Apports des réseaux bayésiens à la prévention du risque de piraterie à l'encontre des plateformes pétrolières

Amal Bouejla

▶ **To cite this version:**

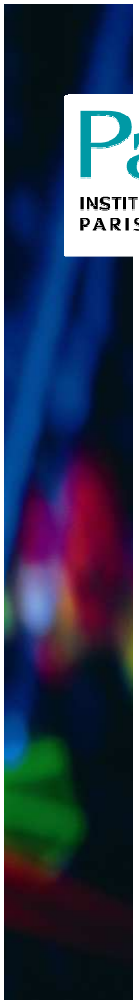
Amal Bouejla. Apports des réseaux bayésiens à la prévention du risque de piraterie à l'encontre des plateformes pétrolières. Statistiques [math.ST]. Ecole Nationale Supérieure des Mines de Paris, 2014. Français. NNT : 2014ENMP0076 . tel-01145589

HAL Id: tel-01145589
https://pastel.hal.science/tel-01145589

Submitted on 24 Apr 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

MINES ParisTech

École doctorale n° 432 : Sciences des Métiers de l'Ingénieur

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

L'École nationale supérieure des mines de Paris
Spécialité " Sciences et Génie des Activités à Risques "

présentée et soutenue publiquement par

Amal BOUEJLA

le 4 Décembre 2014

Apports des réseaux bayésiens à la prévention du risque de piraterie à l'encontre des plateformes pétrolières

Directeur de thèse : **Franck GUARNIERI**

Jury

M. Gilles DUSSERRE, Directeur de recherche, Ecole des Mines d'Alès/LGEI		Rapporteur
M. Tullio TANZI, Professeur, Telecom ParisTech/LabSoc		Rapporteur
M. Aldo NAPOLI, Chargé de recherche HDR, MINES ParisTech/CRC		Examinateur
M. Franck GUARNIERI, Directeur de recherche HDR, MINES ParisTech/CRC		Examinateur
M. Jean Marc RALLO, Directeur général, Preventeo		Invité

T H È S E

MINES ParisTech
Centre de recherche sur les Risques et les Crises
Rue Claude Daunesse, CS 10207 – 06904 Sophia-Antipolis Cedex - France

A ce que j'ai de plus cher, Hassen, mon bébé, ma grand-mère Essioutta, mes parents Rafia et Sassi, ma sœur Bochra, mon frère Mohammed, mes beaux-parents Samia et Ayed et à l'âme de mon grand-père Salah qui m'a quitté sans voir le fruit de son éducation.

Merci pour votre amour et vos encouragements.

Remerciements

Je tiens à remercier les membres du jury de m'avoir fait l'honneur de leur participation.

Je remercie monsieur le professeur Gilles Dusserre et monsieur le professeur Tullio Tanzi de m'avoir fait l'honneur d'être rapporteurs de mon travail de thèse.

Je remercie monsieur Aldo Napoli et monsieur Franck Guarnieri d'avoir participé au jury en tant qu'examinateurs.

Je remercie la société Preventeo qui a été l'un des partenaires financiers de cette recherche.

Je remercie également tout particulièrement M. Franck Guarnieri pour son attention constante dans le cadre de sa direction de thèse, ainsi que pour ses conseils toujours judicieux, ainsi que ses encouragements dans les moments difficiles.

Un grand merci à tous les membres du Centre de recherche sur les Risques et les Crises (CRC) et particulièrement à Bilal Idiri, Xavier Chaze, Melchior Pelleterat de Borde et Dalanda Lachtar pour leur amitié.

Je passe une dédicace « spéciale » à tous mes collègues que j'ai eu le plaisir de côtoyer durant ces trois années à Sophia Antipolis. Ces années ont été riches d'enseignement grâce à nos différents échanges.

Merci à Sandrine Renaux, Stéphanie Garnier, Myriam Perrault Lavigne, Sylvie Michel pour leur disponibilité, ainsi qu'à Valérie Godfrin et Jean-Luc Wybo pour leurs précieux conseils.

Table des matières

Liste des figures

Liste des tables

Liste des équations

Introduction

Contexte : la piraterie maritime, une menace avérée pour l'économie de l'énergie en mer

La production mondiale pétrolière est répartie sur plus de 10.000 champs offshore, impliquant chacun d'une part un ensemble d'équipements pour extraire, traiter et stocker provisoirement le pétrole et d'autre part des navires chargés d'effectuer le transport maritime d'hydrocarbures entre lieux de production et de consommation. La piraterie maritime moderne représente à l'heure actuelle le risque majeur pour la sécurisation de ces sites de production énergétique et du transport maritime pétrolier.

1. La piraterie maritime : un risque majeur sur le milieu maritime

Loin des images fantasmagoriques qui placent la piraterie dans l'univers romancé des bateaux à voiles, la piraterie moderne est un phénomène violent dont la recrudescence inquiète les autorités maritimes internationales.

La piraterie est « *l'acte illicite de violence ou de détention ou toute déprédation commis par l'équipage ou des passagers d'un navire ou d'un aéronef privé, agissant à des fins privées, et dirigé soit contre un autre navire ou aéronef, ou contre des personnes ou des biens à leur bord, en haute mer, soit contre un navire ou aéronef, des personnes ou des biens, dans un lieu ne relevant de juridiction d'aucun État*[1] ».

Force est donc de constater que les individus et organisations qui pratiquent des attaques contre des pêcheurs, des navires de commerce, des plaisanciers ou des plateformes pétrolières sont particulièrement déterminés, souvent suréquipés (moyens de locomotion, moyens de communications, armements…), et leurs « chefs » expérimentés assurent la pérennité de cette activité délictueuse en gérant les attaques comme s'il s'agissait d'une entreprise « mondiale ».

[1] Article 15 de la Convention sur la haute mer.

Les bateaux utilisés par les pirates sont des vedettes très puissantes, des « speed-boats », capables de rattraper aisément un lourd navire de commerce, qui ne peut que ralentir, incapable de virer de bord ou d'augmenter la vitesse au point de semer l'embarcation légère. Ces « dollars flottants » sont des proies faciles, croisant dans des eaux peu fréquentées par les autorités côtières [Onuoha, 2010]. Les « bateaux-mères », des pirates, postés en arrière du champ des « opérations », sont équipés des dernières technologies en matière de repérage dans l'espace, ce qui leur permet de cibler et d'organiser très précisément une attaque en prenant au dépourvu le navire attaqué, en envoyant des vedettes souvent indétectables par les navires assaillis.

Les actes de piraterie ne cessent de se multiplier. En 2013, 264 attaques ont été recensées par le Bureau maritime international (BMI), dont 141 en Asie du Sud-Est et 51 en Afrique de l'Ouest. 85 % des attaques ont eu lieu de nuit et les principales cibles sont les navires de commerce (pétrolier, vraquier et remorqueurs avec barge) au mouillage ou naviguant à faible vitesse. Dans la majorité des cas, les pirates cherchent à voler du matériel facile à revendre, ou à piller les navires, ou leur cargaison mais aussi à kidnapper certains membres d'équipage. Selon le BMI, une attaque sur 4, lorsqu'elle n'est pas interrompue par les forces gouvernementales navales de sécurité, est menée avec succès.

Au début des années 2000, les pirates étaient armés de couteaux. Aujourd'hui, ils attaquent leurs proies à l'arme automatique. La constatation, bien que peu surprenante, est alarmante. A la date du 18 août 2014, selon le rapport du BMI, les pirates ont mené 148 attaques.

2. La maritimisation de l'énergie, nouveaux territoires, nouveaux enjeux et nouvelles menaces

« *La sécurité énergétique fait partie des challenges économiques et sécuritaires les plus sérieux, aussi bien aujourd'hui que dans le futur. La croissance des économies du monde et des sociétés va de pair avec l'importance de l'énergie et de pair avec les infrastructures qui produisent et fournissent cette énergie. Les infrastructures énergétiques critiques fournissent le carburant qui permet à l'économie globale d'avancer et à nos sociétés de fonctionner* ». C'est en ces termes que s'est ouverte

l’allocution de l’OSCE (Organization for Security and Cooperation in Europe) lors de la réunion du comité économique de l’OTAN du 22 septembre 2008 à Bruxelles.

Plusieurs catastrophes ont démontré la vulnérabilité que peuvent avoir de telles infrastructures et l’impérieuse nécessité d’une profonde rigueur dans le respect des procédures, la conception et l’exploitation de ces systèmes « critiques ». La question de la maritimisation de l’énergie se révèle donc comme un enjeu considérable [Napoli., 2014].

La production offshore joue un rôle important dans l’approvisionnement énergétique des sociétés modernes. Si la majorité de la production est opérée par moins de 500 mètres d'eau, l'offshore dit « profond », dans des zones situées par plus de 1 000 m de hauteur d'eau, se développe depuis quelques années grâce à des avancées technologiques majeures, notamment dans le domaine de la sismique ou des installations sous-marines. Pour donner un ordre d'idée, la production d'huile par plus de 1 000 mètres de fond a augmenté de 12 % entre 2006 et 2008. Pour le gaz, la production par plus de 1 000 mètres représente moins de 2 % de la production mondiale et les réserves sont estimées à 2,7 Tm^3 (mille milliards).

Les compagnies pétrolières s’intéressent à l’offshore car c'est l'une des rares zones d'accès aux réserves naturelles et car il permet aussi de se protéger des conflits à terre (comme par exemple dans le golfe de Guinée où il est plus sûr de produire en mer qu'à terre). La production offshore devrait poursuivre son développement, ainsi près de 30 nouveaux champs situés sous plus de 1 000 mètres d'eau devraient être mis en production tous les ans d'ici à 2020, soit plus du double de la décennie 2000-2010.

Le domaine de sécurité maritime présente des multiples risques, comme le risque de naufrage, causés par le tonnage qui devient de plus en plus élevé ou la vitesse croissante des navires. Citons comme exemple le naufrage du traversier sénégalais le *Joola* au large des côtes de Gambie le 26 septembre 2002, faisant officiellement 1 863 morts et disparus, et officieusement plus de 2 000 victimes. La capacité légale du traversier était de 550 personnes…

Les risques de naufrage sont aussi liées aux erreurs humaines ou aux disfonctionnements de systèmes technologiques comme dans le cas du ferry-boat grec *Express Samina* au large de Paros (Grèce), le 26 septembre 2000, faisant 82 morts. La

coque du navire se déchira en deux endroits et coula en une heure, uniquement parce que 9 portes étanches sur 11 n'étaient pas fermées au niveau des salles de machines et des soutes. À la suite de ce naufrage, l'installation de boîtes noires deviendra une obligation sur tous les navires transporteurs de passagers.

Le risque de collision avec des objets flottants (navires, conteneurs tombés à l'eau, etc.) est aussi connu. Durant la Première Guerre mondiale, une terrible explosion se produisit dans le port d'Halifax, en Nouvelle-Écosse au Canada, lorsqu'un navire français transportant des munitions, le *Mont-Blanc*, entra en collision avec un navire norvégien qui se rendait en Belgique. L'explosion des munitions du *Mont-Blanc* advint 19 minutes plus tard : elle rasa 2,5 km² de la ville, tua 2 000 personnes et en blessa des milliers d'autres. Un raz-de-marée de 18 mètres de haut déclenché par l'explosion fut si puissant qu'il emporta des arbres, plia des rails de chemin de fer et démolit des édifices, transportant des débris en tout genre sur des centaines de mètres.

Le risque des catastrophes naturelles (séisme, cyclone, etc.) et aux aléas météorologiques (tempête, vague scélérate, etc.), représente aussi de réels dangers au quotidien comme cela fut le cas pour le ferry-boat *Princess of the Stars*, de la compagnie Sulpicio Lunes faisant 828 morts le 21 juin 2008, le navire a sombré en raison d'énormes vagues provoquées par le typhon Fengshen aux Philippines.

