}_i^{col}(p_i, \mathbf{p}_{-i}, z_i)}{\partial p_i \partial p_i} \geq \sum_{j\neq i} \left|\frac{\partial^2 \tilde{U}_i^{col}(p_i, \mathbf{p}_{-i}, z_i)}{\partial p_i \partial p_j}\right| \tag{5.38}$$

then the NE point can be obtained by iteratively updating the transmit powers according to (5.32) *from any starting point.*

Proof. In a game, the existence of a NE is guaranteed under the following assumptions [103]:

— The users' feasible action sets $\mathcal{P}_i\left(\mathbf{p}_{-i}\right)$ are non empty, closed, convex, and contained in some compact set $\mathcal{C}_i$ for all $\mathbf{p}_{-i} \in \mathcal{P}_i\left(\mathbf{p}_{-i}\right) = \prod_{j\neq i} \mathcal{P}_j$.

— The set $\mathcal{P}_i(\mathbf{p}_{-i})$ vary continuously with p_i.

— Each user's payoff function $\tilde{U}_i(p_i, \mathbf{p}_{-i})$ is quasi-concave in p_i $\forall \mathbf{p}_{-i} \in \mathcal{P}_{-i}$.

In our setting, if condition (5.21) holds, then:

— The sets $\mathcal{P}_i(\mathbf{p}_{-i})$ are non-empty, closed convex, and bounded for every $\mathbf{p}_{-i}$.

— Each of the sets $\mathcal{P}_i(\mathbf{p}_{-i})$ and $\mathcal{P}_i(\mathbf{p}_{-i})$ vary continuously with $\mathbf{p}_{-i}$ since the interference constraint in $\mathcal{P}_{-k}$ is itself continuous in $\mathcal{P}_i(\mathbf{p}_{-i})$ and $\mathcal{P}_i(\mathbf{p}_{-i})$, respectively.

— $\tilde{U}_i^{col}(p_i, \mathbf{p}_{-i})$ is a concave function and consequently is a quasi-concave function.

Therefore, the game $\mathcal{G}_2$ admits to a nonempty set of NE points.

Next, according to [104], the game $\mathcal{G}_2$ is a nice and twice differentiable game since the utility function $\tilde{U}_i^{col}(p_i, \mathbf{p}_{-i}, z_i)$ is concave w.r.t p_i. Thus, if it satisfies the dominance solvability condition

$$-\frac{\partial^2 \tilde{U}_i^{col}(p_i, \mathbf{p}_{-i}, z_i)}{\partial p_i \partial p_i} \geq \sum_j \left| \frac{\partial^2 \tilde{U}_i^{col}(p_i, \mathbf{p}_{-i}, z_i)}{\partial p_i \partial p_j} \right| \forall i \in \mathcal{N} \tag{5.39}$$

then players follow the continuous best response dynamic [98], i.e., the NE point can be obtained by iteratively updating the transmit powers according to (5.32) from any starting point. The corresponding algorithm is reported in Algorithm 2. □

5.4.3 Assigning Approximation Points

The BRD algorithm is used to determine the NE of the game. Similar to the potential game approximation, by exchanging the information about the interference plus noise of each user, (5.32) can be obtained. BRD algorithm guarantees the convergence to a NE and the distributed implementation. However, in such games, the NE may not be unique and it depends on the starting points (*i.e.*, z_i) of the algorithm.

The utility function of player i, as well as the convergence of the game, depending on the initial point z_i ($i \in \mathcal{N}$) for the approximation process. The question on how to choose an efficient initial point must be considered. For a given $\mathbf{p}_{-i}$, the solution of (5.33) is an increasing function with the variable $z_i \geq 0$. The maximum value of $p^+(z_i)$ is

$$p^+(p_i^{\max}) = \frac{1}{c_i + \sum\limits_{j \neq i} \alpha_j \varphi_i(p_i^{\max})} - \sum_{j \neq i} \frac{g_{j,i}}{g_{i,i}} p_j - \frac{\sigma_i^2}{g_{i,i}} \tag{5.40}$$

The individual rate of each player is an increasing function with its own transmission power, but a decreasing function with others' powers. For the network in the low-SINR region, the individual rate of each player hence will be worse if the initial points are the maximum power. Instead of selecting the maximum power as the initial point for the approximation process, we claim that the zero points (*i.e.*, $z_i = 0$ $\forall i \in \mathcal{N}$) will be better for the network performance in term of the aggregate rate.

5.5 The Concave-Potential Game Approximation

For a network with the large number of transmitter-receiver pairs (i.e., N), the distributed implementation by iteratively solving N coupled problems (*i.e.*, the optimization problems (5.7)) as in the game $\mathcal{G}_1$ and $\mathcal{G}_2$ are more complex. In such a case, we adopt a hybrid approach, which is referred as the *concave-potential game*, to approximate the utility function of the games. In particular, we linearize the convex part in (5.5) as follows:

$$\bar{g}_i(p_i, \mathbf{p}_{-i}, z_i) \approx \hat{g}(z_i, \mathbf{p}_{-i}) + \bigtriangledown_{p_i} \hat{g}(p_i, \mathbf{p}_{-i})^T|_{p_i=z_i} (p_i - z_i) \tag{5.41}$$

The corresponding modified utility functions are then given by

$$\bar{U}_i (p_i, \mathbf{p}_{-i}, z_i) = \hat{f}_i(p_i) + \bar{g}_i(p_i, \mathbf{p}_{-i}, z_i). \tag{5.42}$$

where z_i is the initial point of the player i for the approximation process. We formulate the *concave-potential game* as:

$$\mathcal{G}_3 \triangleq \{\mathcal{N}, \{\mathcal{P}_i (\mathbf{p}_{-i})\}_i, \{\bar{U}_i (p_i, \mathbf{p}_{-i})\}_i\}. \tag{5.43}$$

Given the strategy $\mathbf{p}_{-i}$, the best response of user i for the game $\mathcal{G}_3$ is defined as

$$\bar{\mathcal{B}}_i (\mathbf{p}_{-i}) \triangleq \underset{p_i \in \mathcal{P}_i(\mathbf{p}_{-i})}{\arg\max} \bar{U}_i (p_i, \mathbf{p}_{-i}) . \tag{5.44}$$

5.5.1 Properties of the Concave-Potential Game

Some properties of the game $\mathcal{G}_3$ are as follows:

Lemma 5.9. *If condition* (5.21) *holds then* $\bar{\mathcal{B}}_i (\mathbf{p}_{-i})$ *takes the form*

$$\bar{\mathcal{B}}_{-i} (\mathbf{p}_{-i}) = \min\{p_i^{\max}, \max\{p_i^\star, p_i^{tar}\}\}, \tag{5.45}$$

wherein $p_i^{tar} (\mathbf{p}_{-i})$ *is defined as in* (5.23) *and*

$$p_i^\star \triangleq \underset{p_k \in \mathbb{R}^+}{\arg\max} \bar{U}_i (p_i, \mathbf{p}_{-i}) . \tag{5.46}$$

Proof. Please refer to Lemma 5.6. □

Lemma 5.10. *For a given* $\mathbf{p}_{-i}$*, the solution to* (5.46) *is founded to be*

$$p_i^\star = \frac{1}{c_i + \sum\limits_{j \neq i} \alpha_j \frac{g_{i,j}}{\ln(2)\left(g_{i,j} z_i + \sum\limits_{k \neq i,j} g_{k,j} p_j + \sigma_j^2\right)}} \tag{5.47}$$

Proof. In game $\mathcal{G}_3$, the utility function of player i is given by

$$\bar{U}_i(p_i, \mathbf{p}_{-i}, z_i) = \hat{f}(p_i) + \hat{g}(z_i) + \bigtriangledown_{p_i} \hat{g}(z_i)^T (p_i - z_i)$$

Since $\bar{U}_i(p_i, \mathbf{p}_{-i}, z_i)$ is a concave function with p_i, there are unique maximizer point $p_i^\star$ which is determined by

$$p_i^\star \triangleq \arg \max_{p_k \in +} \bar{U}_i (p_i, \mathbf{p}_{-i}, z_i) \tag{5.48}$$

$$\Rightarrow \qquad p_i^\star = \left(c_i + \sum_{j \neq i} \alpha_j \frac{g_{i,j}}{\ln 2 \left(g_{i,j} z_i + \sum\limits_{k \neq i,j} g_{k,j} p_k + \sigma_j^2 \right)} \right)^{-1} \tag{5.49}$$

□

5.5.2 Analysis of the Equilibria

The existence and uniqueness of the NE points of are now studied under the assumption that condition (5.21) holds.

Proposition 5.11. *The game $\mathcal{G}_3$ admits a nonempty set of NE points, which can be obtained by iteratively updating the transmit powers according to* (5.45) *from any starting point, respectively.*

Proof. In our setting, if condition (5.21) holds, then:

— The sets $\mathcal{P}_i (\mathbf{p}_{-i})$ are non-empty, closed convex, and bounded for every $\mathbf{p}_{-i}$.

— Each of the sets $\mathcal{P}_i (\mathbf{p}_{-i})$ and $\mathcal{P}_i (\mathbf{p}_{-i})$ varies continuously with $\mathbf{p}_{-i}$ since the SINR constraint in $\mathcal{P}_{-k}$ is itself continuous in $\mathcal{P}_i (\mathbf{p}_{-i})$ and $\mathcal{P}_i (\mathbf{p}_{-i})$, respectively.

— $\bar{U}_i (p_i, \mathbf{p}_{-i})$ and $\bar{U}_i (p_i, \mathbf{p}_{-i})$ are concave functions and thus are quasi-concave functions.

Therefore, these games admit to a nonempty set of NE points. □

The proof of the uniqueness of the NE builds upon the standard function framework [105], which states that a non-cooperative game admits a unique NE (reachable by iteratively computing the players' best-responses) provided that the game admits at least one equilibrium and the best-response function is a standard function, which is defined as follows:

Definition 5.12. A function $l(p)$ is a standard function if for all $p \geq 0$, the following properties are satisfied:

1. *Positivity*: $l(p) > 0$,
2. *Monotonicity*: If $p \geq p^{'}$ then $l(p) \geq l(p^{'})$,
3. *Scalability*: For all $\epsilon > 1$, $\epsilon l(p) > l(\epsilon p)$.

Proposition 5.13. *The game $\mathcal{G}_3$ admits a unique NE point, which can be obtained by iteratively updating the transmit powers according to* (5.45) *from any starting point.*

Proof. First, we prove that the game $\mathcal{G}_3$ admits a unique NE point by proving that the best-response function (5.45) is a standard function as follows. We first consider the function $p_i^{tar}(\mathbf{p}_i)$:

— *Positivity*: $p_i^{tar}(\mathbf{p}_{-i}) > 0$

— *Monotonicity*: $p_i^{tar}(\mathbf{p}_{-i})$ is increasing in all $\{p_j\}_{j\neq i}$.

— *Scalability*: take any $\omega > 1$ then it holds

$$p_i^{tar}(\omega\mathbf{p}_{-i}) = \omega\frac{\gamma_i^{tar}}{g_{i,i}}\left(\sum_{j\neq i} g_{j,i}p_j + \frac{\sigma_i^2}{\omega}\right) < \omega p_i^{tar}(\mathbf{p}_{-i}).$$

Thus, $p_i^{tar}(\mathbf{p}_i)$ is a standard function. Next, we prove that $p_i^{\star}(\mathbf{p}_i)$ is a standard function as followings:

— *Positivity*: $p_i^{\star}(\mathbf{p}_{-i}) > 0$

— *Monotonicity*: $p_i^{\star}(\mathbf{p}_{-i})$ is increasing in all $\{p_j\}_{j\neq i}$.
If $\mathbf{p}_{-i}^{+} \geq \mathbf{p}_{-i}^{++}$ then

$$p_i^{\star}\left(\mathbf{p}_{-i}^{+}\right) = \frac{1}{c_i + \sum\limits_{j\neq i}\alpha_j \frac{g_{i,j}}{\ln 2\left(g_{i,j}z_i + \sum\limits_{k\neq i,j} g_{k,j}p_k^{+} + \sigma_j^2\right)}} > p_i^{\star}\left(\mathbf{p}_{-i}^{++}\right).$$

— *Scalability*: take any $\varepsilon > 1$ then it holds

$$\varepsilon p_i^{\star} = \frac{1}{\frac{c_i}{\varepsilon} + \sum\limits_{j\neq i}\alpha_j \frac{g_{i,j}}{\ln 2\left(\varepsilon g_{i,j}z_i + \sum\limits_{k\neq i,j} \varepsilon g_{k,j}p_k + \varepsilon\sigma_j^2\right)}} > p_i^{*}(\varepsilon\mathbf{p}_{-i})$$

Therefore, $p_i^{\star}(\mathbf{p}_i)$ is a standard function. Since $p_i^{\max}$ does not depend on $\mathbf{p}_{-i}$ and $\max(\cdot)$ and $\min(\cdot)$ are increasing functions, we conclude that the best response function $\bar{\mathcal{B}}_{-i}(\mathbf{p}_{-i})$ is also a standard function with variable p_i. □

5.5.3 Assigning Approximation Points

The BRD algorithm is adopted to determine the NE pont of $\mathcal{G}_3$. Similar to the game $\mathcal{G}_1$ and $\mathcal{G}_2$, by exchanging the information about the interference between SUs, (5.45) can be obtained. BRD algorithm then guarantees the convergence to a (unique) NE.