Les pollutions dues à l'extraction ou au transport des hydrocarbures sont encore présentes dans nos mémoires. Citons pour exemples l'accident en 2010 sur la plateforme pétrolière *Deepwater Horizon* dans le golfe du Mexique causant la perte de 4,9 millions de barils, 11 personnes portées disparues, 17 blessés et plusieurs zones polluées (littoraux de la Louisiane, du Mississippi, de l'Alabama et de la Floride).

De nouveaux risques, comme le risque sanitaire, qui se présentent avec le transport de déchets nucléaires, d'eaux de ballast et la circulation de navires ou sous-marins à propulsion nucléaire, et éventuellement armés d'engins nucléaires complètent dramatiquement le panorama des menaces.

A ces accidents et catastrophes, s'ajoute le risque de piraterie, toujours présent dans les espaces stratégiques comme le golfe d'Aden ou encore le golfe de Guinée, haut lieu de la production de pétrole offshore dans le monde.

La plupart des sources d'énergie nécessaires au fonctionnement de nos sociétés modernes sont fournies par le gaz et le pétrole. La dépendance mondiale à l'égard du pétrole est énorme, il alimente nos moyens de transport, chauffe ou refroidit des bâtiments et sert à créer des produits chimiques industriels et domestiques. 60% de la production de pétrole est utilisée pour le transport, essentiellement les voitures et les camions. Le pétrole est une énergie non renouvelable dont la consommation actuelle atteint 70 millions de barils par jour, certaines estimations en prévoyant le doublement d'ici 2025.

La production offshore représente 30 % de la production mondiale de pétrole (avec 25 millions de barils par jour) et 27 % de celle de gaz. L'offshore représente par ailleurs 20 % des réserves mondiales de pétrole et 30 % de celles de gaz. Environ 450 champs ont été découverts à plus de 1 000 mètres de profondeur, dont 38 % dans le golfe du Mexique aux États-Unis, 26 % dans le golfe de Guinée en Afrique et 18 % au Brésil. Ils ne représentent pour l'instant que 3 % de la production mondiale de pétrole, mais ce chiffre ne fera que croître dans les années à venir compte tenu des réserves estimées de l'ordre de 72 livre sterling.

La construction, le transport, le fonctionnement d'une plate-forme génèrent divers risques. D'éventuels incidents ou accidents peuvent aggraver des impacts sur l’environnement, les marins ou les biens comme le risque sismique, le risque des rejets et de toxicité, le risque d’incendie ou d’explosion qui est le risque le plus redouté et le risque de pollution qui perturbe la vie marine comme par exemple le cas du *Pasha Bulker*, cargo de 40 000 tonnes transportant du charbon, échoué le 8 juin 2007 sur le littoral australien avec encore 700 tonnes de pétrole à bord. Les 21 personnes de l'équipage ont été hélitreuillées. Restait à traiter le risque de pollution.

A ces accidents et catastrophes [Gordon et al., 1996], s’ajoute depuis le début des années 2000, le risque de piraterie Hansen, 2009], très présent dans les espaces stratégiques comme le golfe d’Aden ou le golfe de Guinée, haut lieu de la production de pétrole offshore dans le monde. Compte tenu des enjeux économiques liés aux hydrocarbures, les champs de production offshore sont devenus une cible de choix pour la piraterie maritime voire la menace terroriste [Anifowose et al., 2012]. Or si les plateformes pétrolières et navires associés forment un réseau industriellement abouti en

ce qui concerne l'exploitation, ils sont démunis face aux actes de malveillance intentionnels : de ce point de vue, ce sont des cibles de choix, isolées et donc très exposées.

3. Revue de littérature sur les attaques de piraterie contre les infrastructures énergétiques en mer, le cas des champs pétroliers

Les cas d'attaques d'infrastructures énergétiques offshore, s'ils restent pour le moment moins fréquents et moins médiatisés que ceux d'attaque de navires, n'en sont pas moins extrêmement inquiétants en ce sens qu'ils dévoilent une grande vulnérabilité des infrastructures.

Les attaques sur les navires transportant de l'énergie représentent un pourcentage significatif. En 2006, elles avoisinaient environ 12 % des attaques pour atteindre plus de 24 % en 2007. La plupart des attaques sont des actes visant à dérober un bien de valeur. Elles se déroulent dans les ports mêmes ou à l'aide de petites embarcations très rapides. Le nombre de détournements et de prises d'otages ainsi que de demandes de rançon a aussi fortement augmenté. En août 2003, le tanker malaisien *Penrider* a été abordé au large de l'Indonésie et une rançon demandée pour un montant de 100 000 dollars. Les cas où le navire est attaqué pour les biens qu'il transporte est clairement un objectif des pirates. En 1998, le *Petro Ranger* a été attaqué hors des eaux territoriales de Singapour. Il transportait près de 12 000 tonnes de produits pétroliers. Les pirates sont allés jusqu'à le débaptiser et le renommer *Wilby* en lui attribuant un pavillon hondurien. Le *Petro Ranger* devient ainsi, pour un temps, un navire fantôme [Nincic., 2009].

La grande majorité des attaques contre des navires transportant de l'énergie concerne les tankers de pétrole et le transport de gaz liquide. Par rapport au nombre total de la flotte de tankers (environ 120 000), 4 000 (3 %) sont des tankers énergétiques. En 2007, les pirates se sont aussi intéressés avec succès aux plateformes pétrolières mobiles et aux transporteurs de gaz liquide. Ainsi, deux ont été attaqués en 2007, l'un en Indonésie, l'autre au large de Singapour. Trois plateformes fixes de forage ont aussi été attaquées, deux au Nigeria (avec un kidnapping et une rançon à la clef) et une en Inde. Ces

évènements démontrent que les pirates sont désormais en capacité de s'attaquer à tout type de cible.

La piraterie à l'encontre des installations pétrolière en mer a depuis 1988 pris une ampleur considérable.

Dans la Figure 0-1, un exemple de scénario d'attaque par 14 pirates lourdement armés contre un navire conteneur est donné. Les pirates ont utilisé deux bateaux dont un navire de ravitaillement et un navire de haute vitesse. Ils sont aisément montés à bord du conteneur. Malgré le déclenchement du système d'alerte et le repli de l'ensemble de l'équipage au sein d'une « citadelle », les pirates ont réussi à pénétrer dans cette dernière et ont enlevé cinq personnes dont le maître de l'équipage. Ils se sont enfin échappés en emportant la trésorerie de l'équipage.

Outre des navires transportant le pétrole ou du matériel en liaison avec l'activité de production, plusieurs plateformes pétrolières ont aussi été attaquées ces dernières années. Le navire-citerne français *Gascogne*, battant pavillon luxembourgeois (il appartient à la société Sea-Tankers), a été attaqué le 4 février 2013. Ce navire de 119 m de long dispose d'un équipage de 17 ou 19 personnes.

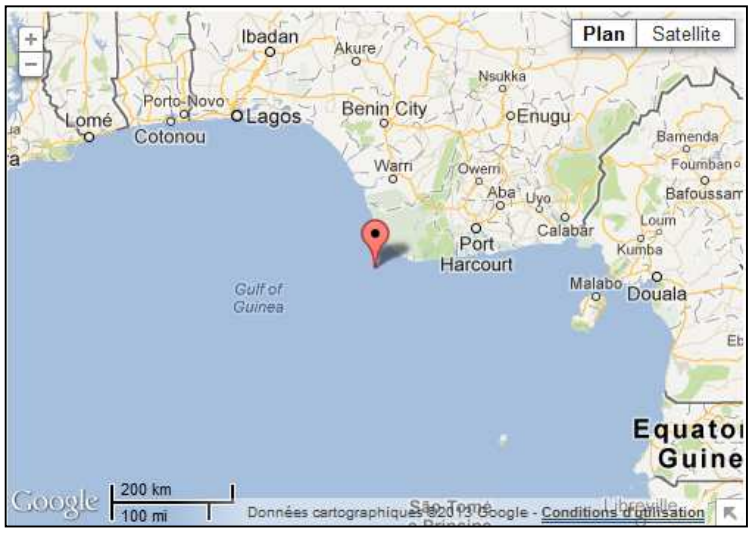


Figure 0-1 : Attaque de pirate contre un navire conteneur le 25 avril 2013 (Source Bureau maritime international)

Selon le ministre des Transports, de la Mer et de la Pêche Frédéric Cuvillier, « *il y a 19 personnes à bord, tous des Togolais (...). Nous n'avons pas reçu de revendication pour*

l'instant », a-t-il ajouté en précisant que le bateau naviguerait « *à la hauteur du sud du Ghana et se dirigerait vers le Togo* », tout proche.

C'est le troisième cas de capture d'un pétrolier au large de la Côte d'Ivoire. Dans les deux premiers cas, le navire a été vidé de sa cargaison, au large du Ghana, puis libéré par les ravisseurs. En octobre 2013, un tanker grec avait été attaqué alors qu'il mouillait devant le port d'Abidjan, tandis qu'en janvier, c'est un tanker battant pavillon panaméen qui avait été la cible des pirates.

Malgré la diminution de nombre d'attaques de piraterie (439 en 2011, 297 en 2012 contre 264 en 2013), la dangerosité et la gravité des conséquences de ces actes sur l'équipage des cibles attaqués restent constantes en évolution.

Force est de constater que les marins des navires de commerce ne sont ni équipés, ni formés pour repousser une attaque armée. Même si des formations de prévention et d'intervention sont réalisées pour les équipages transitant dans des zones à risques, et même si des équipements sont apportés aux navires, il n'appartient pas aux marins de devoir faire face à la violence d'une attaque pirate.

Les pirates ne se limitent plus à l'heure actuelle à piller les marchandises et les effets personnels contenus sur les navires. Après avoir pris le contrôle du navire, ils réclament désormais des rançons pour libérer les équipages. Certains pirates vont même jusqu'à tuer tout l'équipage pour revendre la marchandise et se servir du navire détourné pour faire transiter en toute impunité une marchandise qui sera détournée à nouveau, et ainsi de suite, en modifiant à chaque fois l'immatriculation grâce à des pavillons de complaisance attribués sans aucun contrôle. Les transporteurs, seuls face à leurs décisions, se retrouvent désemparés, et finissent souvent par verser les rançons demandées après les avoir négociées.

Aujourd'hui, une nouvelle forme de piraterie voit le jour : un groupe organisé, hiérarchisé, maîtrisant les dernières technologies en matière de repérage maritime, doté d'informateurs dans le monde, d'armes puissantes et de bases à terre sur des territoires de non-droit. La question se pose de savoir comment il est possible d'éradiquer ce phénomène pourtant vivement condamné qui fait frémir les marins du monde, hésiter les armateurs, et méditer les assureurs.

4. Des solutions technologiques innovantes qui se déploient progressivement

A ce jour, il existe deux types de systèmes opérationnels dédiés à la protection des cibles maritimes :

- La détection d'une menace ;
- La gestion d'une attaque.

4.1 La détection d'une menace

Dans le domaine de la détection en environnement marin, il existe de nombreux systèmes. Citons :

- Des systèmes à base de radar à impulsions tels que par exemple les radars de veille ou de navigation de type TERMA, RURUNO, RACAL ou DECA, ou encore le système Sea-Giraffe d'Ericsson [Saab, 2005]. Ces systèmes sont destinés à détecter en priorité des mobiles coopératifs de taille importante ou moyenne. Ils ont des performances médiocres face à de petites cibles marines non coopératives évoluant dans une mer formée (fouillis de mer) et sont pénalisés par une zone aveugle à faible distance du porteur. Par ailleurs, les systèmes à balayage sont généralement relativement lents pour analyser un domaine étendu.

- Des systèmes de surveillance optroniques (développés par exemple par SAGEM, EADS, THALES, RADAMEC, ALENIA, HGH, FLIR Systems, etc. [Sagem, 2012]). Ces systèmes sont handicapés par les problèmes de réflexion solaire sur la mer et restent sensibles aux conditions météorologiques, leur portée étant rapidement réduite en présence de brume ou brouillard et d'embruns.

A titre d'exemple, le projet SCANMARIS ([Morel et al., 2010] et [Morel et al., 2008]) a permis de tester en milieu marin des modules innovants de détection de comportements suspects d'embarcations de tailles variables de manière globale et à long terme en analysant le trafic maritime régulier et en le croisant avec des bases de données sur les navires, pour identifier des suites spatio-temporelles d'anomalies.

4.2 La gestion d’une attaque

Les solutions élaborées reposent principalement sur des outils de diagnostic convoquant des raisonnements probabilistes et/ou à base de connaissances expertes. Les algorithmes rencontrés dans la littérature révèlent des insuffisances dans l’évaluation et la planification de la réaction [Giraud et al., 2013].

Les exemples d’attaques cités précédemment sont de parfaites illustrations de la faiblesse des dispositifs anti-piraterie actuellement mis en place. La sécurité des installations pétrolières est donc à ce jour assurée par des dispositifs dits classiques. Ces derniers, malgré leurs points forts pour l’aide à la détection, ne traitent pas des différents types de menaces (bateau de pêche, jet ski, tanker, etc.) et leur efficacité dépend de nombreux paramètres liés à l’environnement ainsi qu’aux contraintes techniques et opérationnelles [Giraud et al., 2010].

La solution consiste donc à augmenter le degré de protection des infrastructures en développant un système capable de prévenir la menace et de générer des réactions internes et externes en cas d’intrusion confirmée ([Morel et al., 2007] et [Giraud et al., 2012]).

Problématique et objectifs de recherche

Cette thèse se concentre sur la façon dont une approche bayésienne de l'estimation, de l'inférence et du raisonnement dans l'analyse des risques pourrait compléter avantageusement les approches classiques sous-tendues par des modèles « fréquentistes » [Pichard, 1998].

La fréquence n'est pas une probabilité. Une fréquence est une proportion d'observations alors qu'une probabilité est la mesure d'une incertitude sur un événement.

Les deux cadres classiques, dans lesquels la probabilité intervient avec sa sémantique, sont les suivants :

- Le cadre fréquentiste : la probabilité porte exclusivement sur les observations, conditionnellement à des valeurs hypothétiques des paramètres ; sémantiquement les probabilités sont conçues comme des fréquences. Dans sa version radicale, le cadre fréquentiste exclut toute probabilité sur les paramètres, et partant toute probabilité des hypothèses. Le cadre fréquentiste, mis en place à la fin du XIX^{ème} siècle, reste encore le cadre dominant de la statistique.
- Le cadre bayésien : la probabilisation porte aussi bien sur les observations que sur les paramètres. Le cadre bayésien est un enrichissement du cadre fréquentiste ; il restitue la sémantique naturelle des probabilités et permet les probabilités des hypothèses. Le cadre bayésien, plus ancien que le cadre fréquentiste, remonte au XVIII^{ème} siècle.

Les méthodes bayésiennes permettent de répondre directement aux questions sur les paramètres et les modèles : « Quelle est la probabilité d'un ensemble de paramètres compte tenu des données observées? ». Les méthodes fréquentistes permettent, elles, de répondre aux questions sur : « Quelle est la probabilité des données sans aucune hypothèse ? ».

Les deux approches bayésienne et fréquentiste sont généralement combinées comme techniques d'estimation et d'inférence ([Efron, 2005] et [Little, 2006]).

Le couplage de l'approche fréquentiste et de l'estimation bayésienne dans le cadre de notre problématique de lutte contre la piraterie apparaît donc pertinent. Il fournit une compréhension conceptuelle utile à la pluralité des données et connaissances convoquées

dans la prévention du risque et conduit à développer une boîte à outils statistiques particulièrement polyvalente à fin d'aide à la décision.

Afin de démontrer cette hypothèse, l'objectif principal de ce travail de thèse est de proposer une nouvelle approche permettant d'améliorer la prévention, le diagnostic, le management et la prise de décision face au risque de piratage maritime. Plus précisément, les objectifs de la thèse sont :

- D'étudier la faisabilité d'intégrer, au sein d'un outil de conception des réseaux bayésiens statiques, des données et des retours d'expériences des attaques de pirateries sur différents types de navires. Cela permettra ainsi de mieux comprendre l'environnement maritime, de préciser et de décrire des actes réels de piraterie et surtout de présenter les avantages de l'approche fréquentiste.
- De coupler des modèles quantitatifs d'analyse des risques avec des données et connaissances qualitatives acquises auprès d'experts du domaine maritime. Ce qui permettra de concevoir à l'aide d'un réseau bayésien dit « statique » un modèle de diagnostic de la menace plus adapté à la protection des champs pétroliers. Le couplage permettra de présenter la complémentarité entre l'approche fréquentiste et l'approche probabiliste.
- De concevoir un modèle dynamique d'aide à la décision grâce aux potentiels des réseaux bayésiens dits « dynamiques ». Ce modèle permettra l'amélioration des résultats obtenus à partir du modèle « statique ».
- De valider le couplage entre le modèle statique et le modèle dynamique afin d'obtenir un système performant pour le management du risque de piraterie maritime.

Organisation du manuscrit de thèse

Le manuscrit est organisé en 6 chapitres.

Le chapitre 1 présente une vue d'ensemble du projet de publications qui a sous-tendu ce travail de thèse.

Le chapitre 2 situe le premier article publié dans la revue « *Radio Science Bulletin*[2] ». Ce chapitre est constitué de deux sections, dont la première décrit en français le travail accompli pour concevoir un système de management du risque de piraterie basé sur les potentiels des réseaux bayésiens; la seconde livrant l'article tel que publié en langue anglaise par la revue.

Le chapitre 3 est lui aussi composé de deux sections. La première décrit en français le travail réalisé afin de démontrer l'adaptation à chaque type d'attaque de la planification générée par le système conçu. La seconde livre l'article tel que publié dans la revue « *Safety Science*[3] ».

Les résultats obtenues dans les chapitres 2 et 3 ont permis la construction d'un réseau bayésien « statique » pour le management du risque de piraterie contre les champs pétroliers et a permis de discuter des résultats acquis au plan tant méthodologique qu'opérationnel.

Le chapitre 4 présente l'article soumis à la revue « *International Journal of Critical Infrastructure Protection*[4] » qui propose un système de management du risque de piraterie basé sur les réseaux bayésiens dits « dynamiques ».

Enfin, le chapitre 5 décrit le couplage entre le réseau bayésien « statique » et le réseau bayésien « dynamique ». Les résultats sont présentés dans le cadre d'un article soumis à la revue « *Ocean Engineering*[5] ».

Les chapitres 4 et 5 sont composés de deux sections comme les précédents.

[2] http://www.ursi.org/en/publications_rsb.asp
[3] http://www.journals.elsevier.com/safety-science/
[4] http://www.journals.elsevier.com/international-journal-of-critical-infrastructure-protection/
[5] http://www.journals.elsevier.com/ocean-engineering/

Le chapitre 6 synthétise en français l'intégralité du travail effectué pendant cette thèse. Nous avons présenté le contexte général, le modèle conçu basé sur les réseaux bayésiens statiques, le modèle final basé sur les réseaux bayésiens dynamiques et enfin le couplage entre réseaux bayésiens statiques et réseaux bayésiens dynamiques.

Le manuscrit se termine par une conclusion qui pose le bilan de ce travail, met en avant les principales contributions et présente des perspectives de recherche.

Chapitre 1 : Le projet de publications

1.1. Introduction

L'établissement d'un programme de publications implique un repérage des revues et des conférences susceptibles d'être intéressées par le projet d'article. Cela nécessite une identification préalable des attentes scientifiques et thématiques de la revue et/ou de la conférence visée.

Le choix des objets abordés doit se fonder avant tout sur le matériau scientifique disponible permettant d'étayer convenablement un article, mais aussi sur les probabilités d'acceptation du projet par les revues et les conférences pressenties. Il est donc clair que le fait de lire et analyser régulièrement les revues à comité de lecture dès le début de la thèse (ou de mettre à profit un stage de master d'une durée de 6 mois au sein du laboratoire d'accueil, comme cela a été le cas pour moi) constitue un « avantage concurrentiel » important, en se familiarisant avec les thématiques les plus porteuses, mais aussi avec les bibliographies, et en permettant de bien définir le ou les sujets qui pourront être traités par les articles soumis à l'évaluation par les pairs académiques.

Ce chapitre présente donc l'ensemble des projets de publications portés et finalisés durant ces trois années de thèse. Le chapitre est organisé en trois sections : les articles soumis, acceptés et présentés à des conférences nationales à comité de lecture (1.1), les articles soumis, acceptés et présentés à des conférences internationales à comité de lecture (1.2), enfin, les articles soumis, évalué (ou en cours d'évaluation) et publiés dans des revues internationales à comité de lecture (1.3).

1.2. Les conférences nationales à comité de lecture

Les travaux réalisés pendant cette thèse ont été présentés dans quatre conférences nationales. Ces conférences traitent des domaines de l'analyse des risques, des systèmes d'information et de l'aide à la décision.

1.2.1. Workshop Interdisciplinaire sur la sécurité globale (WISG 2012) : 6ème colloque sur la sécurité globale (24 et 25 janvier 2012)

Cette conférence est organisée par l'Agence nationale de la recherche (ANR).

[Bouejla et al., WISG, 2012] présente le contexte général de la piraterie maritime et la dangerosité des attaques avec une étude comparative des dispositifs de prévention actuels. Ensuite, l'article détaille le système global de management du risque de piraterie face à des champs pétroliers prenant en compte toute la chaîne de traitement depuis la détection d'une menace potentielle jusqu'à la mise en œuvre de la réaction. Enfin, un « premier » modèle (à caractère exploratoire) basé sur les réseaux bayésiens est décrit. Des résultats d'attaques en présentant plusieurs scénarios d'attaques sont explicités et modélisés. Les résultats sont présentés mais pas discutés.

1.2.2. Informatique des organisations et Systèmes d'Information et de Décision (INFORSID 2012) : 30ème édition (29 au 31 mai 2012)

Cette conférence est organisée par Espace-Dev[6], Lirmm[7] et Tetis[8]. La conférence porte principalement sur l'ingénierie et la gouvernance des systèmes d'information. L'article présenté [Bouejal et al., INFORSID, 2012] a permis d'avancer la formalisation d'un réseau bayésien à partir des données (acquises par datamining). Le modèle proposé a été présenté comme un prototype de système d'aide à la décision visant à répondre à des situations d'urgence.

[6] http://www.espace.ird.fr/
[7] http://www.lirmm.fr/
[8] http://tetis.teledetection.fr/index.php/en/

1.2.3. Lambda Mu 18 (λmu18 2012) : Maîtrise des risques et sûreté de fonctionnement (16 au 18 octobre 2012)

La conférence de maîtrise des risques et sûreté de fonctionnement est en France parmi les meilleures conférences dans le domaine de la prévention des risques. Elle est organisée par l'Institut pour la maîtrise des risques (IMdR[9]). Les communications faites lors de la conférence fédèrent des résultats industriels et académiques. L'article [Bouejla et al., Lambda mu, 2012] présenté à cette conférence est une version plus abouti que celui présenté à WISG 2012. Lors de cette conférence, nous avons obtenu le prix de la meilleure communication (Figure 1-1).