The utility function of each player in game $\mathcal{G}_3$ depend on the initial points for the approximation process. We observed that the value of $p^{\star}(z_i)$ in (5.46) only depend on the interference plus noise of other users and the initial point. We observe that, for a given $\mathbf{p}_{-i}$,

TABLE 5.1 Wireless network simulation parameters

Parameter	**Value**
Antenna configuration	1×1
Cell size (rectangular)	500 m
Central frequency	2.1 GHz
Spectral noise density (20^0C)	- 174 dBm/Hz
Maximum transmit power	$p^{\max} = 20$ dBm
SINR constrain	$\gamma_i^{tar} = -5$dB
Monte Carlo realizations	1000

$p^{\star}(z_i)$ is an increasing function with the variable $z_i \geq 0 \in$. The maximum value of $p_i^{\star,\max}$ is

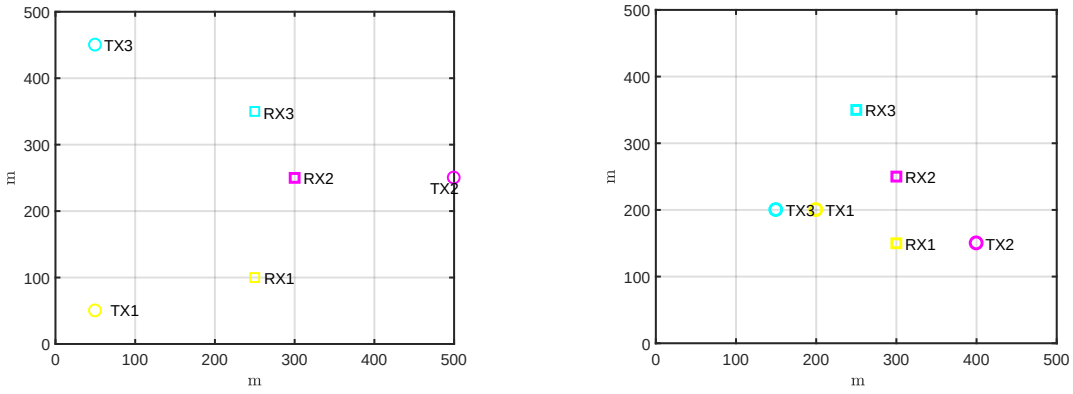
$$p_i^{\star,\max} = \left(c_i + \sum_{j \neq i} \alpha_j \frac{g_{i,j}}{\ln 2 \left(g_{i,j} p_i^{\max} + \sum\limits_{k \neq i,j} g_{k,j} p_k + \sigma_j^2 \right)} \right)^{-1} \tag{5.50}$$

The individual rate of each player is an increasing function with its own transmission power, but a decreasing function with others' powers. For the network with large number of users, the rate of each player will be worse if the initial points are the maximum power. Instead of selecting the maximum power as the approximation point, we claim that the zero points (*i.e.*, $z_i = 0 \ \forall i \in \mathcal{N}$) will be better for the network performance in term of the aggregate rate.

5.6 Simulation Results

To validate the performance of collaborative power control in the wireless interference networks, two scenarios are considered: i) the network in the high-SINR region (i.e., the users are far apart), and ii) the network in the low-SINR region (otherwise). To make the simulation results clear and easy to follow, we start with a CRN with $N = 3$ SUs. The simulation scenarios are illustrated as in Figure 5.3a and 5.3b, respectively. For comparison purposes, we use the fairness between the individual rate of each user and the aggregate rate of the network obtained by considering the collaborative power control, the distributed power control with BRD algorithm [33, 62], and the centralized power control with branch-and-bound algorithm [41] [1]. These algorithms will stop if the total tolerance between two consecutive power allocations (or between the upper-bound and the lower-bound of the weighted sum-rate) is smaller than $\epsilon = 10^{-6}$. Note that the cost factor, $c_i = 0.01 \ \forall i \in \mathcal{N}$, is

1. In the centralized power allocation, we take into account the problem of maximization of the aggregate performance (i.e., the sum of $f_i(p_i, \mathbf{p}_{-i})$). Brand-and-bound algorithm is considered as an efficient method to tackle two classes of problems, the minimization of the total transmit power and the maximization of data throughput [41]. Hence, we adopts this algorithm to determine the centralized power allocation strategy.



(A) High-SINR scenario (B) Low-SINR scenario

FIGURE 5.3 The simulation scenarios with $N = 3$ SUs.

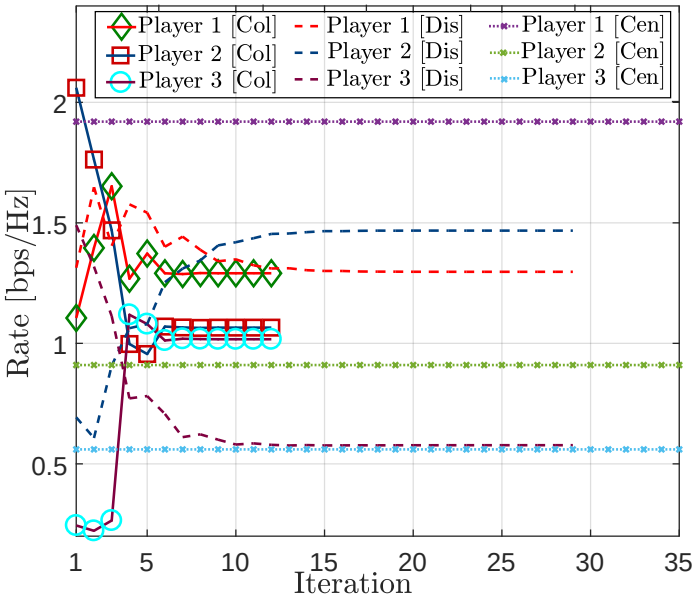


FIGURE 5.4 The rate of each CR user with the collaborative power allocation based on the potentialized game, the distributed power control, and the centralized power control for the CR network with high SINR region where $\alpha_i = 1/3\ \forall i = 1, 2, 3$.

chosen to back off the user's transmission power instead of transmit at its maximum. Other parameters are in Table 5.1.

The fairness among users is quantitatively evaluated by using the Jain's fairness index [106]. For the power control problem, the fairness index in term of rate for the power control profile $\mathbf{p}$ is defined as:

$$f(\mathbf{p}) = \frac{\left[\sum_{i=1}^{N} r_i(\mathbf{p})\right]^2}{N \sum_{i=1}^{N} r_i^2(\mathbf{p})} \tag{5.51}$$

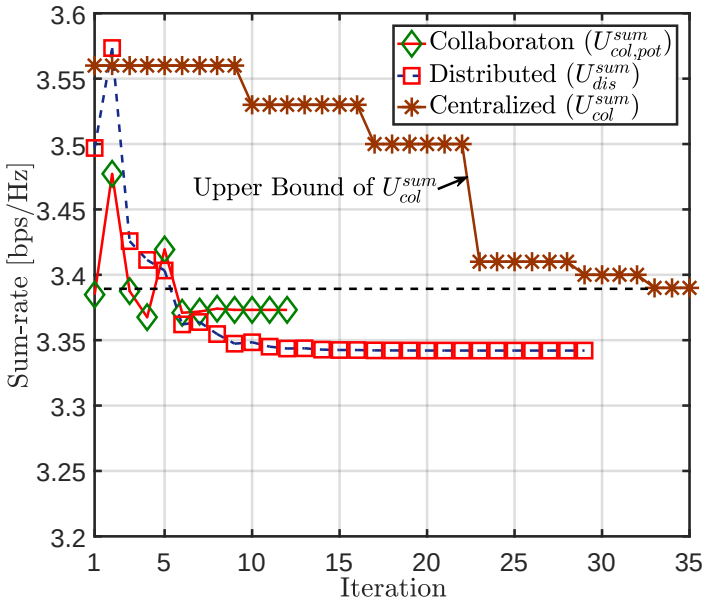


FIGURE 5.5 The sum-rate of the network with the collaborative power allocation based on the potentialized game, the distributed power control, and the centralized power control for the CR network with high SINR region where $\alpha_i = 1/3\ \forall i = 1, 2, 3$.

The Potential Game Approximation

First, we consider the CR network in the high-SINR region. The potentialized game approach is adopted to determine the optimal collaborative power allocation. The collaboration factors are $\alpha_i = 1/3$ $(i = 1, 2, 3)$ [2]. Figure 5.4 shows the rates, which are obtained by the collaborative power control paradigm, are more fair than the distributed and the centralized approaches. For the collaborative power allocation, the fairness index is 0.989, which is much higher than the distributed power allocation (0.893) and the centralized power allocation (0.793). Next, Figure 5.5 indicates that the sum-rate of the network by following the collaborative power control paradigm outperforms the distributed one and is close to the centralized one. The reason is that each player aims to improve not only its own rate (*i.e.*, through the (approximated) performance metric) but also the others' rate (*i.e.*, through the (approximated) collaboration metric). Hence, the sum-rate of the network is higher than the one in distributed power control. Moreover, since the game is an exact potential game with strictly concave potential function, fewer iterations are required to converge to the NE point. We, therefore, conclude that the collaborative power control paradigm provides better fairness between users, higher performance and lower convergence time.

Figure 5.6 shows the influence of the collaboration factors to the network performance in term of the sum-rate. We fix the collaboration factor of user 1 (α_1) and change that of other

2. We first take the same collaboration factor between all users such that $\sum \alpha_i \leq 1$, *i.e.*, $\alpha_i = 1/3$, $i = 1, 2, 3$.

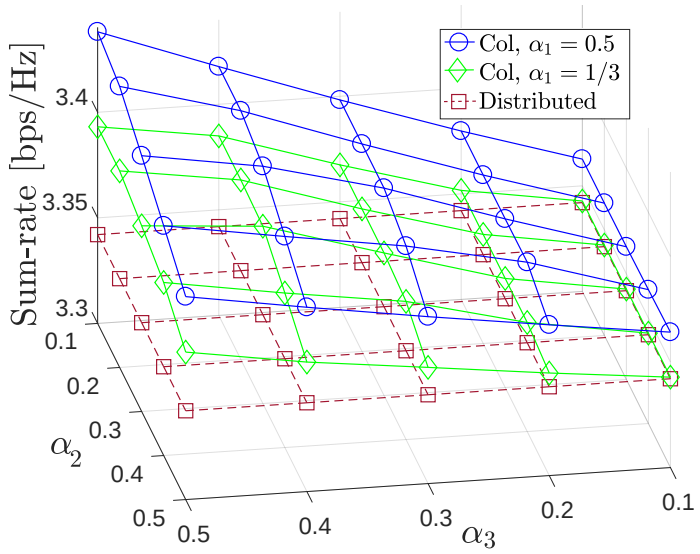


FIGURE 5.6 The performances of the collaborative power allocation based on the potentialized game approach for varying collaboration factors.

users while ensuring the SINR condition. We observe that the sum-rate of the collaborative power control is higher than the distributed one. Moreover, it reaches its maximum if the collaboration factors are $(0.5,\ 0.1,\ 0.5)$. In the simulation scenario (Figure 5.3a), the distance between the transmitter and the receiver of user 2 is lower than the one of other users. In addition, the distance between the user transmitters of other users to the receiver of user 2 is larger than the others. It means, with the same transmission power, the SINR of user 2 is higher than the ones of user 1 and 3. We claim that, in the high SINR scenario, the higher the SINR the smaller the collaboration factor. In addition, we conclude that the sum-rate of the system strongly depends on the collaboration factors.