Figure 1-1 : Lambda mu d'or (26 octobre 2012)

1.2.4. Lambda mu 19 (λmu19 2014) : Congrès de maîtrise des risques et sûreté de fonctionnement (20 au 23 octobre 2014)

L'article [Bouejla et al., Lambda mu, 2014] présente un prototype de réseau bayésien dit « dynamique ». Cet article reprend les limités posées lors de l'article présenté dans la même conférence en date de 2012.

La conférence Lambda mu 2014 est spécialement en lien avec le sujet de cette thèse puisque son intitulé est « Décider dans un monde incertain : enjeu majeur de la maîtrise des risques ».

[9] http://www.imdr.fr/

1.3. Les conférences internationales à comité de lecture

La plupart des conférences internationales retenues sont inscrites dans la thématique « gestion des risques ».

1.3.1. Technologies d'information pour le secteur maritime (Information Technologies for the Maritime Sectors ITEMS 2012) : Premier atelier international (15 avril 2012)

Cette conférence a permis de mettre en avant le contexte général de la thèse, celui de la piraterie maritime, et ses enjeux pour le secteur maritime [Chaze et al., ITEMS, 2012]. Plusieurs scénarios d'attaques ont conduit à démontrer l'efficacité de la planification des réactions proposées afin de supprimer l'attaque sans risquer la vie de l'équipage et l'activité de production.

1.3.2. Journée Francophones sur les Réseaux Bayésiens (JFRB 2012) : 6ème édition (11 au 13 mai 2012)

Cette conférence a été l'occasion de présenter en détail l'approche bayésienne retenue dans les travaux de thèses et le logiciel utilisé pour la conception du réseau bayésien (BayesiaLab[10]). Par rapport aux thématiques de la conférence, notre proposition s'est inscrite comme une application pré-opérationnelle des réseaux bayésiens [Bouejla et al., JFRB, 2012]. Nous avons obtenu lors de cette conférence, le prix du meilleur poster (Figure 1-2).

[10] http://www.bayesia.com/

Figure 1-2 : Prix meilleur poster

1.3.3. Système de l'ingénierie des systèmes (System of Systems Engineering 2012) : 7ème conférence internationale (16 au 19 juillet 2012)

Par rapport aux autres publications, l'article [Chaze et al., SOSE, 2012] présenté dans cette conférence met l'accent sur le prototype développé pour le traitement des rapports d'alerte et la génération des rapports de planification des réactions contre une menace potentielle. Le réseau bayésien est présenté comme une boîte noire intégrée au sein d'un système plus global de gestion du risque.

1.3.4. Analyse des Risques (Risk Analysis 2012) : 8ème conférence internationale sur l'analyse et l'atténuation des risques (19 au 21 septembre 2012)

Cette conférence a été l'occasion de préciser le concept de vulnérabilité des plateformes pétrolières face à la piraterie maritime [Bouejla et al., Risk Analysis, 2012]. L'aspect management des différents équipements de protection disponibles sur les champs pétroliers et l'interaction entre eux a été l'un des points développé dans l'article.

1.4. Les revues internationales à comité de lecture

Les multiples communications faites dans les conférences à comité de lecture ont contribué à rassembler, organiser et améliorer un riche matériau qui a permis de s'engager pleinement dans un processus de publications d'articles dans des revues unanimement reconnues.

Quatre articles ont été soumis. Deux ont été publiés et deux sont en cours d'évaluation (Table 1-1).

Nom de la revue	**Rédacteur en chef**	**Impact factor**	**Titre de l'article**	**Liste des auteurs**	**Date de publication**	**Date de soumission**
Radio Science Bulletin	Paul Lagasse	1,45	Causal Probabilistic Modeling with Bayesian Networks to Combat the Risk of Piracy against Offshore Oil Platforms	Amal Bouejla, Xavier Chaze, Franck Guarnieri et Aldo Napoli	Juin 2013	Janvier 2013
Safety Science	Jean Luc Wybo	1,672	A Bayesian network to manage risks of maritime piracy against offshore oil fields.	Amal Bouejla, Xavier Chaze, Franck Guarnieri et Aldo Napoli	1er septembre 2014	28 janvier 2013
International Journal of Critical Infrastructure Protection	Sujeet Shenoi	0,652	Contribution of dynamic Bayesian networks to the protection of critical infrastructure: offshore oil platforms	Amal Bouejla et Franck Guarnieri		1er juillet 2014

Ocean Engineering	Atilla Incecik et Matthew Collette	1,615	A coupled Static and Dynamic Bayesian Network able to respond to Maritime Piracy against Offshore Oil Fields	Amal Bouejla et Franck Guarnieri		11 juin 2014

Table 1-1 : Présentation des articles publiés et soumis

1.4.1. *The Radio Science Bulletin*

Chaze X, Bouejla A, Guarnieri F et Napoli A., (2013). Causal Probabilistic Modeling with Bayesian Networks to Combat the Risk of Piracy against Offshore Oil Platforms, *The Radio Science Bulletin*, Volume 345, Disaster Management special issue, pp. 21-34, June 2013.

http://www.ursi.org/en/publications_rsb.asp

1.4.1.1. Présentation et ambition de la revue

La revue publie des articles scientifiques couvrant les domaines d'intérêt des dix commissions scientifiques de l'Union radio scientifique internationale (URSI). L'accent est mis sur les contributions non spécialistes qui sont orientées vers la communauté de sciences radio.

Le volume 345 de la revue propose un numéro spécial sur la gestion des catastrophes. Dans ce numéro, une section spéciale sur «Le rôle des sciences de la radio dans la gestion des catastrophes » a été réalisée. C'est dans le cadre de ce dernier que notre article a été soumis et accepté pour publication.

1.4.1.2. Pourquoi publier dans cette revue ?

Le facteur d'impact de la revue est égal à 1,45. Cet indice montre à la fois la quantité d'articles publiés (113 articles en 2012) et leur visibilité (3 245 citations). En plus la

composition du comité de lecture renseigne sur les valeurs et l'orientation de la revue qui avait sollicité pour ce projet des experts de rang mondial du domaine des risques.

1.4.1.3. Résumé de l'article

L'article est organisé en trois sections. La première compte trois sous-sections. La première détaille quelques données de référence sur le sujet de la piraterie en général et sur celles liées à l'énergie en particulier. La deuxième établit une typologie des menaces et la troisième dresse un état succinct des dispositifs contemporains d'alerte et de mise en sécurité des installations pétrolières. Ensuite la deuxième section est organisée en trois sous-sections. La première énonce brièvement des besoins opérationnels et des contraintes inhérentes à la conception et au développement d'un dispositif performant de détection, d'alerte et de traitement d'une menace. La deuxième présente le concept de réseau bayésien et l'outil logiciel utilisé. Enfin, la troisième section détaille les modalités de construction d'un réseau bayésien fondé sur le couplage entre des données quantitatives et des connaissances expertes. La dernière section est organisée en deux sous-sections. La première décrit les scénarios conçus pour le test. La seconde décrit l'intégration du réseau bayésien développé au sein d'un système global de gestion de l'alerte et de la réponse.

1.4.1.4. Les principales remarques des rapporteurs

Les rapporteurs ont unanimement apprécié l'article. Ils ont néanmoins demandé d'étoffer la revue de littérature en s'appuyant sur des références aisément accessibles et en limitant la citation de rapports techniques.

Cette remarque nous a permis de grandement améliorer notre état de l'art initial.

1.4.2. Safety Science

Bouejla A, Chaze X, Guarnieri F et Napoli A., (2014). A Bayesian network to manage risks of maritime piracy against offshore oil fields. *Safety Science*, Volume 68, pp. 222-230, Elsevier, 31 octobre 2014.

http://www.journals.elsevier.com/safety-science/

1.4.2.1. Présentation et ambition de la revue

Safety Science a été créée en 1991. Son facteur d'impact est égal à 1,672 (selon Thomson Reuters Journal Citation Reports 2014).

La revue sert de support international pour la recherche en science et en technologie de la sécurité de l'homme et de l'industrie. Elle s'étend de la sécurité des personnes au travail à d'autres domaines, tels que les transports, l'énergie ou les infrastructures, ainsi que tous les autres domaines d'activités humaines dangereuses.

Safety Science est multidisciplinaire. Ses collaborateurs et son public rassemblent tout à la fois des chercheurs en sciences de l'ingénieur et des sciences humaines et sociales. Elle recouvre de multiples thématiques liées par exemple à : l'ingénierie de la sécurité, les politiques et questions humaines et organisationnelles; l'évaluation, la gestion et la communication sur les risques; l'efficacité des techniques de contrôle et de gestion de la sécurité; la normalisation, la législation, l'inspection, l'assurance, l'économie de la prévention etc. Les communications portant sur les interfaces entre la technologie, les hommes et les organisations sont aussi acceptées.

1.4.2.2. Pourquoi publier dans cette revue ?

Safety Science est parmi les revues de référence dans le domaine de l'analyse des risques.

La publication de cet article a nécessité plusieurs phases de réécriture. Celles-ci sont guidées par les échanges avec la revue. Les évaluateurs ont demandé des modifications qui consistent en des réductions et des apports de précision relatifs à certains éléments de réflexion de la première version de l'article proposée. Ces modifications ont permis d'enrichir très significativement la présentation et la discussion des résultats de notre recherche.

1.4.2.3. Résumé de l'article

L'article se compose de cinq sections avec une introduction qui décrit le contexte général de la piraterie moderne alors que la 2ème section décrit la piraterie à l'encontre des

champs pétroliers : les enjeux économiques et politiques, la violence des attaques, le besoin urgent d'un dispositif de protection efficace et la description du système global de détection, diagnostique et planification des réactions contre une menace potentielle. La 3ème section présente le couplage entre les connaissances quantitatives et les connaissances qualitatives pour la conception du réseau bayésien. L'établissement des scénarios d'attaque a permis de démontrer les résultats du modèle proposé. Enfin, la conclusion montre le potentiel du prototype développé avec la discussion des limites et les perspectives possibles comme l'utilisation des ontologies afin d'enrichir la partie détection et diagnostic et les réseaux bayésiens dynamiques qui pourra intégrer la notion temporelle dans le modèle proposé.

1.4.2.4. Les principales remarques des rapporteurs

Les rapporteurs ont souhaité des développements plus importants dans les parties suivantes :

- **La méthode de recherche**

Nous avons détaillé la démarche de construction du réseau bayésien. Celle-ci est basée sur une construction automatique à partir de la base de données de l'Organisation maritime internationale (OMI) associée à des connaissances d'experts du domaine maritimes avec lesquels nous avons pu collaborer.

- **La validation des résultats**

La description fine de différents scénarios d'attaques, avec en particulier l'adaptation de la planification des réactions selon les paramètres spécifiques de la menace, a permis de consolider les énoncés sur la validation du prototype développé.

- **La discussion des limites et la présentation des futures recherches**

Les limites du modèle basé sur un réseau bayésien statique ont été plus largement discutées. L'idée du couplage entre réseau bayésien statique et réseau bayésien dynamique a été avancée et développée comme perspective de recherche ainsi que le recours au concept d'ontologie.

- **Une revue de littérature plus large**

La revue de littérature a été complétée sans pour autant prétendre à l'exhaustivité.

1.4.3. International Journal of Critical Infrastructure Protection

Bouejla A et Guarnieri F., (2014). Contribution of dynamic Bayesian networks to the protection of critical infrastructure: offshore oil platforms. *International Journal of Critical Infrastructure Protection*, soumis le 1er juillet 2014.

http://www.journals.elsevier.com/international-journal-of-critical-infrastructure-protection/

1.4.3.1. Présentation et ambition de la revue

La revue a été lancé en 2008, avec pour objectif principal de publier des articles scientifiques de la plus haute qualité dans tous les domaines de la protection des infrastructures critiques. Plus précisément, les articles qui présentent la science, la technologie, le droit et la politique et qui vise à élaborer des solutions sophistiquées et pratiques pour la sécurisation des actifs dans les différents secteurs d'infrastructures critiques intéressent cette revue. Ces secteurs d'infrastructures essentielles comprennent : les technologies de l'information, des télécommunications, de l'énergie, de la banque et de la finance, les systèmes de transport, les produits chimiques, l'industrie de l'agriculture et de l'alimentation, le secteur de la défense, de la santé publique, les monuments nationaux, l'eau potable et des systèmes de traitement de l'eau, les établissements commerciaux, les barrages, les services d'urgence, des réacteurs nucléaires, des matériaux et des déchets, les services postaux et des installations gouvernementales...

1.4.3.2. Pourquoi publier dans cette revue ?

Le concept d'infrastructure critique est en plein essor et de nombreux thèmes de la revue se rapprochent significativement de nos travaux :

- L'analyse des défis de sécurité.
- L'identification des techniques de sécurité qui peuvent être appliquées à la protection des infrastructures critiques.

- L’élucidation des dépendances et les interdépendances qui existent entre les secteurs et les technologies pour atténuer les effets dévastateurs des défaillances.
- La création de solutions sophistiquées, mais opérationnelles pour la protection des infrastructures essentielles qui impliquent des techniques mathématiques, scientifiques et techniques, des méthodes de sciences économiques et sociales, et / ou des constructions juridiques et de politique publique.

1.4.3.3. Résumé de l’article

L’article soumis à cette revue est composé de quatre sections : la première présente la vulnérabilité des infrastructures pétrolières face à la multitude des menaces et incidents et qui peuvent générer des dégâts importants. Ensuite une deuxième section démontre que le risque de piraterie à l’encontre de ces infrastructures présente une menace à prendre aux sérieux. La troisième section décrit les bénéfices de l’usage des réseaux bayésiens dynamiques pour lutter contre ce risque majeur. Dans cette section, le choix des réseaux bayésiens a été justifié avec la présentation de la structure du réseau et la prise en compte de l’indice temporel dans le modèle proposé. Il était intéressant de tester le réseau bayésien élaboré en jouant différents scénarios d’attaque. L’étude de ces scénarios permet ainsi d’apprécier d’une part l’efficacité du prototype proposé à planifier des réponses adaptées à chaque attaque et d’autre part de démontrer les apports à coupler un réseau bayésien « statique » à un réseau bayésien « dynamique ».

1.4.4. Ocean Engineering

Bouejla A et Guarnieri F., (2014). A coupled Static and Dynamic Bayesian Network able to respond to Maritime Piracy against Offshore Oil Fields. *Ocean Engineering*, soumis le 11 juin 2014.

http://www.journals.elsevier.com/ocean-engineering/

1.4.4.1. Présentation et ambition de la revue

Ocean Engineering fournit un support pour la publication de travaux de recherche et de développement dans le domaine maritime. Parmi les secteurs couverts par cette revue : l'ingénierie offshore, l'architecture navale, la mécanique marine, la sécurité et la fiabilité, les matériaux, les pipelines et canalisations verticales, l'hydrodynamique, la technologie sous-marine, la géotechnique, l'ingénierie des fondations, etc.

1.4.4.2. Pourquoi publier dans cette revue ?

Nous avons choisi de publier nos travaux dans cette revue, car elle est en liaison évidentes avec nos axes de recherche : les systèmes d'information, l'analyse des risques, la protection des infrastructures offshore et enfin le domaine maritime. Cette revue est présentée comme parmi les revues de référence dans l'ingénierie maritime. L'évaluation de nos travaux par des experts maritimes nous donc est apparue plus que pertinente.

1.4.4.3. Résumé de l'article

Cet article décrit un prototype d'outil d'aide à la décision pour lutter contre la piraterie maritime. Deux types de réseaux bayésiens, l'un « statique », l'autre « dynamique » ont été retenus afin de concevoir un modèle graphique d'aide à la décision dans un univers incertain. La construction de ce type de réseaux bayésiens, outre la comparaison dans les apports respectifs et complémentaires de chacun, permet d'incorporer au sein de bases de connaissances des distributions de probabilités utiles pour la prédiction du futur en tenant compte du passé. L'article a donc pour but de détailler la démarche méthodologique qui a permis de concevoir un prototype visant à diagnostiquer le risque et à planifier les contre-mesures à appliquer contre les attaques de piraterie à l'encontre d'une plateforme pétrolière en mer. Le prototype accompagne la prise de décision en tenant compte de l'influence de la décision prise au temps T – 1 sur la décision à prendre au temps T.

1.5. Conclusion

Soumettre un article n'est pas toujours couronné de succès. Il n'existe pas de formule garantissant la réussite d'un projet de publication, mais il est possible d'accroître significativement ses « chances de réussite » en procédant avec méthode. La prise en compte des remarques des comités de rédaction nous a permis d'améliorer sensiblement le fond et souvent la forme de nos différents projets d'article.

Ecrire un article conduit également à réduire à l'essentiel la partie consacrée à la présentation des résultats figurant dans la partie de thèse concernée de même que les paragraphes de présentation des résultats de l'analyse quantitative. Ainsi, écrire des projets d'article permet d'apporter très significativement des améliorations au contenu de chaque article.

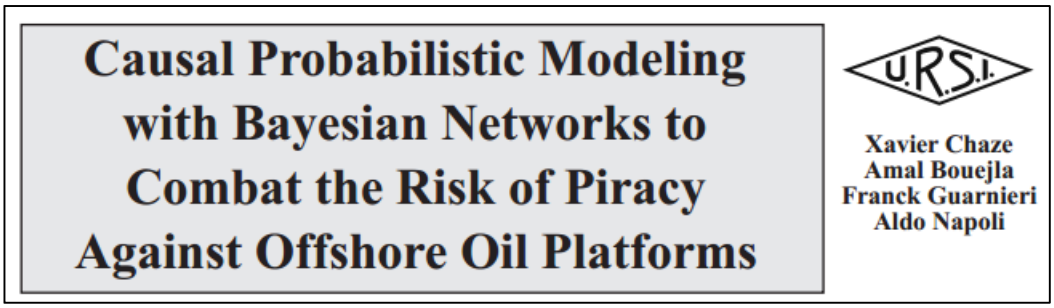
Notre projet de publications nous a permis d'une part de présenter nos travaux à des chercheurs et experts des différentes domaines en liaison avec la thèse et d'autre part d'avoir des avis et des conseils critiques sur la problématique, la méthodologie et les résultats obtenus. Ceci nous a évidemment aidé dans l'amélioration du travail et dans la rédaction des articles.

Chapitre 2 : Article 1 : Modélisation causale probabiliste à l'aide des réseaux bayésiens pour prévenir le risque de piraterie à l'encontre des plateformes pétrolières en mer

2.1. Présentation de l’article

L’article a été publié en juin 2013 dans la revue *Radio Science Bulletin*. Il décrit en détails le contexte général, le modèle proposé et la discussion des résultats obtenus.

2.2. Version anglaise de l'article



Abstract

Pirate attacks against offshore oil platforms are multiplying. To reduce the vulnerability of this critical, highly strategic infrastructure operators are actively investigating potential new information and communication technologies. Among the available options, techniques from Artificial Intelligence and particularly Bayesian networks offer promising avenues for research. This article describes the development and assessment of a prototype Bayesian network designed to assess the risk of attack against offshore oil platforms.

Keywords

Bayesian networks, piracy, offshore oil platforms, threat, protection, quantitative and qualitative knowledge.

1. Introduction

More than seven thousand oil rigs are scattered across the world's oceans. These high-tech facilities offer a range of facilities to extract, process, and temporarily store oil. Vessels that transport oil between the place of production and consumption form another essential part of the operation.

Modern maritime piracy is undoubtedly a major threat to the security of both energy production sites and maritime oil transport. It is clear that current monitoring methods have major weaknesses, in terms of threat detection and particularly the defensive procedures to be implemented in response to a threat. This is demonstrated by the fact

that in 2011, 552 attacks were registered with the International Maritime Bureau[11], compared to 487 attacks in 2010. It is clear that an effective and efficient system that can guarantee the safety of all facilities and stakeholders (operators, subcontractors, etc.) involved in the exploitation of oil fields is needed.

There are two aspects to data and domain knowledge: quantitative (databases containing information about the operating conditions of oil fields and particularly acts of piracy), and qualitative (the expertise and experiences of operators and stakeholders who organize prevention and the response to attacks).

An approach that couples both quantitative and qualitative aspects of data seems particularly useful. Methods and models from Artificial Intelligence have repeatedly demonstrated the benefits of such an undertaking. Similarly, Bayesian networks have been mobilised – as much for their ability to formalize knowledge resulting from various worlds – as for predictive reasoning capabilities that can provide decision support.

This article is organized into three sections. It first outlines the current situation related to acts of piracy against energy infrastructure. We then introduce the concept of Bayesian networks. In this section we focus on the development of a methodology that led to the construction of a Bayesian network based on two data sources (the Piracy and Armed Robbery database of the International Maritime Organization and the collection and formalization of expert knowledge). The last section presents and discusses our results obtained through simulations of comprehensive and realistic pirate attack scenarios.

2. "Energy" piracy at sea

This part is organized into three sections. The first section outlines some baseline data concerning piracy in general and the energy sector in particular. The second establishes a typology of threats, and the third provides a short summary of the tools currently available for alerting and securing oil installations.

[11] http://www.icc-ccs.org/home/imb

2.1 Piracy facts and figures and attacks on energy installations

On average, 5.9 vessels are attacked per 1,000 trips made [Brown, 2006]. In 2007, a pirate attack was reported on average every 31 hours. In the early 1980s the international community responded by setting up a regulatory framework (the United Nations Convention on the Law of the Sea [United Nations, 1982]). This defines "piracy" and the ways in which states and vessels can protect themselves and if necessary respond to attacks. In the 1990s the number of attacks increased considerably, and the International Maritime Organization[12] (IMO) under the aegis of the United Nations was made responsible for creating a database of incidents and providing monthly, quarterly and annual reports [IMO, 2008]. The IMO produced its first report in 1998 and so far nearly 4,000 attacks have been documented. Figure 2-1 is a summary of attacks in the ten-year period up to September 2008.

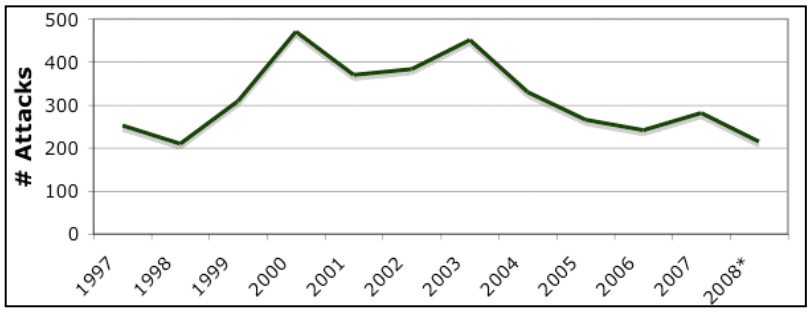


Figure 2-1 : Global maritime pirate attacks, January 1997 - September 2008. Total attacks: 3,566 (Source: IMO database)

The IMO estimates that the costs (losses) are 13 – 15 billion dollars per year in the Pacific region [Ryan, 2006]. Other sources suggest a sum of 16 billion dollars [Burnett, 2002], [Dillon, 2000]. Losses include direct costs such as the theft of ships and goods, but also indirect costs due to the act of piracy (delays, higher insurance premiums, etc.). The human cost is also very high. In 2006, 15 sailors were killed, 188 were taken hostage and 77 were kidnapped and released in exchange for a ransom. Since 1995, more than 350 sailors have lost their lives.