The Concave Game Approximation

We next consider the wireless interference network in the low-SINR region. The concave game approach is adopted to determine the optimal collaborative power allocation. The collaboration factors are $\alpha_i = 1/3$, $(i = 1, 2, 3)$. In order to simplify the problem, we suppose that the initial points for the approximation process are zero, *i.e.*, $z_i = 0$, $\forall i$. Figure 5.7 shows the rates, which are obtained by the collaborative, the distributed and the centralized power control approaches. The fairness index are 0.72, 0.84 and 0.67, respectively. It means the collaborative one is fairer in term of the achievable rate than the centralized one but less than the distributed one. For the initial points $z_1 = 1.5935$ dBm, $z_2 = 1.8166$ dBm, and $z_3 = 1.2335$ dBm, the fairness index of collaborative power control is $f(\mathbf{p}) = 0.92$, which is much higher than the other power control approaches. Moreover, for both cases, the collaborative power control provides a faster convergence rate than others approaches.

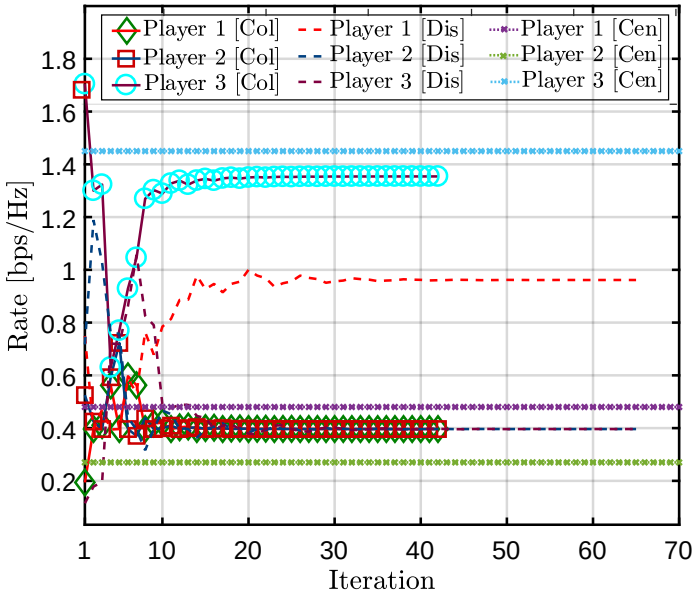


FIGURE 5.7 The rate of CR users with the collaborative power allocation based on the concave game approach, the distributed power control, and the centralized power control for the CR network with low SINR region where $\alpha_i = 1/3\ \forall i = 1, 2, 3$.

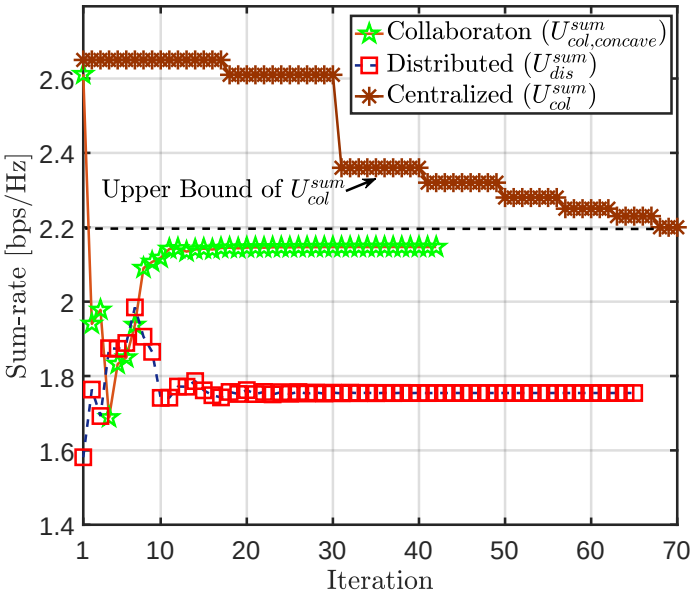


FIGURE 5.8 The sum-rate of the network with the collaborative power allocation based on the concave game approach, the distributed power control, and the centralized power control for the CR network with low SINR region where $\alpha_i = 1/3\ \forall i = 1, 2, 3$.

Figure 5.8 indicates that the sum-rate of the network by following the collaborative power control outperforms the distributed one and is close to the joint optimization one. Figure 5.9 shows the impact of the collaboration factor on the network performance by fixing the collaboration factor of user 1 and changing the collaboration factors of other users. We

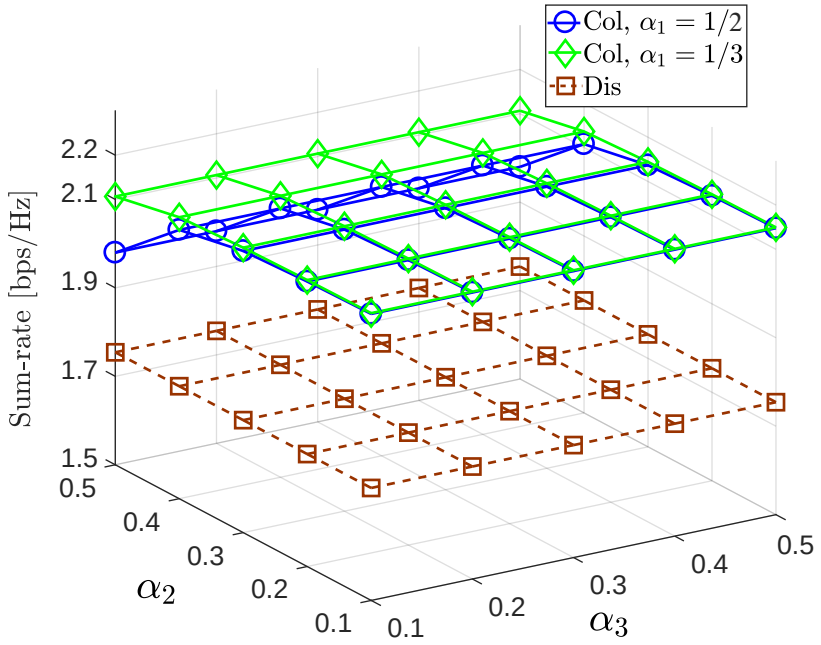


FIGURE 5.9 The performance of the collaborative power allocation based on the concave game approach for varying collaboration factors.

observed that the sum-rate in the collaboration scheme is always higher than the distributed one and gets maximal when the collaboration factors are $(1/3, 0.1, 0.1)$. In the simulation scenario (Figure 5.3b), the transmitter of user 1 influences more to the other receivers in term of interference. We claim that, in the low SINR scenario, the user with more influence will choose the higher collaboration factor. In addition, the collaboration factor will smaller than the one in the high SINR scenario. We conclude that the sum-rate of the system strongly depends on the collaboration factors.

Figure 5.10 shows the sum-rate of the system as well as the number of iterations to reach the NE for varying initial points. We observed that the best initial point in terms of both sum-rate and convergence rate is $z_i = 0 \; \forall i$. Moreover, the sum-rate in the collaborative power allocation is greater than or equal to the one in the distributed power allocation scheme. Interestingly, if the initial points are the maximum power or the NE of the distributed power allocation, the sum-rate in the collaborative power allocation scheme closes to the one in the distribution power allocation case. We conclude that the selection of zero points for the approximation process will be most beneficial when investigating the collaborative power allocation based on the concave game framework.

The Concave-Potential Game Approximation

Finally, for the network with a large number of users, we employed the collaborative power control based on the concave-potential game approach. A wireless interference network

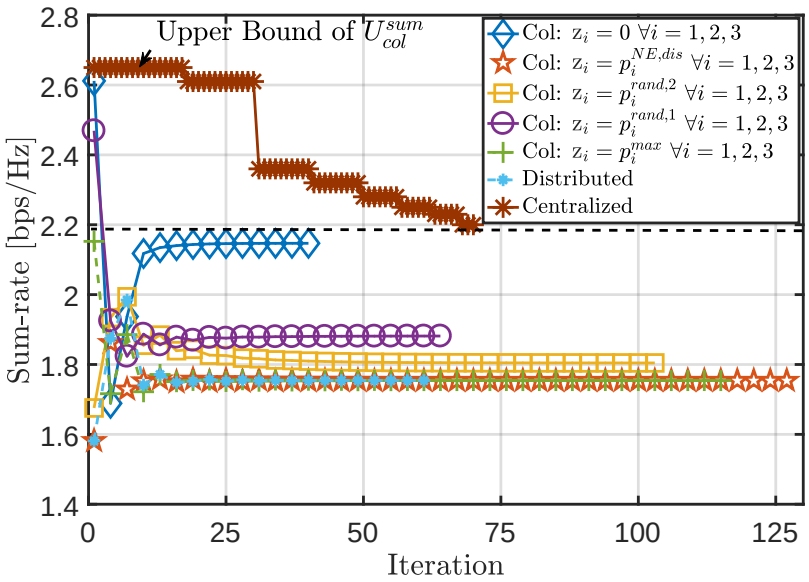


FIGURE 5.10 The sum-rate of the CR network obtaining by employing the collaborative power allocation based on the concave game framework for some initial points z_i.

with $N = 5$ users is considered, where the initial points for the approximation process are (i) zero, and (ii) the maximum power, respectively. Figure 5.11 shows the sum-rate of the network for the collaboration factors $\alpha_i = 1/5\ \forall i \in \mathcal{N}$. We observe that, by considering the collaborative power control based on the concave-potential game approach, the obtained sum-rate is higher than the one obtained by the distributed power control and is close to the one obtained by the centralized power control. Moreover, its convergence rate is much faster than otherwise. The reason is that we can directly find the best response through an analytical solution (5.47). Also, we observed that, for the collaborative power control based on the concave-potential game approach, the selection of the minimum points for the approximation process provides a better sum-rate. In contrast, the selection of the maximum power for the approximation process provides a better convergence rate.

Finally, we compare the convergence rate of the collaborative power allocation based on the concave-potential game framework with the conventional power allocation approaches. Table 5.2 shows the number of iterations which is used by the algorithms (BRD and branch-and-bound) to determine the power allocation strategy. The maximum power is chosen as the initial point for the approximation process. We observe that the collaborative power control outperforms the other approaches in term of convergence rate. We conclude that, for the large network, it will be better to adopt the concave-potential game approximation approach. Otherwise, we adopt the potential game approach for the network with the high-SINR region and the concave game approach for the network with the low-SINR region.

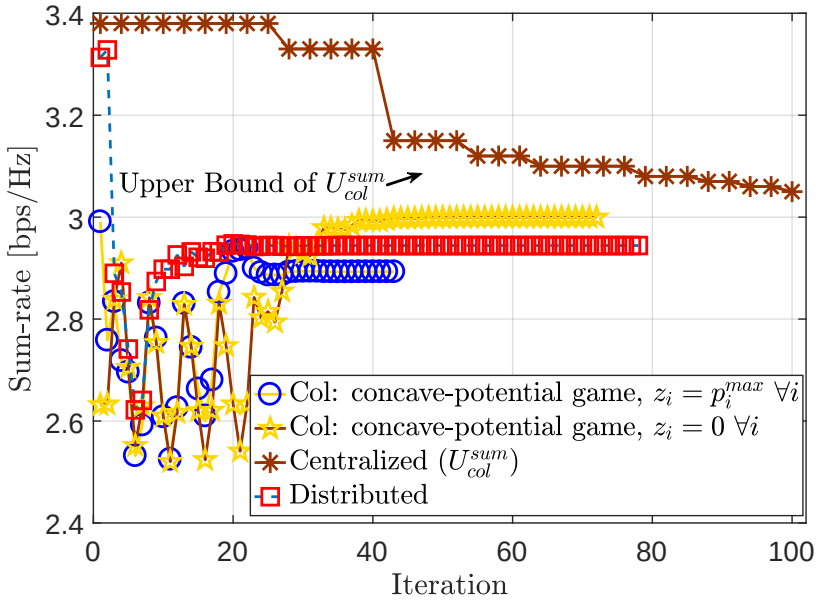


FIGURE 5.11 The sum-rate of the CR network with $N = 5$ users obtaining by using the collaborative power allocation strategy based on the concave-potential game framework.

TABLE 5.2 The average number of iterations which is used by BRD/branch-and-bound algorithm to determine the power allocation strategy in: (*left*) the distributed strategy, (*middle*) the collaborative strategy based on the concave-potential game, and (*right*) the joint optimization strategy.

	$N = 3$			$N = 5$			$N = 7$			$N = 9$		
Low Interference	29	**9**	35	46	**25**	61	113	**45**	133	225	**77**	203
High Interference	65	**14**	70	79	**43**	103	301	**85**	286	597	**151**	488

5.7 Concluding Remarks

This chapter examined the problem of coexistence between cognitive users in the distributed based-CR networks. The collaborative resource allocation problem, in particular, the collaborative power allocation problem, is proposed to ensure the coexistence between SUs while ensuring the quality of service constraint of the primary user or the network users. Under the collaborative scheme, the power allocation problem was shown to be nonconcave. The chapter then proposes three solution approaches, namely potential game approximation, concave game approximation and the concave-potential game approximation, to approximate and transform the original nonconcave problem into convex optimization ones. In the potential game approximation approach, for the CR network in the high SINR region, the nonconcave optimization problem is approximated by a potential game. The existence of NE is then proven by using the characteristics of the potential game. In the concave game approximation approach, for the CR network in the low SINR region, the nonconcave optimization problem is approximated by a concave game. The concave-potential game

approximation approach is then adopted to approximate the CR network with a large number of users. Simulations confirmed the convergence analysis of the proposed algorithms and showed a significant enhancement in the network sum-rate, the fairness in term of individual rate and the convergence time as compared to competitive design.