Attacks on vessels carrying energy products represent a significant percentage of incidents. In 2006, they averaged about 12% of attacks and reached more than 24% in 2007 (Figure 2-2). Most of these attacks aim to steal an asset. They take place either

[12] http://www.imo.org

while the vessel is still in port or with the help of small, very fast boats. The number of hijackings, hostage-taking and ransom demands have also increased sharply. In August 2003, the Malaysian tanker Penrider was seized while off the coast of Indonesia and a 100,000 dollar ransom was demanded.

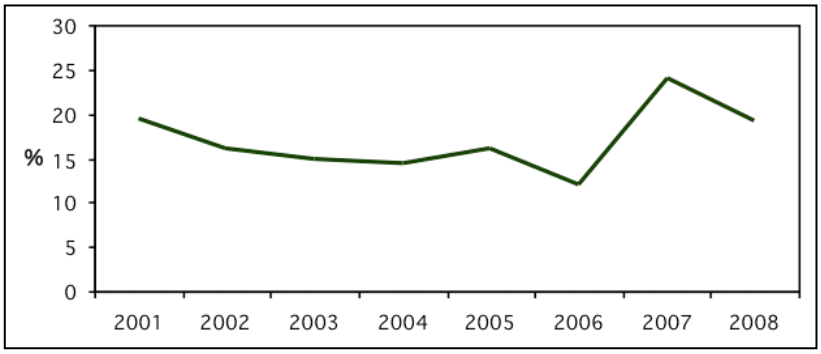


Figure 2-2 :Percentage of attacks on energy vessels, January 2001 – September 2008 (Source: IMO database)

A clear target for pirates is vessels that are attacked for the goods they are transporting. In 1998, the Petro Ranger was attacked outside the territorial waters of Singapore. It was carrying nearly 12,000 tons of petroleum products. Pirates went to the lengths of renaming the ship Wilby and assigning it a Honduran flag. The Petro Ranger became, for a time, a ghost ship [Nincic, 2009].

As Figure 2-3 shows, the vast majority of attacks against vessels carrying energy products concerns tankers transporting oil and liquid gas. About 3% (4,000 vessels) of the total tanker fleet (120,000 vessels) is energy tankers. In 2007, pirates started to take an interest in mobile oil platforms and liquid gas carriers, with some success. Two platforms were attacked in 2007, one in Indonesia and the other off Singapore. Three fixed drilling platforms were also attacked, two in Nigeria (including a kidnapping and a ransom demand) and one in India. These events show that pirates are able to tackle any type of target.

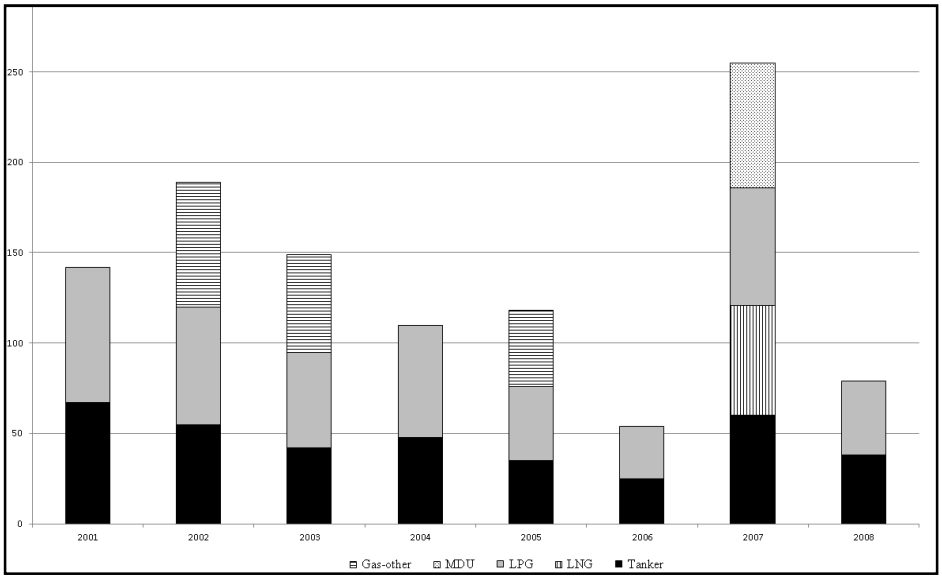


Figure 2-3 :Number of attacks by vessel type 2001–2008 (Source: IMO database)

Figure 2-4 shows that most pirate attacks are concentrated in Indonesia and the Malacca Straits. In 2007, Nigeria suddenly emerged as a dangerous area particularly for vessels transporting energy products, which accounted for 29% of attacks, although Indonesia still led the field with over 35% of attacks. However, in 2008, Somali pirates increased their response capacity beyond 200 nautical miles. Consequently, in 2008, more attacks occurred in Nigeria and Somalia than in Indonesia and the Malacca Straits. By the end of 2008, the IMO had recorded more than 60 attacks.

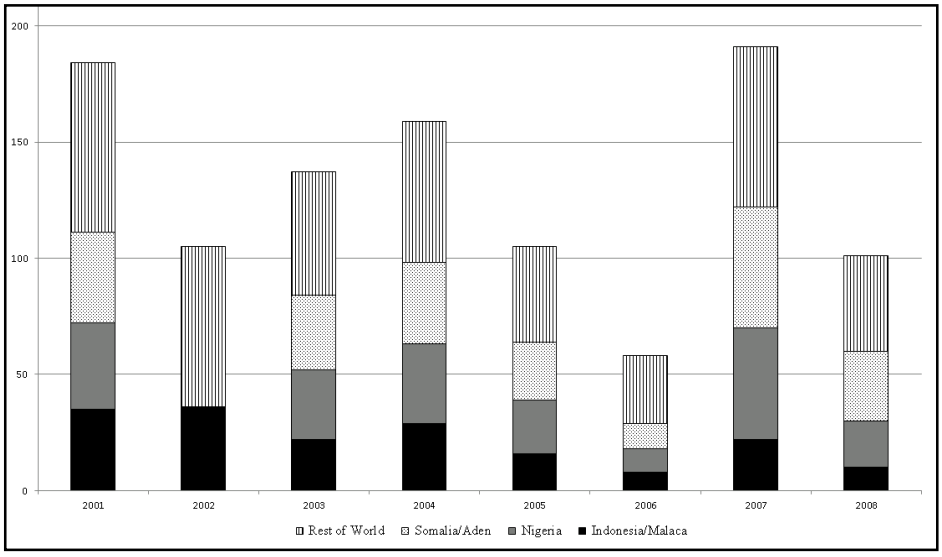


Figure 2-4 :Number of pirate attacks by country 2001–2008. Source: IMO database

2.2 Typology of threats against oil platforms

[Jenkins, 1988] established the first typology of threats to oil platforms based on feedback from reports. He identified:

- The bomb scare: this aims to disrupt operations by forcing an evacuation and generating an expensive and extensive search in order to end the alarm, which is usually false. However, Jenkins includes cases where a real bomb has been placed either by platform personnel or by underwater divers.
- Floating mines: remnants of the Second World War, they pose a very low level of risk.
- Sabotage: mainly by installation personnel or terrorist organizations.
- Boarding (or collision) by a non-governmental organization: usually to bring to the public's attention an environmental cause.
- The destructive attack: a terrorist attack by a guerrilla or regular army.
- Hostage-taking: this hypothesis was formulated by Jenkins based on the example of planes and trains. At the time the typology was established (1988), he had no feedback about it and estimated the risk to be low because of the resources that would have to be deployed and the difficulty of accessing an offshore platform.
- "Kamikaze" ships or an aircraft (piloted or not).
- Attacks against platform personnel: although this is similar to hostage-taking, here it relates to intercepting personnel before they assume their duties.
- Acts of piracy against offshore oil installations have increased considerably since 1988. In 2008, [Kashubsky, 2008] conducted a very detailed study of Nigeria. Here we have selected a few significant events as illustrations:
- On 12 June 2005 an armed group boarded the Jameston FPSO (floating production, storage and offloading unit) and took 45 hostages. They were released following the payment of a ransom three days later.
- On 11 January 2006 a Shell platform was attacked and four people were taken hostage from the maintenance vessel anchored to the platform.
- On 15 January 2006 a very violent attack against a Shell facility resulted in a fire, extensive damage and 17 deaths.
- On 18 February 2006 a speedboat attacked an installation and nine personnel were wounded.

- On 2 October 2006 Shell barges were attacked. Three soldiers were killed protecting the facility.
- On 1 April 2007 an installation suffered a dual attack. The maintenance ship was diverted by pirates who were then able to come alongside.
- On 19 April 2007 a security vessel was attacked; the pirates managed to strip it of its own weapons.
- On 3 May 2007 the FPSO Mystras was attacked; the attackers used the anchor chain to board. Eight employees were kidnapped.
- On 21 October 2007 a large armed group simultaneously attacked two maintenance ships.
- On 19 June 2008 the FPSO Bonga was attacked and damaged, production stopped, and losses were estimated at more than 200,000 barrels of oil per day.
- On 14 September 2008 platforms belonging to Shell and Chevron were simultaneously attacked.
- On 16 September 2008 eight speedboats loaded with dynamite and hand grenades attacked the Shell (Orubiri) pumping station causing extensive damage.
- Etc.

These events highlight the extent of the human, material and economic damage. They also highlight the forms of criminal action and strategies used by pirates: surprise, extreme mobility, rapid action, the small number of assailants and the weapons they use.

2.3 Protection of installations and shipping

Military authorities consider it impossible to protect all of the world's merchant fleet. It is the same for ships carrying energy products. The IMO has therefore issued a set of recommendations for ship-owners and crews aimed at ensuring the safety of persons, property and equipment. The IMO does not recommend arming ships and oil platforms in order to avoid violent confrontations. This is especially relevant given that pirates are particularly well-armed (with automatic rifles, grenades, etc.) and seem to favour hostage-taking and ransoms. This leads to hope that hostages will be well-treated and the rejection of a policy of armed and violent responses to attacks.

Merchant ships have two ways to respond to an attack: they can either seek to avoid it by changing routes and/or increasing ship security. The first option is not possible for oil platforms that are anchored to the sea bed. For them, detection and warning systems are essential.

The IMO has issued a series of recommendations that include:

- Increased and permanent vigilance.
- Increased use of detection technologies (radar, infrared, searchlights, etc.).
- Installation of audible alarms, illuminating suspicious vessels.
- Etc.

Despite these recommendations, some owners and operators have resorted to security companies. Most use non-lethal means to repel attacks. In November 2008, in the Gulf of Aden a security team defeated heavily armed pirates using water cannon combined with a noise repulsion device.

Table 2-1 provides an overview of the defensive actions implemented in Somalia in 2008 to prevent pirate attacks. The final column indicates whether the measure can be applied to offshore oil platforms.

Action taken by vessel	**Number of vessels taking action**	**Applicable to offshore platforms?**
Raised alarm	21	Yes
Took evasive manoeuvres	28	No
Increase speed	16	No
Crew mustered	8	Yes
SASS activated	2	Yes
Coalition warship advised/responded	12	Yes
Fire hoses activated	6	Yes
Sent distress signal	1	Yes
Fired flares	1	No
Sounded ship's whistle	1	Yes

Table 2-1 : Actions taken by ships to protect themselves against attack in Somalia January – September 2008. Number of attacks: 67 (Source: IMO Database).