Chapter 6

Conclusion and Future Works

6.1 Summary

Maintaining a harmonized coexistence between the network users has been a critical issue for current and future dynamics spectrum access-based communication systems like cognitive radio networks. The question on how to share the spectrum fairly for multiple users in overlapping coverage areas while mitigating the influence of the attack raised by the misbehaving users is a particularly important challenge that needs to be addressed. This thesis has been concerned with the deployment of the self-coexistence mechanism between the cognitive radio users under two network architectures: centralized and distributed. Specifically, to ensure the coexistence among SUs, we have proposed the surveillance processes to mitigate the influence of the misbehaving user in the centralized CR networks. In addition, we have also presented the collaborative resource allocation strategy to allocate the radio resources between the network users in the distributed CR networks.

Chapter 3 has considered the coexistence mechanism between SUs in the spectrum-sensing based CR networks through the surveillance process to deal with the PUEA. Via the game theory framework, we have formulated the relationship between the multi-channel PUEA and the surveillance process as an extensive-form game and determined the efficient surveillance strategy for the network coordinator through the NE of the game. To improve the efficiency of the surveillance strategy, we have taken into account the leadership and commitment in the game model in which the network coordinator leverage its position of leader by committing to a defense strategy and forcing the attacker as the follower to plays its best response regarding the observed surveillance strategy. Generally, numerical results have shown a significant improvement in terms of the network coordinator's performance and the computational time by the following the leadership and commitment model.

Chapter 4 has studied the coexistence mechanism between SUs in the database-driven based CR networks by considering the verification processes to deal with the location and ID spoofing attack. Using the game theory framework, we have formulated the relationship

between the location spoofing attack and the requests' location verification as a strategic-form game and the relationship between the data identification and the ID spoofing attack as an extensive-form game. We have examined the corresponding attack and verification strategy of the attacker and the network coordinator through the NE strategy of the corresponding game. A closed-form solution is shown for the location verification game while the sequence-form representation method is adopted to solve the ID verification game. The simulation results have shown the influence of penalty policies on the verification strategies of the defender.

In chapter 5, we have studied the resource allocation process to ensure the coexistence between the cognitive users in the distributed-based CR networks. Specifically, we have proposed a collaborative power allocation framework where each user optimizes its power strategy by collaborating with others and formulate these relationships as a strategic game. Since the collaborative resource allocation is nonconcave, obtaining its globally optimal solution is rather computationally complex. Consider the example of the power allocation problem; we have then proposed a low-complexity method for efficiently solving this issue by approximating the utility function of the game for each region on SINR of the network to obtain a well-known game. We have examined the conditions on the existence and uniqueness of a stable NE strategy in these games. Distributed implementation to the approximated games has also been presented in the chapter. The simulation results have confirmed the superior of the collaborative resource allocation approach in term of performance, convergence time, as well as the fairness of the system.

6.2 Potential Future Works

The research presented in this thesis has examined only a small tip of the iceberg on self-coexistence problems for the CR networks. There are avenues for further research to refine and improve the coexistence mechanism in the practical implementation of CR networks.

1. *Surveillance-based defense mechanism prototyping and testing:* Based on the current results on the surveillance process to mitigate the PUEA in the spectrum-sensing based CR networks, it will be interesting to set up a testbed of a practical CR system with different types of devices, *e.g.*, the PUs and the SUs, and different types of the attacker's behavior, *e.g.*, selfish or malicious. The testbed would help for testing not only the surveillance process but also the proposed collaborative resource allocation scheme in CR networks.

2. *Learning-based defense mechanism for mitigating PUEA:* The current surveillance processes to mitigate the influence of PUEA in the spectrum-sensing based CR networks comes in the sense that the attacker and the network coordinator performs the PUEA/surveillance process at each time slot. The new research question on the long-time attack/surveillance strategy in which the network coordinator monitors the

frequency bands and learn to adapt to the changes of primary user signal and the PUEA. The similar question must be considered for the case of database-driven CR networks. Certainly, it will be interesting to investigate the corresponding surveillance/verification strategy in such a case.

3. *Online learning scheme for collaborative resource allocation in CR networks:* In Chapter 5, we have investigated the collaborative power allocation between cognitive users in the distributed-based CR networks. Extension of the collaborative resource allocation scheme in the scenario of multiple networks sharing common frequency bands is also an interesting research direction. In addition, due to the unpredictable behavior of the network users and the complex multi-part fading environments, a static solution is no longer relevant. Certainly, it will be interesting to further investigate the collaborative power allocation strategy by online learning scheme, which allows users/networks to adapt to changes in the wireless environment, quickly and efficiently.

Appendix A

A Brief Overview of Game Theory

Game theory is a brand of mathematics studying the conflict and cooperation between the rational decision-makers [50, 87, 107]. The purpose of game theory is to model and understand the strategic interaction between competing players. Game theory is mainly applied in economics, political science, and psychology, as well as logic, computer science and biology. Recently, game theory is successfully adopted for solving problems in various engineering fields, including signal processing, information, and communication theories [108]. As communication networks become more intelligent and self-organized, many communication problems can be naturally formulated as a game between the rational network entities. This thesis, aims to the study the interaction between the bab behavior user and the network manager in the coordinated network as well as the collaboration behavior of the users in the uncoordinated network, relies on game theory in the modeling and studying the interaction between the user-the network manager and between the users. The aim of this appendix is to present a brief overview of game theory and review the theory behind the games studied in this thesis.

A.1 Game Formulation and Nash Equilibrium

Let $\Omega = \{1, 2, \ldots, Q\}$ denotes the set of Q players and $\mathcal{S}_q$ denote the set of admissible strategies of player-q. Let $s_q \in \mathcal{S}_q$ be a (pure) strategy of player-q and $\mathbf{s}_{-q}$ be a strategy profile of other players, except player-q. Collectively, let $(s_q, \mathbf{s}_{-q}) \in \mathcal{S} \stackrel{\Delta}{=} \prod_{q=1}^{Q} \mathcal{S}_q$. The aim of player-$q$, given other player's strategies, is to choose a strategy that maximizes his payoff function $u_q(s_q, \mathbf{s}_{-q})$, i.e.,

$$\begin{aligned} \underset{s_q}{\text{maximize}} \quad & u_q(s_q, \mathbf{s}_{-q}) \\ \text{subject to} \quad & s_q \in \mathcal{S}_q. \end{aligned} \tag{A.1}$$

Such optimal strategy is termed as the *best response* strategy.

Mathematically, a generic game $\mathcal{G}$ can be defined as

$$\mathcal{G} = (\Omega, \{\mathcal{S}_q\}_{q\in\Omega}, \{u_q\}_{q\in\Omega}) . \tag{A.2}$$

Definition A.1. *A strategy profile* $\mathbf{s}^\star = \left(s_q^\star, \mathbf{s}_q^\star\right)$ *constitutes a (pure) Nash Equilibrium of game* $\mathcal{G}$ *when*

$$u_q\left(s_q^\star, \mathbf{s}_{-q}^\star\right) \geq u_q\left(s_q, \mathbf{s}_{-q}^\star\right), \quad \forall q \in \mathcal{S}_q, \forall q \in \Omega. \tag{A.3}$$

NE is an important concept in game theory to analyze the outcome of the strategic interaction between the rational players. In particular, the analysis of NE characterizes the stable operating point of the game where each player has no incentive to unilaterally change its strategy, i.e., given other players' strategies, one player cannot improve its own utility at a NE. The definition of the pure NE can be also generalized to contain mixed strategies, i.e., the possibility of choosing a set of pure strategies by each player. Given $\mathcal{S}_q$, a mixed-strategy ρ_q is a probability distribution over $\mathcal{S}_q$. Let ρ_{-q} denotes the mixed-strategy profile of other players, except player-q and Δ_q denotes the set of all probability distributions over $\mathcal{S}_q$. Collectively, let $\Delta = \prod_{q=1}^{Q} \Delta_q$.

Definition A.2. *A mixed strategy profile* $\rho^\star = \left(\rho_q^\star, \rho_{-q}^\star\right)$ *constitutes a mixed Nash Equilibrium of game* $\mathcal{G}$ *when*

$$u_q\left(\rho_q^\star, \rho_{-q}^\star\right) \geq u_q\left(\rho_q, \rho_{-q}^\star\right), \quad \forall \rho_q \in \Delta_q, \forall q \in \Omega. \tag{A.4}$$

Obtaining a NE state is often the ultimate objective in a game. Hence, analyze equilibrium properties of games, i.e., the existence and the uniqueness of equilibrium point is an important problem. The existence of NE in a game is started by the work of Nash [61], which proved that every finite strategy game has a NE in mixed strategies, and then by the work of Debreu [103], Fan [109] and Glicksberg [110] for certain classes of games as follows.

Theorem A.3. *A game* $\mathcal{G}$ *has a pure-strategy Nash equilibrium if for all* $q \in \Omega$*, the strategy set* $\mathcal{S}_q$ *is a nonempty, convex and compact subset of a Euclidean space, and the utility function* u_q *is continuous and quasi-concave in each* $\mathcal{S}_q$*.*

Proof. Please refer to [81], pp. 34. □

Theorem A.4. *A game* $\mathcal{G}$ *has a mixed-strategy Nash equilibrium if for all all* $q \in \Omega$*, the strategy set* $\mathcal{S}_q$ *is a nonempty compact subset of a metric space and the utility function* u_q *is continuous.*

Proof. Please refer to [81], pp. 36. □

A.2 Game Representation

When the game is presumed that each player acts simultaneously or, at least, without knowing the actions of the other, the strategic form representation is used to represented by a

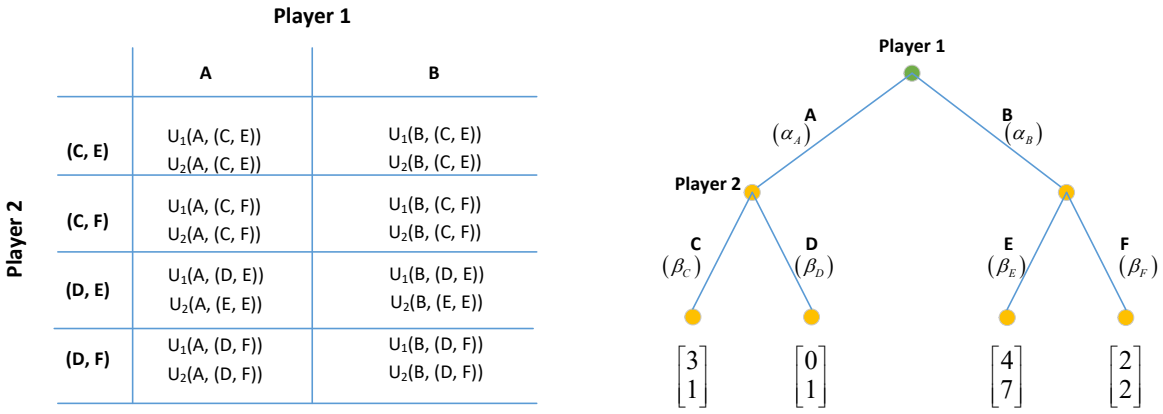


FIGURE A.1 Two representations of a sequential move game with 2 players: (left), the strategic form, (right) the extensive form.

matrix which shows the players, strategies, and payoffs. More generally it can be represented by any function that associates a payoff for each player with every possible combination of actions.

For the sequential move game in which players have some information about the choices of other players, the extensive-form representation is usually used. Specifically, the game is represented by a game tree, where each vertex (or node) represents a point of choice for a player or a change move. The player is specified by a number listed by the vertex, called sequence strategy. The lines out of the vertex represent a possible action for that player. The payoffs are specified at the bottom of the tree (or the terminal node). Nevertheless, the extensive-form representation can also capture simultaneous-move games and games with imperfect information. Notice that the strategic form representation can use to present the sequential move game, but may result in an exponential blowup in the size of the representation, making it computationally impractical. For example, we consider two representation methods for a sequential move game as shown in the figure below. There are two players in this game: player 1 and player 2. Player 1 can choose to play A or B. If player 1 plays A, player 2 can choose one of two actions C or D. If player 1 plays B, player 2 can choose one of two actions E or F. Hence, the strategic form representation lead to four combination strategies of player 2: (C, E), (C, F), (D, E) and (D, F). It means, by adopting the strategic form representation method, there are total 8 strategies pairs in the game. However, by adopting the extensive form representation method, there are only 4 strategy pairs, which correspond to 4 terminal node of the game tree.

The extensive-form representation approach can reduce the size of the representation of a game, but it is not a straight method to determine the NE. A slightly modified representation, namely the sequential-form representation, is proposed to determine the NE of a game by considering the sequential move of each player in the game tree. Set $\emptyset$ denote the action at root nodes (i.e., $\Pr(\emptyset) = 1$). The sequential strategy set of a player is defined as the set of its

sequential actions from root to the terminal node. The relation between the corresponding probabilities of these sequence strategy is called the *realization plan*. By default, for a root sequence, the probability is 1. For any node, the probability of sequential strategy at this node is the sum of all mixed strategies from this. For example, in the game illustrated in Figure A.1, the sequence strategy of player 1 is $\{\emptyset, A, B\}$ and the sequence strategy of player 2 is $\{\emptyset, C, D, E, F\}$.

Let $(\alpha_\emptyset, \alpha_A, \alpha_B)$ be the probability of each sequence in the sequence strategy set of player 1 and $(\beta_\emptyset, \beta_C, \beta_D, \beta_E, \beta_F)$ be the probability of each sequence in the sequence strategy set of player 2. The relation plan of these probabilities is given by

$$\begin{cases} \alpha(\emptyset) = 1, \\ \alpha(A) + \alpha(B) = \alpha(\emptyset), \\ 0 \le \alpha(A) \le 1 \\ 0 \le \alpha(B) \le 1, \end{cases} \quad \text{and} \quad \begin{cases} \alpha(\emptyset) = 1, \\ \alpha(C) + \alpha(D) = \alpha(\emptyset), \\ \alpha(E) + \alpha(F) = \alpha(\emptyset), \\ 0 \le \alpha(C), \alpha(D) \le 1 \\ 0 \le \alpha(E), \alpha(F) \le 1, \end{cases} \tag{A.5}$$

or in the matrix form as

$$\begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha(\emptyset) \\ \alpha(A) \\ \alpha(B) \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 1 & 0 & 0 \\ -1 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} \alpha(\emptyset) \\ \alpha(C) \\ \alpha(D) \\ \alpha(E) \\ \alpha(F) \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}. \tag{A.6}$$

The payoff matrix of the game then can be rewritten in the sequential-form as follows.

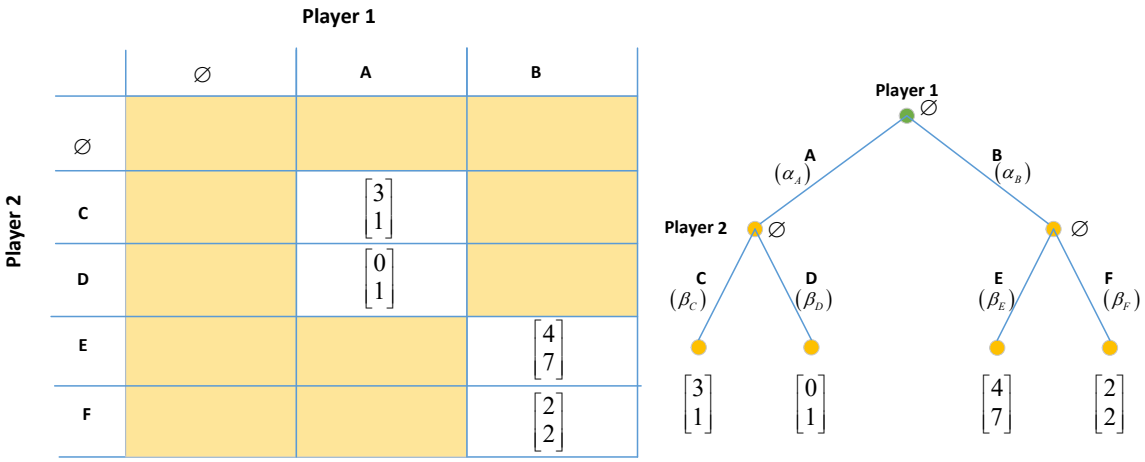


FIGURE A.2 The payoff matrix of the sequential-form representation method.

In general, the NE strategy of the game represented by the sequential-form representation can be found by solving the Linear Complementary Problem (LCP) [88] through the *Lemke algorithm* [79, 88, 89]. The original work on sequence-form game representation [79] has proved that the algorithm terminates with at least one solution in an acceptable time. For more details on the LCP, please refer to Appendix B.

A.3 Some Basic Games

Stackelberg Game

Typically, the NE has investigated in such a game that players move simultaneously. For such a game that players move sequentially, one other important concept is Strong Stackelberg Equilibrium (SSE), which is used to analyze the Stackelberg leader-follower model. A generic Stackelberg model has two players, a leader which moves first, and a follower which observes the leader's strategy and moves sequentially. Let $s_l \in \mathcal{S}_l$ be a (pure) strategy of the leader and $s_f \in \mathcal{S}_f$ be a strategy profile of the follower. Collectively, let $(s_l, s_f) \in \mathcal{S} \overset{\Delta}{=} \mathcal{S}_l \times \mathcal{S}_f$. The aim of the follower is to choose a best response strategy that maximizes his payoff function $u_f(s_l, s_f)$ regarding the leader's strategy, i.e.,

Definition A.5. *A strategy profile* $\mathbf{s}^\star = \left(s_f^\star(s_l^\star), s_l^\star\right)$ *constitutes a Strong Stackelberg Equilibrium (SSE) if it satisfies the following:*

1. *The follower plays a best response*

$$u_f\left(s_f^\star(s_l^\star), s_l^\star\right) \geq u_f\left(s_f^{'}, s_f^\star\right) \quad \forall s_f^{'} \in \mathcal{S}_f$$

2. *The leader plays a best response*

$$u_l\left(s_f^\star(s_l^\star), s_l^\star\right) \geq u_l\left(s_f^\star(s_l^{'}), s_l^{'}\right) \quad \forall s_l^{'} \in \mathcal{S}_l$$

3. *If the follower has the choice of best response, then it advantages the leader*

$$u_l\left(s_f^\star(s_l^\star), s_l^\star\right) \geq u_l\left(s_f^{'}, s_l^\star\right) \quad \forall s_f^{'} \in \Delta_F^*(s_l)$$

where $s_f^\star(\cdot)$ *denotes the follower's response function and* $\Delta_F^*(s_l)$ *denotes the set of the follower's best responses to* s_l*.*

Potential Game

Another important concept to analyze equilibrium properties of games is the potential game [33, 111, 112]. In game theory, a game is said to be a potential game if the incentive of all players to change their strategy can be expressed using a single global function called the *potential function.*

Definition A.6. *A game* $\mathcal{G} = (\Omega, \{\mathcal{S}_q\}_{q\in\Omega}, \{u_q\}_{q\in\Omega})$ *is*

— *an* ***exact potential game*** *if there is a function* $\Phi : \mathcal{S} \to \mathbb{R}$ *such that*

$$\Phi_q\left(s_q^{'}, \mathbf{s}_{-q}\right) - \Phi_q\left(s_q^{''}, \mathbf{s}_{-q}\right) = u_q\left(s_q^{'}, \mathbf{s}_{-q}\right) - u_q\left(s_q^{''}, \mathbf{s}_{-q}\right) \quad \forall \mathbf{s}_{-q}, \forall s_q^{'}, s_q^{''} \in \mathcal{S}_q, \tag{A.7}$$

— *a* ***weighted potential game*** *if there is a function* $\Phi : \mathcal{S} \to \mathbb{R}$ *and a vector* $\mathbf{w} \in \mathbb{R}_+$ *such that*

$$\Phi_q\left(s_q^{'}, \mathbf{s}_{-q}\right) - \Phi_q\left(s_q^{''}, \mathbf{s}_{-q}\right) = w_q\left(u_q\left(s_q^{'}, \mathbf{s}_{-q}\right) - u_q\left(s_q^{''}, \mathbf{s}_{-q}\right)\right) \quad \forall \mathbf{s}_{-q}, \forall s_q^{'}, s_q^{''} \in \mathcal{S}_q, \tag{A.8}$$

— *an* ***ordinal potential game*** *if there is a function* $\Phi : \mathcal{S} \to \mathbb{R}$ *such that*

$$\Phi_q\left(s_q^{'}, \mathbf{s}_{-q}\right) - \Phi_q\left(s_q^{''}, \mathbf{s}_{-q}\right) > 0 \Leftrightarrow u_q\left(s_q^{'}, \mathbf{s}_{-q}\right) - u_q\left(s_q^{''}, \mathbf{s}_{-q}\right) > 0 \quad \forall \mathbf{s}_{-q}, \forall s_q^{'}, s_q^{''} \in \mathcal{S}_q. \tag{A.9}$$

— *an* ***generalized ordinal potential game*** *if there is a function* $\Phi : \mathcal{S} \to \mathbb{R}$ *such that*

$$u_q\left(s_q^{'}, \mathbf{s}_{-q}\right) - u_q\left(s_q^{''}, \mathbf{s}_{-q}\right) > 0 \Rightarrow \Phi_q\left(s_q^{'}, \mathbf{s}_{-q}\right) - \Phi_q\left(s_q^{''}, \mathbf{s}_{-q}\right) > 0 \quad \forall \mathbf{s}_{-q}, \forall s_q^{'}, s_q^{''} \in \mathcal{S}_q. \tag{A.10}$$

In exact potential games, the change in a single player's utility due to its own strategy deviation results in exactly the same amount of change in the potential function. For such a game, an equivalent definition to A.6 states that, $\forall q \in \Omega$:

$$\frac{\partial u_q(s_q, \mathbf{s}_{-q})}{\partial s_q} = \frac{\partial \Phi_q(s_q, \mathbf{s}_{-q})}{\partial s_q}, \quad \forall s_q \in \mathcal{S}_q, \forall \mathbf{s}_{-q} \in \mathcal{S}_{-q}. \tag{A.11}$$

Especially, in [111], the author proved that

Theorem A.7. *The game* $\mathcal{G}$ *is a continuous exact potential game if and only if*

$$\frac{\partial u_q(s_q, \mathbf{s}_{-q})}{\partial s_q \partial s_p} = \frac{\partial u_p(s_p, \mathbf{s}_{-p})}{\partial s_q \partial s_p}, \quad \forall s_q \in \mathcal{S}_q, \mathbf{s}_{-q} \in \mathcal{S}_{-q}, s_p \in \mathcal{S}_p, \mathbf{s}_{-p} \in \mathcal{S}_{-p}. \tag{A.12}$$

From Definition A.6, the exact potential game is a special case of the weighted potential game and then the ordinal potential game. Also, the theorem A.7 allows us to identify a continuous exact potential game without knowing its potential function.

In potential game, the key idea to show the existence of the pure Nash equilibrium is based on the fact that the set of equilibria such a game is tied to that of an identical-interested game, where every player maximizes the common potential function.

Theorem A.8. *Every finite (ordinal) potential game admits at least one pure-strategy Nash equilibrium. Every continuous (ordinal) potential game whose strategy space* $\mathcal{S}$ *is compact (i.e.,*

closed and bounded) and potential function Φ *is continuous admits at least one pure-strategy Nash equilibrium. Moreover, if* Φ *is strictly concave, the Nash equilibrium is unique.*

Proof. Please refer to [33, 111]. □

To achieve a NE, the sequential decision dynamics in which players take a turn to act in sequence or in a round-robin manner is adopted. Particularity, each player, in turn, selects a new strategy based on a certain decision rule, thus creating a unilateral strategy deviation and inducing a corresponding change in the potential function. If the change represents an improvement in the value of the function, one expects a series of improvement that drives the game toward one of its equilibria.

Concave Game

In many application, such as the power allocations problem between multiple independent users in wireless networks, the possible actions belong a continuous set. In such a case, we consider a game played by a finite set of player $i \in \mathcal{N} = \{1, 2, \ldots, N\}$. Suppose that each player i choose an action s_i from a compact convex subset $\mathcal{X}_i$. Let $\mathbf{x} = \{x_1, x_2, \ldots, x_N\}$ be the action profile of all users and $\mathbf{x_{-i}}$ be the set of the actions of all users, except user i. Let $\mathcal{X} = \prod_i \mathcal{X}_i$ be the action space of the game, where the corresponding payoff of each player is determined by an associated payoff function $u_i : \mathcal{X} \to \mathbb{R}$. The game $\mathcal{G} = (\mathcal{N}, \{\mathcal{X}_i\}_{i\in\mathcal{N}}, \{u_i\}_{i\in\mathcal{N}})$ is defined as a *concave game* if

Definition A.9. A game $\mathcal{G} = (\mathcal{N}, \{\mathcal{X}_i\}_{i\in\mathcal{N}}, \{u_i\}_{i\in\mathcal{N}})$ is a concave game if the strategy set $\{\mathcal{X}_i\}_{i\in\mathcal{N}}$ is a closed bounded convex set and the payoff function of player i is continuous in $\mathbf{x} \in \{\mathcal{X}_i\}_{i\in\mathcal{N}}$ and concave in x_i.