The United States Department of Homeland Security has produced a set of recommendations for the protection of vessels. The document, entitled "Port Security Advisory (2-09) (REV 1)" advocates the following responses to an attack:

- Activate the alert system (in conjunction with the United States Coast Guard).
- Make a mayday call on the VHF channel.
- Inform local authorities.

- Inform the management of the operating company.
- Deploy the anti-aggression plan.
- Ensure that the AIS (Automatic Identification System) is operational.
- Send a distress message via systems such as Inmarsat-C.
- Prepare to move to the refuge area.
- Begin escape manoeuvres aimed at outrunning the attackers or enabling external intervention (for ships).
- Use non-lethal means aimed at stopping the intrusion and repelling the attackers.
- Owners and operators are asked to notify the attack (and suspected attacks) to the United States' authorities.

It is clear that the proposed methods and solutions are simple, limited, and to say the least, rustic. New technologies should be able to improve on these current prevention systems.

3. The contribution of Bayesian networks to reducing the vulnerability of offshore oil installations

This second part is organized into three sections. The first briefly outlines the operational requirements and constraints inherent in the design and development of a high-performance detection, alert and threat processing system. The second introduces the concept of the Bayesian network and the software tool used in development of the system. Finally, the third section describes how to construct a Bayesian network based on both quantitative data and expert knowledge.

3.1 Operational requirements and technical issues

To date, there is no technological solution on the market that manages the entire processing chain of a threat. The main systems currently available manage the detection and the response to a threat independently. Among detection tools, radar-based systems (pulses[13]) are able to locate large or medium-sized mobile vessels but they perform

[13] Radar emits microwave pulses towards the target. These signals are then reflected and intercepted by the radar receiver that also collects an electric signal called the "echo".

poorly in the detection of small craft (such as fishing boats, motor boats, etc.), in rough seas and moreover, are relatively slow to analyse a wide geographical area [Morel and al., 2011]. There are also optronic surveillance systems[14] which, despite their strengths in the long-range detection of small targets remain handicapped by problems of solar reflection on the sea surface and have proved to be very sensitive to weather conditions [Giraud and al., 2011]. As for counter-attack systems (water hoses, noise guns, etc.), they are often inappropriate or misused.

In terms of threat response, oil platforms that are the victim of an attack are able to broadcast warnings to security vessels deployed in the area, but their diffusion is geographically very restricted. Moreover, even if the security vessel is notified, its ability to intervene remains uncertain, particularly if it is remote from the location of the attack.

The goals of our research are therefore limited. We aim, taking into account work undertaken so far, to improve the ability of an installation to detect a threat, raise the alert and secure the installation if the threat is verified. There are many constraints inherent in this problem. The first challenge is a direct consequence of the large number of attack parameters. These include input and output system parameters related to the target (platform or mobile vessel), the danger (type, criticality, vulnerability, on-board security facilities, etc.), the threat (vessel used by the attackers, its speed, weapons, etc.) and the environment (time of day, visibility, sea state, etc.). The second challenge is that these parameters may interact. For example, whether it is relevant to request the intervention of the security vessel depends in particular on the time needed for it to reach the installation under attack, and the weaponry and speed of the threat. Therefore a second constraint lies in the management of the many interdependent relationships between system variables.

A further constraint is the need to take into account the uncertainty of threat data. The alert report not only contains aggregated data from detection instruments such as FMCW[15] radar (the type of vessel detected, number of occupants, potential weapons, etc.), but also mathematical calculations based on dynamic variables (distance between the target and the attacker, time before they are able to board the platform, etc.). This necessarily leads to the question of how to manage errors and false alarms. For example,

[14] These systems bring together optics and electronics. They usually consist of an optical sensor, an image processing system and a display or data recording system.
[15] Frequency Modulated Continuous Wave.

despite the improved performance of radar, the information it provides becomes increasingly unreliable as the distance to the threat increases, and the sea state deteriorates.

These constraints suggest the design and development of a decision support system based on graph theory [Harris, 2011] that is able to translate and exploit (by means of a graph) a large number of variables, their dependency relationships, impacts, etc. When the uncertainty inherent in the data is taken into account, the need to find a solution that is based on probability theory and probabilistic calculations is clear. We therefore propose a model based on Bayesian networks. This tool should be able to automatically prepare response plans tailored to the nature of the detected intrusion.

3.2 Bayesian networks and BayesiaLab software

Depending on the application, the practical implementation of a Bayesian network is similar to that of other models: neural networks, expert systems, decision trees, data analysis (linear regression) models, fault trees and logical models. Naturally, the choice of method depends on criteria such as ease of use, and the cost and time needed to implement a solution. In addition to theoretical considerations, the following aspects of Bayesian networks make them, in many cases, a better choice than other models [Becker and Naïm, 1999]:

- Knowledge acquisition. The ability to collect and merge different kinds of knowledge in the same model: feedback (historical or empirical data), expertise (expressed as logical rules, equations, statistics or subjective probabilities) and observations.
- Knowledge representation. The graphical representation provided by a Bayesian network is explicit, intuitive and understandable by a non-specialist. This facilitates both the validation of the model, it’s possible extension and particularly its use. A decision-maker is more likely to rely on a model that they understand and know how it works, than to trust a black box.
- Knowledge use. A Bayesian network is versatile: the same model can be used to assess, predict, diagnose, and optimize decisions, all of which helps to recover its initial development costs.

- Quality of software. Nowadays there are various software tools available to understand and process Bayesian networks. These tools offer functionality that is more or less advanced: probabilistic learning, learning the structure of the Bayesian network, the option to integrate continuous, utility and decision variables, etc.

A Bayesian network can both represent knowledge and make it possible to calculate conditional probabilities. Widely used for diagnosis (medical or industrial) [Lee and Lee, 2006], they can capitalize and exploit knowledge and are particularly suitable for the assessment of uncertainty [Hudson and al., 2002], [Martin and al., 2009].

A Bayesian network BN is a directed acyclic graph defined by a set of nodes corresponding to attributes H and by $E \subset H \times H$, the set of arcs of the graph. A conditional probability distribution $P_{A_i|\Pi_{A_i}}$ is associated with each node, where $\Pi_{A_i} = \left\{ A_j \middle| \left(V_{A_j}, V_{A_i}\right) \in E \right\}$ are the parents of node Ai. One of the properties of a Bayesian network is that it uniquely defines the joint probability distribution over H:

$$P_H^{RB} = \prod_{i=1}^{n} P_{A_i} \middle| \Pi_{A_i} \qquad (1)$$

An association rule R is a pattern $X \Rightarrow Y$, where X and Y are itemssets such as $Y \neq \phi$ and $X \cap Y = \phi$. X denotes the left side of the rule and Y the right side. Let I be an itemset. The support for I in database BD, denoted suppBD (I) is the set of records (or transactions) of BD that contain I.

Thus, given a database BD defined on a set of attributes H and a Bayesian network BN, we obtain the confidence of the association rule $R = X \Rightarrow Y$ [Kalev and Dechter, 1999]:

$$Conf_{BD}(X \Rightarrow Y) = P_{Y|X},$$
$$= \prod_{i=1}^{m} P_{Y_i} \middle| \Pi_{Y_i} \qquad (2)$$

And from data estimates:

$$Conf_{BD}(X \Rightarrow Y) = \frac{\text{supp}_{BD}(X \cup Y)}{\text{supp}_{BD}(X)} \quad (3)$$

In our study, the Bayesian network is used to develop a tailored, graduated and progressive response to a threat. Database records and the knowledge of experts in the maritime and oil domains are used to overcome the initial lack of knowledge and feedback from the application domain.

BayesiaLab software was used to construct the Bayesian network. This is a decision support tool for modelling uncertain knowledge. It provides analysis, diagnosis, simulation, optimization and risk management functions and offers two methods to develop a Bayesian network:

- Automatic "data mining" modelling. This module makes it possible to collect and merge various kinds of knowledge in the same model (e.g. historical or empirical data). The software provides several functions to construct a Bayesian network from an imported data source: definition of missing and filtered values, definition of an initial network, supervised learning, clustering, probabilistic structural equations, integration of continuous, utility and decision variables, etc.
- "Brainstorming" modelling. This enables the construction of a Bayesian network based on expert knowledge. The benefit of this model is the constructive discussion between experts that makes it possible to model situations that are rare or have not yet occurred. The drawback is that expert knowledge is often incomplete, partially incorrect and subjective. The development of a Bayesian network through brainstorming involves three key steps. The initial step is to clearly define objectives, prepare a list of dimensions, and define the variables related to each dimension (their type and states) taking into account the need to minimize the number of states. Next, structural modelling consists of determining cause and effect relationships and adding new variables that simplify the network. Finally, parametric modelling techniques are used to elicit knowledge.

These two types of modelling are complementary and are used to construct a Bayesian network based on data mining and expert knowledge. The usefulness of the graphical representation of a Bayesian network is very dependent on the number of nodes that compose the network. The software offers two algorithms for automatic positioning:

- A dynamic algorithm suitable for arborescent or weakly connected structures that takes account of parental relations between nodes, the force of arcs and the weight of nodes defined according to the number of children and parents of each node.
- A genetic algorithm for processing more complex networks. This algorithm can take into account the relationships between nodes, the force of arcs, overlapping nodes and the intersection of arcs with other arcs and nodes.

For the analysis of results, the software provides four tools:

- Arc analysis is provided by a comprehensive tool that highlights the force of arcs. Arc thickness reflects the strength of the probabilistic relationship it represents in the associated probability law.
- Target node analysis is a more localised tool. The analysis focuses on a target variable, which enables the user to see the amount of data contibuted by each node to the knowledge of the target node.
- The target node state analysis tool makes it possible to visualise, for each node, two pieces of information related to its probabilistic relationship with the target variable: the influence of the variable on a particular state of the target variable, and the information gain provided by the node to the knowledge of the target state.
- Causal analysis is a tool to remove the orientation of arcs whose orientation can be inverted without changing the joint probability law.

In addition to these analysis tools the software makes it possible to edit the report. This HTML report provides a description of all observed variables, probability distributions, etc. The software can also prepare a second report focused on a global analysis of all observations. The purpose of this report is to determine whether there are contradictory findings or if they all point in the same direction.

3.3 Coupling of quantitative and qualitative knowledge

A key feature of our Bayesian network is that it combines quantitative knowledge from the IMO database and qualitative knowledge acquired from experts in the maritime domain.

The first step was to construct a Bayesian network from records related to attacks against vessels and offshore platforms, while the second step used expert knowledge to refine the results and add counter-measures.

Quantitative data was provided by the IMO's Piracy and Armed Robbery database. This is the only database in existence containing records (dating back to 1994) of piracy attacks in the maritime environment. In July 2011 it contained 5,502 records, and data included: the name of the asset attacked, the number of people involved in the attack, the type of weapons used, the measures taken by the crew in order to protect themselves, the impact on the crew and the pirates, etc.

The software automatically generated a Bayesian network from this data and suggested dependency relationships between the main database elements. It also offers various unsupervised learning methods (e.g. data segmentation algorithms or target node characterization). We decided to use an association discovery algorithm as it generated the most relevant model.

Figure 2-5 shows the Bayesian network built from the IMO database.