Similar as the case of strategic game, the Nash Equilibrium (NE) in a concave game is defined a strategy $\mathbf{x}^* = \{x_1^*, x_2^*, \ldots, x_N^*\}$ such that, for all $i \in \mathcal{N}$, $u_q(x_i^*, \mathbf{x}_{-i}^*) \geq u_i(x_i, \mathbf{x}_{-i}^*)$ $\forall x_i \in \mathcal{X}_i$. The existence of the NE of a concave game is provided as follows.

Theorem A.10. *A concave game always has at least one pure Nash Equilibrium.*

Proof. According to [103, 109, 110], if a strategic form game $\mathcal{G} = (\mathcal{N}, \{\mathcal{X}_i\}_{i\in\mathcal{N}}, \{u_i\}_{i\in\mathcal{N}})$ satisfies that

1. $\mathcal{X}_i$ is compact and convex for all $i \in \mathcal{N}$,
2. $u_i(x_i, \mathbf{x_{-i}})$ is continuous in $\mathbf{x}_{-i}$,
3. $u_i(x_i, \mathbf{x_{-i}})$ is continuous and concave in x_i,

then a pure strategy Nash equilibrium exists. □

Appendix B

The Linear Complementarity Problem

The *Linear Complementarity Problem* (LCP) is one of the fundamental problems of mathematical programming which finding a solution to a set of simultaneous linear equations. The study of LCP has led to an elegant framework for the theory of linear and quadratic programming, as well as bimatrix games.

B.1 Problem Formulation

The LCP problem is defined as the following.

Definition B.1. *Let* $\mathbf{M}$ *be the given square matrix of order* n *and* $\mathbf{b}$ *a column vector in* $\mathbb{R}^n$. *The* $LCP(\mathbf{b}, \mathbf{M})$ *is the problem of finding a vector* $\mathbf{z} \in \mathbb{R}^n$ *and a vector* $\mathbf{w} \in \mathbb{R}^n$ *which satisfy the following constraints*

$$\mathbf{w} = \mathbf{M}\mathbf{z} + \mathbf{b}, \quad \mathbf{z} \geq 0, \quad \mathbf{w} \geq 0, \quad \mathbf{z}^T\mathbf{w} = 0.$$

The non-negative constraints $\mathbf{z} \geq 0$, $\mathbf{w} \geq 0$ implies that $\mathbf{z}$ and $\mathbf{w}$ are non-negative vector in $\mathbb{R}^n$. The complementary constraints $\mathbf{z}^T\mathbf{w} = 0$, or $z_i w_i = 0 \; \forall i = 1, 2, \ldots, n$, implies that at least one of the variables in the pair $\{w_i, z_i\}$ should be zero.

In [113], the author proves that a sufficient condition for existence a solution to this problem is that $\mathbf{M}$ be a positive semidefinite matrix and $LCP(\mathbf{b}, \mathbf{M})$ is feasible. Then, the basic-exchange pivoting methods, such as the Lemke algorithm [88, 114], can be adopted to determine the solution of the LCP. Also, if $\mathbf{M}$ be a symmetric positive-definite matrix, the solution is uniqueness.

B.2 Applications

Linear Programming

Once application of the LCP is in the linear programing (LP) problems. Usually, the linear programing can be solved by using the pivoting method. Also, the linear programing problem can be transformed to the complementarity problem as follows.

The primal problem of LP and its corresponding dual problem are given as

$$\begin{array}{lrcll} \max & \mathbf{x}^T\mathbf{A}\mathbf{y} & & \max & \mathbf{e}^T\mathbf{p} \\ \text{subject to} & \mathbf{x}^T\mathbf{E}^T = \mathbf{e}^T & \xrightarrow{\text{primal}\to\text{dual}} & \text{subject to} & \mathbf{E}^T\mathbf{p} \geq \mathbf{A}\mathbf{y} \\ & \mathbf{x} \geq 0 & & & \mathbf{p} \text{ is unrestricted} \end{array} \tag{B.1}$$

The relationship between the primal and the dual problems is given by:

$$\begin{aligned} \mathbf{x}^T\mathbf{A} &= \mathbf{e}^T p \\ \mathbf{x}^T\mathbf{A} &= \mathbf{x}^T\mathbf{E}^T\mathbf{p} \\ \mathbf{x}^T(-\mathbf{A} + \mathbf{E}^T\mathbf{p}) &= 0 \end{aligned} \tag{B.2}$$

By setting $\mathbf{z} = [\mathbf{x}, \mathbf{p}^{'}, \mathbf{p}^{''}]^T$ where $\mathbf{p}^{'}, \mathbf{p}^{''}$ are non-negative vectors of the same dimension as $\mathbf{p} = \mathbf{p}^{'} - \mathbf{p}^{''}$, $\mathbf{b} = [\mathbf{A}, -\mathbf{e}, \mathbf{e},]^T$ and $\mathbf{M} = [0, -\mathbf{E}^T, \mathbf{E}^T; \mathbf{E}, 0, 0; -\mathbf{E}, 0, 0]$, we can transform the linear programing problem to a LCP as follows:

$$\begin{aligned} \mathbf{z} &\geq 0 \\ \mathbf{b} + \mathbf{M}\mathbf{z} &\geq 0 \\ \mathbf{z}^T(\mathbf{b} + \mathbf{M}\mathbf{z}) &= 0^{'} \end{aligned}$$

where the constraint $\mathbf{z}^T(\mathbf{b} + \mathbf{M}\mathbf{z}) = 0$ implies that

$$\mathbf{x}^T(0 - \mathbf{A} + \mathbf{E}^T(\mathbf{p}^{'} - \mathbf{p}^{''})) = 0 \quad \text{or} \quad \begin{aligned} (\mathbf{p}^{'})^T(-\mathbf{e} + \mathbf{E}\mathbf{x}) &= 0 \\ (\mathbf{p}^{''})^T(\mathbf{e} - \mathbf{E}\mathbf{x}) &= 0 \end{aligned} \tag{B.3}$$

This implications are valid since $\mathbf{e} = \mathbf{E}\mathbf{x}$. Also, $\mathbf{b} + \mathbf{M}\mathbf{z} \geq 0$ is implies that

$$\mathbf{E}^T\mathbf{p} \geq \mathbf{A}. \tag{B.4}$$

Bi-matrix Games

Another application of the linear complementarity problem is in bimatrix games, a game with two players in which each player aims to find the best response strategy (pure or mixed)

that maximizes its payoff given the other's strategy. Let consider a bimatrix game which is defined as follows. Let $A \in \mathbb{R}^{m\times n}$ and $B \in \mathbb{R}^{m\times n}$ denote the payoff matrix of each player, separately. Let $\mathbf{x} \in \mathbb{R}^m$ be the (mixed) strategy profile of player 1, while $\mathbf{y} \in \mathbb{R}^n$ be the (mixed) strategy profile of player 2. Obliviously, we have

$$\mathbf{x} \geq 0, \quad \textstyle\sum_{i=1}^{m} x_i = 1 \tag{B.5}$$

$$\mathbf{y} \geq 0, \quad \textstyle\sum_{i=1}^{n} y_i = 1 \tag{B.6}$$

The corresponding expected payoffs are $\mathbf{x}^T\mathbf{A}\mathbf{y}$ for player 1 and $\mathbf{x}^T\mathbf{B}\mathbf{y}$ for player 2, respectively.

According to the Definition A.1, for such a game, a strategy pair $(\mathbf{x}^*, \mathbf{y}^*)$ is NE if and only if

$$(\mathbf{x}^*)^T\mathbf{A}\mathbf{y}^* \geq (\mathbf{x})^T\mathbf{A}\mathbf{y}^* \quad \forall \mathbf{x} \geq 0 \quad \text{and} \quad \textstyle\sum_{i=1}^{m} x_i = 1 \tag{B.7}$$

$$(\mathbf{x}^*)^T\mathbf{B}\mathbf{y}^* \geq (\mathbf{x}^*)^T\mathbf{B}\mathbf{y} \quad \forall \mathbf{y} \geq 0 \quad \text{and} \quad \textstyle\sum_{i=1}^{n} y_i = 1 \tag{B.8}$$

The conditions $\sum_{i=1}^{m} x_i = 1$ and $\sum_{i=1}^{n} y_i = 1$ can be rewritten in the matrix form as

$$\begin{aligned} \mathbf{x}^T\mathbf{E}^T &= \mathbf{e}^T, \\ \mathbf{y}^T\mathbf{F}^T &= \mathbf{f}^T, \end{aligned} \tag{B.9}$$

where $\mathbf{E}$ and $\mathbf{F}$ refer to square matrix of all 1's of size m and n, $\mathbf{e}$ and $\mathbf{f}$ refer to vector of all 1's of size m and n, respectively.

The bimatrix game then can be transformed to the LCP as follows:

First, for player 1, the primal problem in (B.7) and its corresponding dual problem are given as

$$\begin{array}{lrcll} \max & \mathbf{x}^T\mathbf{A}\mathbf{y} & & \max & \mathbf{e}^T\mathbf{p} \\ \text{subject to} & \mathbf{x}^T\mathbf{E}^T = \mathbf{e}^T & \xrightarrow{\text{primal}\to\text{dual}} & \text{subject to} & \mathbf{E}^T\mathbf{p} \geq \mathbf{A}\mathbf{y} \\ & \mathbf{x} \geq 0 & & & \mathbf{p} \text{ is unrestricted} \end{array} \tag{B.10}$$

The relationship between the primal and the dual problems of player 1 is given as

$$\begin{aligned} & \mathbf{x}^T\mathbf{A}\mathbf{y} && = \mathbf{e}^T\mathbf{p} \\ \Rightarrow & \mathbf{x}^T\mathbf{A}\mathbf{y} && = \mathbf{x}^T\mathbf{E}^T\mathbf{p} \\ \Rightarrow & \mathbf{x}^T(-\mathbf{A}\mathbf{y} + \mathbf{E}^T\mathbf{p}) && = 0 \end{aligned} \tag{B.11}$$

Similarly, for player 2, the primal problem in (B.8) and its corresponding dual problem are given by:

$$\begin{array}{lll} \max & \mathbf{x}^T\mathbf{B}\mathbf{y} & \\ \text{subject to} & \mathbf{y}^T\mathbf{F}^T = \mathbf{f}^T & \xrightarrow{\text{primal}\to\text{dual}} \\ & \mathbf{x} \geq 0 & \end{array} \quad \begin{array}{lll} \max & \mathbf{f}^T\mathbf{q} & \\ \text{subject to} & \mathbf{F}^T\mathbf{q} \geq \mathbf{B}\mathbf{x} & \\ & \mathbf{q} \text{ is unrestricted} & \end{array} \tag{B.12}$$

The relationship between the primal and the dual problems of player 2 is given as

$$\begin{aligned} \mathbf{y}^T\mathbf{B}^T\mathbf{x} &= \mathbf{f}^T\mathbf{q} \\ \Rightarrow \mathbf{y}^T\mathbf{B}^T\mathbf{x} &= \mathbf{y}^T\mathbf{F}^T\mathbf{q} \\ \Rightarrow \mathbf{y}^T(-\mathbf{B}^T\mathbf{x} + \mathbf{F}^T\mathbf{q}) &= 0 \end{aligned} \tag{B.13}$$

Inspired by [79], we set the non-negative vector $\mathbf{z} = [\mathbf{x}, \mathbf{y}, \mathbf{p}', \mathbf{p}'', \mathbf{q}', \mathbf{q}'']^T$ where $\mathbf{p}', \mathbf{p}''$ and $\mathbf{q}', \mathbf{q}''$ are non-negative vectors of the same dimension as $\mathbf{p} = \mathbf{p}' - \mathbf{p}''$ and $\mathbf{q} = \mathbf{q}' - \mathbf{q}''$. Furthermore, we let

$$\mathbf{M} = \begin{bmatrix} 0 & -\mathbf{A} & \mathbf{E^T} & -\mathbf{E^T} & 0 & 0 \\ -\mathbf{B^T} & 0 & 0 & 0 & \mathbf{F^T} & -\mathbf{F^T} \\ -\mathbf{E} & 0 & 0 & 0 & 0 & 0 \\ \mathbf{E} & 0 & 0 & 0 & 0 & 0 \\ 0 & -\mathbf{F} & 0 & 0 & 0 & 0 \\ 0 & \mathbf{F} & 0 & 0 & 0 & 0 \end{bmatrix} \tag{B.14}$$

and $\mathbf{b}^T = \begin{pmatrix} 0, & 0, & \mathbf{e}, & -\mathbf{e}, & \mathbf{f}, & -\mathbf{f} \end{pmatrix}^T$. Then, we have the LCP problem as follows:

$$\begin{aligned} &\text{find} \quad \mathbf{z} \\ &\text{s.t} \quad \mathbf{M}\mathbf{z} + \mathbf{b} \geq \mathbf{0} \\ &\qquad \mathbf{z^T}(\mathbf{M}\mathbf{z} + \mathbf{b}) = 0 \\ &\qquad \mathbf{z} \geq 0 \end{aligned} \tag{B.15}$$

where the conditions $\mathbf{z}^T(\mathbf{b} + \mathbf{M}\mathbf{z}) = 0$ implies that

$$\begin{aligned} \mathbf{x}^T(0 - \mathbf{A}\mathbf{y} + \mathbf{E}^T(\mathbf{p}' - \mathbf{p}'')) &= 0 \\ \mathbf{y}^T(0 - \mathbf{B}^T\mathbf{x} + \mathbf{F}^T(\mathbf{q}' - \mathbf{q}'')) &= 0 \end{aligned} \tag{B.16}$$

or

$$\begin{aligned}(\mathbf{p}^{'})^T(\mathbf{e}-\mathbf{E}\mathbf{x}) &= 0\\ (\mathbf{p}^{''})^T(-\mathbf{e}+\mathbf{E}\mathbf{x}) &= 0\\ (\mathbf{q}^{'})^T(\mathbf{f}-\mathbf{F}\mathbf{y}) &= 0\\ (\mathbf{q}^{''})^T(-\mathbf{f}+\mathbf{F}\mathbf{y}) &= 0\end{aligned} \tag{B.17}$$

This implications are valid because $\mathbf{e} = \mathbf{E}\mathbf{x}$ and $\mathbf{f} = \mathbf{F}\mathbf{x}$.

Similarly, the constraints $\mathbf{M}\mathbf{z} + \mathbf{b} \geq 0$ implies that

$$\begin{aligned}-\mathbf{A}\mathbf{y} + \mathbf{E}^T(\mathbf{p}^{'} - \mathbf{p}^{''}) \geq 0\\ -\mathbf{B}^T\mathbf{x} + \mathbf{F}^T(\mathbf{q}^{'} - \mathbf{q}^{''}) \geq 0\end{aligned} \tag{B.18}$$

This implications are valid because $\mathbf{E}^T\mathbf{p} \geq \mathbf{A}\mathbf{y}$ and $\mathbf{F}^T\mathbf{q} \geq \mathbf{B}^T\mathbf{x}$.

In order to solve (B.15), the Lemke algorithm is adopted by using the auxiliary variable z_0 to replace the term $\mathbf{b} + \mathbf{M}\mathbf{z}$ by $\mathbf{b} + \mathbf{d}\mathbf{z}_0 + \mathbf{M}\mathbf{z}$ and rewritten the problem (B.15) to

$$\begin{aligned}\text{Find} \quad & \mathbf{w} \geq 0, \mathbf{z}_0 \geq 0, \mathbf{z} \geq 0\\ \text{s.t.} \quad & \mathbf{I}\mathbf{w} - \mathbf{d}\mathbf{z}_0 - \mathbf{M}\mathbf{z} = \mathbf{b},\\ & \mathbf{z}^T\mathbf{w} = 0\end{aligned} \tag{B.19}$$

where $\mathbf{I}$ is the $n \times n$ identity matrix, d is an n-vector with positive components, e.g., $\mathbf{d} = \{1, 1, \ldots, 1\}^T$.

The solution of (B.19) defines a solution to (B.15) if and only if $\mathbf{z}_0 = 0$. Since in (B.19), $\mathbf{b}$ is represented as the nonnegative combination of certain columns of the matrix $[\mathbf{I}, \mathbf{d}, \mathbf{M}]$, the pivoting operation is used to determine the solution of the problem. In [79], the authors present an algorithm to solve (B.19) such that $\mathbf{z}_0 = 0$, hence the solution of (B.15). The algorithms solves the LCP (B.15) except for two possible problems: ray termination and degeneracy. However, in [79], the author proves that

Theorem B.2. *If i.)* $\mathbf{z}^T\mathbf{M}\mathbf{z} \geq 0$ *for all* $\mathbf{z} \geq 0$*, and ii.)* $\mathbf{z} \geq 0$, $\mathbf{M}\mathbf{z} \geq 0$ *and* $\mathbf{z}^T\mathbf{M}\mathbf{z} = 0$ *imply* $\mathbf{z}^T\mathbf{b} \geq 0$*, then Lemke's algorithm computes a solution of the LCP* (B.15) *and does not terminate with a secondary ray.*

Proof. Please refer to [79]. □

Theorem B.3. *If* $\mathbf{A} \geq 0$ *and* $\mathbf{B} \geq 0$*, then* $\mathbf{M}$ *and* $\mathbf{b}$ *in* (B.14) *satisfy all assumption of Theorem B.2.*

Proof. Please refer to [79]. □

The conditions $\mathbf{A} < 0$ and $\mathbf{B} < 0$ can be assumed without loss of generality, by subtracting a constant from the payoffs to the players at the leaves of the tree so that these become

non-positive. This transformation does not change the game as well as the equilibrium point of the game.

Bibliography

[1] I. F. Akyildiz, W. y. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, pp. 40–48, April 2008.

[2] M. A. Uusitalo, "Global vision for the future wireless world from the wwrf," *IEEE Vehicular Technology Magazine*, vol. 1, no. 2, pp. 4–8, 2006.

[3] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127 – 2159, 2006.

[4] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE signal processing magazine*, vol. 24, no. 3, pp. 79–89, 2007.

[5] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 201–220, Feb 2005.

[6] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[7] C. R. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. J. Shellhammer, and W. Caldwell, "Ieee 802.22: The first cognitive radio wireless regional area network standard," *IEEE communications magazine*, vol. 47, no. 1, pp. 130–138, 2009.

[8] IEEE, "Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 22: Cognitive wireless ran medium access control (mac) and physical layer (phy) specifications: Policies and procedures for operation in the tv bands," *IEEE Std 802.22-2011*, pp. 1–680, July 2011.

[9] IEEE, "802.11af-2013: Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 5: Television white spaces (tvws) operation," December 2013.

[10] R. W. Brodersen, A. Wolisz, D. Cabric, S. M. Mishra, and D. Willkomm, "Corvus: a cognitive radio approach for usage of virtual unlicensed spectrum," *Berkeley Wireless Research Center (BWRC) White paper*, pp. 1–21, 2004.

[11] H. Zheng and C. Peng, "Collaboration and fairness in opportunistic spectrum access," in *Communications, 2005. ICC 2005. 2005 IEEE International Conference on*, vol. 5, pp. 3132–3136, IEEE, 2005.

[12] C. Peng, H. Zheng, and B. Y. Zhao, "Utilization and fairness in spectrum assignment for opportunistic spectrum access," *Mobile Networks and Applications*, vol. 11, no. 4, pp. 555–576, 2006.

[13] K. R. Chowdhury and I. F. Akyildiz, "Cognitive wireless mesh networks with dynamic spectrum access," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, 2008.

[14] M. Di Felice, R. Doost-Mohammady, K. R. Chowdhury, and L. Bononi, "Smart radios for smart vehicles: cognitive vehicular networks," *IEEE Vehicular Technology Magazine*, vol. 7, no. 2, pp. 26–33, 2012.

[15] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1023–1043, 2015.

[16] R. Chen, J. Park, Y. Hou, and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, pp. 50–55, April 2008.

[17] K. Zeng, S. Ramesh, and Y. Yang, "Location spoofing attack and its countermeasures in database-driven cognitive radio networks," in *IEEE Conference on Communications and Network Security (CNS)*, pp. 202–210, Oct 2014.

[18] W. Wang and Q. Zhang, *Location Privacy Preservation in Cognitive Radio Networks*. Springer, 2014.

[19] S. Anand, Z. Jin, and K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *Proc. of 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, 2008.

[20] K. Bian and J.-M. J. Park, "Security vulnerabilities in IEEE 802.22," in *Proc. of 4th Annual International Conference on Wireless Internet*, ICST, 2008.

[21] R. Chen and et al, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 25–37, Jan 2008.

[22] A. Abrardo, M. Barni, K. Kallas, and B. Tondi, "A game-theoretic framework for optimum decision fusion in the presence of byzantines," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 1333–1345, June 2016.

[23] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 59, pp. 774–786, Feb 2011.

[24] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys Tutorials*, vol. 11, pp. 116–130, First 2009.

[25] P. Murty, "SenseLess: A Database-Driven White Spaces Network," *IEEE Transactions on Mobile Computing*, vol. 11, pp. 189–203, Feb 2012.

[26] FCC12-36, "Third memorandum opinion and order," tech. rep., Federal Communications Commission, May 2012.

[27] Z. Jin, S. Anand, and K. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *Proc. of IEEE International Conference on Communications (ICC)*, pp. 1–5, June 2009.

[28] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in *IEEE INFOCOM*, pp. 2751–2759, April 2013.

[29] B. Bahrak, S. Bhattarai, A. Ullah, J.-M. Park, J. Reed, and D. Gurney, "Protecting the primary users' operational privacy in spectrum sharing," in *IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, pp. 236–247, April 2014.

[30] J. Liu, C. Zhang, H. Ding, H. Yue, and Y. Fang, "Policy-based privacy-preserving scheme for primary users in database-driven cognitive radio networks," in *2016 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Dec 2016.

[31] S. Bakşi and D. C. Popescu, "Distributed power allocation for spectrum sharing in mutually interfering wireless systems," *Physical Communication*, vol. 22, pp. 42–48, 2017.

[32] G. J. Foschini and Z. Miljanic, "A simple distributed autonomous power control algorithm and its convergence," *IEEE Transactions on Vehicular Technology*, vol. 42, pp. 641–646, Nov 1993.

[33] G. Scutari, S. Barbarossa, and D. P. Palomar, "Potential games: A framework for vector power control problems with coupled constraints," in *ICASSP*, vol. 4, pp. IV–IV, May 2006.

[34] U. O. Candogan, I. Menache, A. Ozdaglar, and P. A. Parrilo, "Near-optimal power control in wireless networks: A potential game approach," in *INFOCOM, 2010 Proceedings IEEE*, pp. 1–9, IEEE, March 2010.

[35] A. Ghosh, L. Cottatellucci, and E. Altman, "Normalized nash equilibrium for power allocation in cognitive radio networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 1, pp. 86–99, March 2015.

[36] D. Goodman and N. Mandayam, "Power control for wireless data," *IEEE Personal Communications*, vol. 7, pp. 48–54, Apr 2000.

[37] A. Zappone, E. Jorswieck, *et al.*, "Energy efficiency in wireless networks via fractional programming theory," *Foundations and Trends® in Communications and Information Theory*, vol. 11, no. 3-4, pp. 185–396, 2015.

[38] A. Gjendemsjø, D. Gesbert, G. E. Øien, and S. G. Kiani, "Binary power control for sum rate maximization over multiple interfering links," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 3164–3173, August 2008.

[39] L. Venturino, N. Prasad, and X. Wang, "Coordinated scheduling and power allocation in downlink multicell ofdma networks," *IEEE Transactions on Vehicular Technology*, vol. 58, pp. 2835–2848, July 2009.

[40] L. Zheng and C. W. Tan, "Maximizing sum rates in cognitive radio networks: Convex relaxation and global optimization algorithms," *IEEE Journal on Selected Areas in Communications*, vol. 32, pp. 667–680, March 2014.

[41] P. C. Weeraddana, M. Codreanu, M. Latvaaho, A. Ephremides, C. Fischione, *et al.*, "Weighted sum-rate maximization in wireless networks: A review," *Foundations and Trends® in Networking*, vol. 6, no. 1–2, pp. 1–163, 2012.

[42] A. Zappone, Z. Chong, E. A. Jorswieck, and S. Buzzi, "Energy-aware competitive power control in relay-assisted interference wireless networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 4, pp. 1860–1871, 2013.

[43] A. Zappone, L. Sanguinetti, G. Bacci, E. Jorswieck, and M. Debbah, "Energy-efficient power control: A look at 5g wireless technologies," *IEEE Trans. on Signal Processing*, vol. 64, no. 7, pp. 1668–1683, 2016.

[44] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 355–379, 2012.

[45] R. Yu, Y. Zhang, Y. Liu, S. Gjessing, and M. Guizani, "Securing cognitive radio networks against primary user emulation attacks," *IEEE Network*, vol. 29, no. 4, pp. 68–74, 2015.

[46] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, pp. 111–122, ACM, 2007.

[47] S. Chen, K. Zeng, and P. Mohapatra, "Hearing Is Believing: Detecting Wireless Microphone Emulation Attacks in White Space," *IEEE Transactions on Mobile Computing,*, vol. 12, pp. 401–411, March 2013.

[48] K. M. Borle, B. Chen, and W. K. Du, "Physical layer spectrum usage authentication in cognitive radio: Analysis and implementation," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 2225–2235, Oct 2015.

[49] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 1850–1860, 2012.

[50] R. B. Myerson, "Game theory: analysis of conflict," *Harvard University*, 1991.

[51] H. Li and Z. Han, "Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems, Part I: Known Channel Statistics," *IEEE Transactions on Wireless Communications*, vol. 9, pp. 3566–3577, November 2010.

[52] B. Wang, Y. Wu, K. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 877–889, 2011.

[53] N. Nguyen-Thanh, P. Ciblat, A. T. Pham, and V. T. Nguyen, "Attack and surveillance strategies for selfish primary user emulator in cognitive radio network," in *2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 1199–1203, Dec 2014.

[54] N. N. Thanh, P. Ciblat, A. Pham, and V.-T. Nguyen, "Surveillance strategies against primary user emulation attack in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 14, pp. 4981–4993, Sept 2015.

[55] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE journal on selected areas in communications*, vol. 23, no. 2, pp. 201–220, 2005.

[56] C. Chen, H. Cheng, and Y.-D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2135–2141, 2011.

[57] G. Tian, X. Tian, D. Shen, and G. Chen, "A stackelberg game approach to cognitive radio network with anti-jamming capability," tech. rep., Michigan Technological Univ Houghton, 2012.

[58] IEEE, "802.19-2014:part 19: Tv white space coexistence methods," May 2014.

[59] T. Ehrenkranz and J. Li, "On the state of ip spoofing defense," *ACM Transactions on Internet Technology (TOIT)*, vol. 9, no. 2, p. 6, 2009.

[60] D. S. Benco, P. C. Kanabar, J. C. Nguyen, and H. Song, "Caller id spoofing," Oct. 16 2006. US Patent App. 11/581,634.

[61] J. F. Nash *et al.*, "Equilibrium points in n-person games," *Proceedings of the national academy of sciences*, vol. 36, no. 1, pp. 48–49, 1950.

[62] C. U. Saraydar, N. B. Mandayam, and D. J. Goodman, "Efficient power control via pricing in wireless data networks," *IEEE transactions on Communications*, vol. 50, pp. 291–303, Feb 2002.

[63] M. Rasti and A. R. Sharafat, "Distributed uplink power control with soft removal for wireless networks," *IEEE Transactions on Communications*, vol. 59, no. 3, pp. 833–843, 2011.

[64] M. Rasti, A. R. Sharafat, and J. Zander, "Pareto and energy-efficient distributed power control with feasibility check in wireless networks," *IEEE Transactions on Information Theory*, vol. 57, no. 1, pp. 245–255, 2011.

[65] M. Rasti, A. R. Sharafat, and J. Zander, "A distributed dynamic target-sir-tracking power control algorithm for wireless cellular networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 906–916, 2010.

[66] H. Mahdavi-Doost, M. Ebrahimi, and A. K. Khandani, "Characterization of sinr region for interfering links with constrained power," *IEEE Transactions on Information Theory*, vol. 56, no. 6, pp. 2816–2828, 2010.

[67] Y.-F. Liu, Y.-H. Dai, and Z.-Q. Luo, "Joint power and admission control via linear programming deflation," in *Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on*, pp. 2873–2876, IEEE, 2012.

[68] I. Mitliagkas, N. D. Sidiropoulos, and A. Swami, "Joint power and admission control for ad-hoc and cognitive underlay networks: Convex approximation and distributed implementation," *IEEE Transactions on Wireless Communications*, vol. 10, no. 12, pp. 4110–4121, 2011.

[69] A. Zappone, B. Matthiesen, and E. A. Jorswieck, "Energy efficiency in mimo underlay and overlay device-to-device communications and cognitive radio systems," *IEEE Transactions on Signal Processing*, vol. 65, no. 4, pp. 1026–1041, 2017.

[70] E. Dall'Anese, S. J. Kim, G. B. Giannakis, and S. Pupolin, "Power control for cognitive radio networks under channel uncertainty," *IEEE Transactions on Wireless Communications*, vol. 10, pp. 3541–3551, October 2011.

[71] S. Maharjan, Y. Zhang, C. Yuen, and S. Gjessing, "Distributed spectrum sensing in cognitive radio networks with fairness consideration: Efficiency of correlated equilibrium," in *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*, pp. 540–549, Oct 2011.

[72] Z. Q. Luo and S. Zhang, "Dynamic spectrum management: Complexity and duality," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, pp. 57–73, Feb 2008.

[73] N. Agmon, V. Sadov, G. A. Kaminka, and S. Kraus, "The impact of adversarial knowledge on adversarial planning in perimeter patrol," in *Proc. of 7th international joint conference on Autonomous agents and multiagent systems-Volume 1*, pp. 55–62, 2008.

[74] J. Pita, M. Jain, J. Marecki, F. Ordóñez, C. Portway, M. Tambe, C. Western, P. Paruchuri, and S. Kraus, "Deployed armor protection: the application of a game theoretic model for security at the los angeles international airport," in *Proc. of 7th international joint conference on Autonomous Agents and Multiagent systems*, pp. 125–132, 2008.

[75] T. Duc-Tuyen, N. Nguyen-Thanh, P. Ciblat, and V.-T. Nguyen, "Extra-sensing game for malicious primary user emulator attack in cognitive radio network," in *2015 European Conference on Networks and Communications (EuCNC)*, pp. 306–310, June 2015.

[76] T. Duc-Tuyen, N. Nguyen-Thanh, P. Maille, P. Ciblat, and V. T. Nguyen, "Mitigating selfish primary user emulation attacks in multi-channel cognitive radio networks: A surveillance game," in *IEEE Globecom'16*, 2016.

[77] D.-T. Ta, N. Nguyen-Thanh, P. Maillé, and V.-T. Nguyen, "Strategic surveillance against primary user emulation attacks in cognitive radio networks," *IEEE Transaction on Cognitive Communications and Networking*, 2018.

[78] J. Harsanyi, "Games with Incomplete Information Played by "Bayesian" Players, I-III," *Manage. Sci.*, vol. 50, pp. 1804–1817, #dec# 2004.

[79] D. Koller, N. Megiddo, and B. Von Stengel, "Efficient computation of equilibria for extensive two-person games," *Games and Economic Behavior*, vol. 14, no. 2, pp. 247–259, 1996.

[80] H. Kuhn, "Extensive games and the problem of information," *Annals of Mathematics Studies*, vol. 28, 1953.

[81] D. Fudenberg and J. Tirole, "Game theory," *Cambridge, MA*, p. 86, 1991.

[82] J. C. Harsanyi and R. Selten, *A general theory of equilibrium selection in games*, vol. 1. The MIT Press, 1988.

[83] E. Hossain, D. Niyato, and Z. Han, *Dynamic Spectrum Access and Management in Cognitive Radio Networks*. Cambridge University Press, 2009. Cambridge Books Online.

[84] P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kraus, "Playing games for security: An efficient exact algorithm for solving bayesian stackelberg games," in *Proc. of 7th international joint conference on Autonomous Agents and Multiagent systems*, pp. 895–902, International Foundation for Autonomous Agents and Multiagent Systems, 2008.

[85] D. Korzhyk, V. Conitzer, and R. Parr, "Complexity of computing optimal stackelberg strategies in security resource allocation games.," in *AAAI*, 2010.

[86] C. Lemke and J. Howson Jr, "Equilibrium Points of Bimatrix Games," *Journal of the Society for Industrial and Applied Mathematics*, vol. 12, no. 2, pp. 413–423, 1964.

[87] M. J. Osborne and A. Rubinstein, *A course in game theory*. MIT press, 1994.

[88] R. W. Cottle, J.-S. Pang, and R. E. Stone, *The linear complementarity problem*, vol. 60. Siam, 1992.

[89] B. von Stengel, A. Van Den Elzen, and D. Talman, *Tracing equilibria in extensive games by complementary pivoting*. Tilburg University, 1996.

[90] B. Von Stengel and S. Zamir, "Leadership with commitment to mixed strategies," *CDAM Research Report, LSE-CDAM-2004-01*, 2004.

[91] V. Conitzer and D. Korzhyk, "Commitment to correlated strategies.," in *AAAI*, 2011.

[92] Y. Shoham and K. Leyton-Brown, *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations*. New York, NY, USA: Cambridge University Press, 2008.

[93] H. Von Stackelberg, *Market structure and equilibrium*. Springer Science & Business Media, 2010.

[94] IBM, "Cplex optimizer."

[95] N. Nguyen-Thanh, D.-T. Ta, and V.-T. Nguyen, "Spoofig attack and surveillance game in geo-location database driven spectrum sharing.".

[96] D.-T. Ta, D. H. Nguyen, N. Nguyen-Thanh, and V.-T. Nguyen, "Collaborative paradigm for next generation wireless networks." to be submitted.

[97] K. Gomadam, V. R. Cadambe, and S. A. Jafar, "A distributed numerical approach to interference alignment and applications to wireless interference networks," *IEEE Transactions on Information Theory*, vol. 57, pp. 3309–3322, June 2011.

[98] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Econometrica: Journal of the Econometric Society*, pp. 520–534, 1965.

[99] D. T. Ngo, L. B. Le, T. Le-Ngoc, E. Hossain, and D. I. Kim, "Distributed interference management in two-tier cdma femtocell networks," *IEEE Transactions on Wireless Communications*, vol. 11, pp. 979–989, March 2012.

[100] D. T. Ngo, L. B. Le, and T. Le-Ngoc, "Distributed pareto-optimal power control for utility maximization in femtocell networks," *IEEE Transactions on Wireless Communications*, vol. 11, pp. 3434–3446, October 2012.

[101] V. Chandrasekhar, J. G. Andrews, and A. Gatherer, "Femtocell networks: a survey," *IEEE Communications Magazine*, vol. 46, pp. 59–67, September 2008.

[102] DARPA, "DARPA Spectrum Collaboration Challenge (SC2)," 2016.

[103] G. Debreu, "A social equilibrium existence theorem," *Proceedings of the National Academy of Sciences*, vol. 38, no. 10, pp. 886–893, 1952.

[104] H. Moulin, "Dominance solvability and cournot stability," *Mathematical social sciences*, vol. 7, no. 1, pp. 83–102, 1984.

[105] R. D. Yates, "A framework for uplink power control in cellular radio systems," *IEEE Journal on Selected Areas in Communications*, vol. 13, pp. 1341–1347, Sep 1995.

[106] R. Jain, D.-M. Chiu, and W. R. Hawe, *A quantitative measure of fairness and discrimination for resource allocation in shared computer system*, vol. 38. Eastern Research Laboratory, Digital Equipment Corporation Hudson, MA, 1984.

[107] R. Gibbons, *Game theory for applied economists*. Princeton University Press, 1992.

[108] M. Felegyhazi and J. Hubaux, "Game Theory in Wireless Networks: A Tutorial," *ACM Computing Surveys*, 2006.

[109] K. Fan, "Fixed-point and minimax theorems in locally convex topological linear spaces," *Proceedings of the National Academy of Sciences*, vol. 38, no. 2, pp. 121–126, 1952.

[110] I. L. Glicksberg, *Minimax theorem for upper and lower semi-continuous payoffs*. Rand Corporation, 1950.

[111] D. Monderer and L. S. Shapley, "Potential games," *Games and economic behavior*, vol. 14, no. 1, pp. 124–143, 1996.

[112] Q. D. Lã, Y. H. Chew, and B.-H. Soong, *Potential Game Theory*. Springer, 2016.

[113] K. G. Murty, "On the number of solutions to the complementarity problem and spanning properties of complementary cones," *Linear Algebra and Its Applications*, vol. 5, no. 1, pp. 65–108, 1972.

[114] R. W. Cottle and G. B. Dantzig, "Complementary pivot theory of mathematical programming," *Linear algebra and its applications*, vol. 1, no. 1, pp. 103–125, 1968.