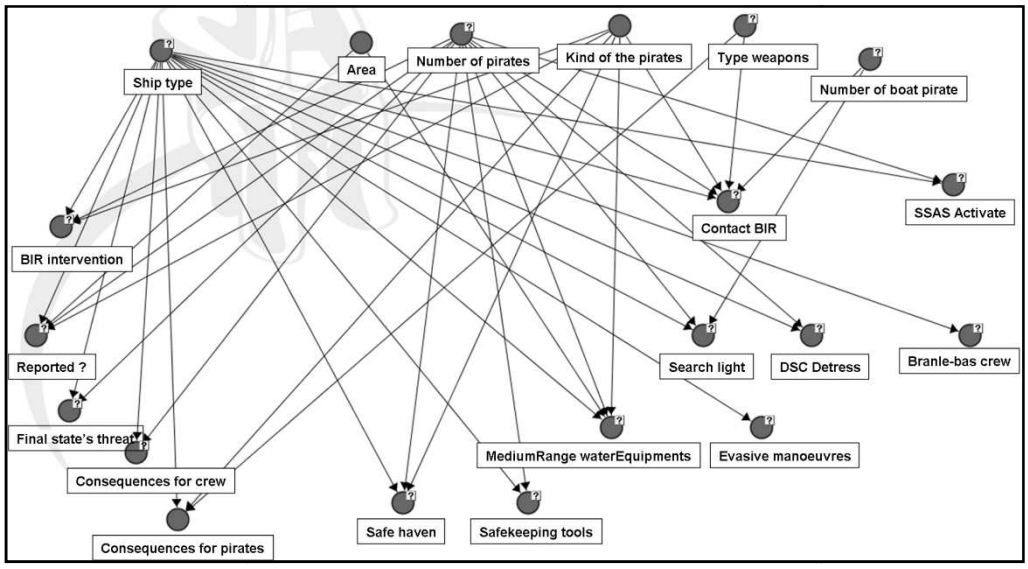


Figure 2-5 : The Bayesian network generated from IMO data

Information such as longitude, latitude, name of the asset attacked, etc. was not retained as these fields were not listed for all attacks. The network contained around

twenty nodes related to the type of vessel attacked, the location of the attack, the type of weapons used by the pirates, their numbers, etc. The relationships between these variables were identified through an automatic learning process.

A classical statistical analysis of this data provided a first set of information. The most interesting results included: most ships that are attacked are bulk carriers or tankers, 48% of attacks take place in international waters (due to the absence of security controls), and pirates benefit from attacking in numbers (68% of attacks are carried out by teams of five or more). As a result of this network, a clear picture emerged of pirate tactics, their weapons and particularly the number of people involved.

In the example that follows, specific threat nodes characteristics were set in order to identify counter-measures used by the crew of the attacked target. Figure 2-6 illustrates the selected hypothesis:

- The asset under attack: a tanker.
- The location of the accident: international waters.
- Type of attackers: thieves.
- Type of weapon: gun.

In this example, the Bayesian network indicates that (as in most cases) the assailants fired shots at the target and that the crew, to protect themselves from this danger, applied evasive manoeuvres and used water hoses on the attackers.

This analysis of the IMO database made it possible to identify the main actions taken by most entities when attacked, namely: initiate evasive manoeuvres, activate the SSAS alert system, contact the security vessel, secure the crew, activate searchlights, etc. The network created from the IMO database also made it possible to determine the principal tools and methods used by the crew of attacked entities to protect themselves, to evaluate the effectiveness of these tools and to define the probability of certain types of attacks.

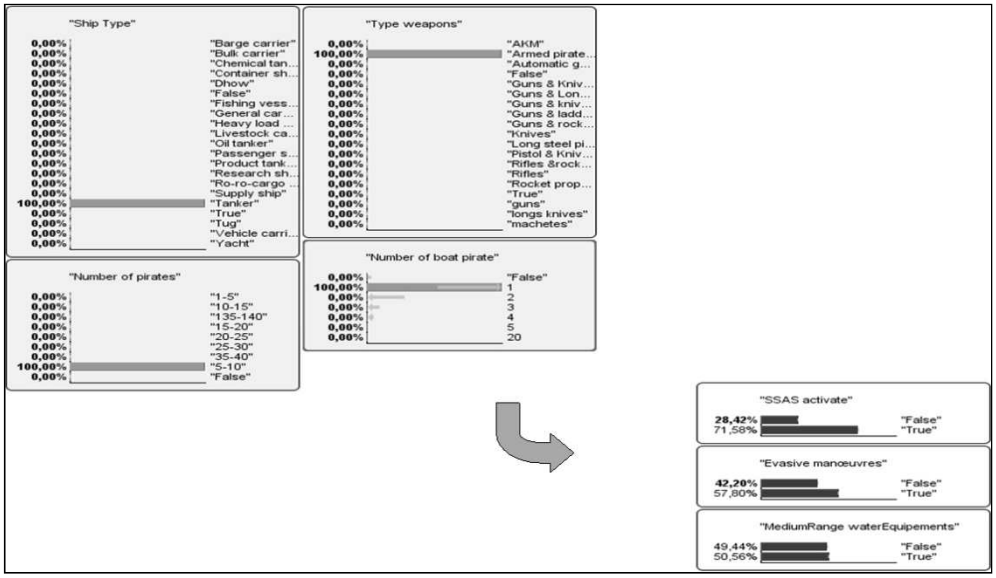


Figure 2-6 : Attack scenario against a tanker

This Bayesian network, through its states and conditional probabilities provided a formal framework into which maritime domain experts were able to add their knowledge in order to build a second Bayesian network.

The second step of the methodology consisted of the analysis of information extracted from the IMO Bayesian network by maritime and oil experts. The IMO database primarily contains information related to attacks on shipping. Experts were able to contribute knowledge that made it possible to transpose the results to oil fields: nodes and arcs were added to make the model as versatile as possible. Although each Bayesian network is unique for the two broad categories of target (shipping or oil platforms), the input variables are the same regardless of the nature of the target (type of ship, threat, kinematics, etc.). However, the counter-measures recommended by the network are tailored to the type of target (for example evasive manoeuvres are not proposed for an offshore platform).

This new Bayesian network, tailored to the constraints and conditions found on oil platforms was developed as a result of numerous brainstorming sessions during which maritime and security experts shared their experiences and discussed network states and probabilities [Chaze and al., 2012].

The complementarity of the IMO data and the knowledge of maritime and offshore security experts made it possible to generate a response planning network. The architecture consists of four modules and five sub-modules (Figure 2-7).

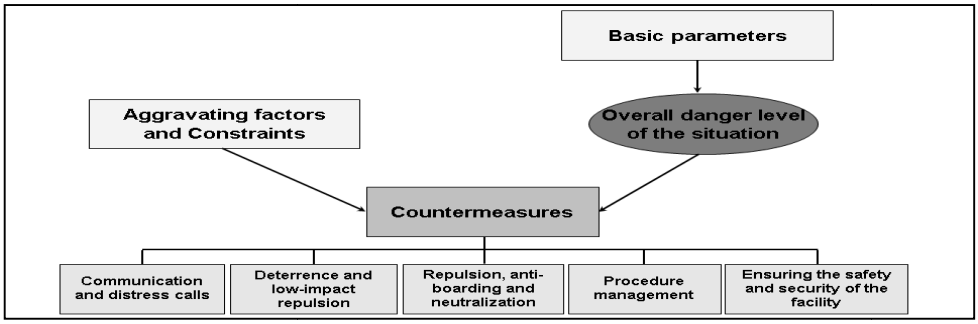


Figure 2-7 : Structure of the Bayesian network

The scope of each of these modules is directly related to the meaning of its constituent nodes. The classification includes basic parameters, the overall danger level of the situation, aggravating factors and constraints, communication nodes, those related to requests for help and counter-measures, given in Table 2-2.

<table>
<tr><th colspan="4">Basic parameters</th></tr>
<tr><td colspan="4">Static or dynamic physical data that characterise the threat and the target. They can be the direct result of the alert report, or are derived from intermediate calculations. They constitute the minimum level of modelling that is sufficiently detailed to give a full understanding of the threat / target in the response scenario.</td></tr>
<tr><th colspan="4">The overall danger level of the situation</th></tr>
<tr><td colspan="4">Calculated from basic parameters, this level ranges from 1 to 4 (maximum overall danger level) and changes in real time in response to the situation in order to plan appropriate counter-measures.</td></tr>
<tr><th colspan="4">Aggravating factors and constraints</th></tr>
<tr><td colspan="2">Aggravating factors make it possible to take into account the potential deterioration of the situation and therefore to anticipate alternative plans (such as environmental factors: visibility and time of day).</td><td colspan="2">Constraints are represented by parameters that can influence the effectiveness of the response. They are directly related to the ease of use of counter-measures (such as the immediate availability of an operator or whether the device can be operated remotely).</td></tr>
<tr><th colspan="4">Counter-measures</th></tr>
<tr><td colspan="4">These are defensive measures that are implemented by the target under attacked in order to protect itself against an identified threat and to normalize the situation as soon as possible. Counter-measures are the physical manifestation of the response plan and are increasingly forceful depending on the nature of the threat detected.</td></tr>
<tr><th>Communication and the request for help</th><th>Low-level repulsion measures</th><th>Repulsion, anti-boarding and neutralisation measures</th><th>Prodedure management</th></tr>
<tr><td>Objectives:
- Alert relevant personnel.
- Warn, at various levels of intervention, maritime security actors (security vessels, coastal countries).
This enables installations and and vessels in the oil field to anticipate their response plan and find out if outside intervention is possible.</td><td>Objectives:
- Advise the attackers that the target knows their intentions and is able to respond.
Small-scale repulsion is the ability of the target to repel the attackers using low-level methods (searchlights, fire hoses, sound guns).</td><td>Objectives:
– Slow down the progress of the attack to give the crew enough time to prepare other security measures.
- Slow down or neutralise the attackers.
These active counter-measures have a high impact and rely on equipment that can repulse an attack from a distance while remaining within the framework of non-lethal self-defense.</td><td>Objectives:
- If there is a security alert, sound action stations and gather crew at pre-defined assembly points.
- Secure the installation (activate the citadel, stop production, secure access to sensitive areas, etc.).</td></tr>
</table>

Table 2-2 : Bayesian network modules

In this Bayesian network each module or sub-module consists of one or more nodes that receive and /or transmit causal relationships to other nodes. Each node is composed of a matrix of conditional probabilities that is calculated taking into account the various interactions with other nodes and the actual reality that the node itself represents. For

example, the probability distribution of activating searchlights (“Activate Search Light”) is directly subject to interactions with visibility, time of day and technical constraints such as availability and remote control.

The probabilities of base nodes were standardised and elements characterising a specific attack were not included. The initial probability distribution for activation of the sonic cannon (“Activate LRAD”) is therefore distributed as follows: stand-by; 99.51%: Activate LRAD Loudspeaker; 0.27%: Activate LRAD Sonic Weapon; 0.22%.

In the next section we assess the relevance of our Bayesian network using a set of attack scenarios.

4. Attack scenarios and discussion

This last part is organized into two sections. The first describes the test scenarios. The second describes the integration of the Bayesian network into a global system for the management of alerts and responses, namely SARGOS.

4.1 Attack scenarios: case studies

Several scenarios were developed to test the ability of the Bayesian network to prepare real-time response plans tailored to a detected intrusion. These scenarios were developed in collaboration with experts (Table 2-3).

Threat type	**Target type**	**Context**	**Distance target / threat**	**Time target / threat**	**Time for the security ship to react**	**Danger level**
Unknown	FPSO (critical importance)	Good visibility Daytime	200 < d < 500 m	900 s < t	t < 300 s	**2 (64.68%)**
Highly manoeuvrable vessel (firearms detected)	FPSO (critical importance)	Poor visibility Night	d < 50 m	t < 300 s	900 s < t	**4 (79.79%)**
Unknown	FPSO (normal importance)	Poor visibility	200 < d < 500 m	t < 300 s	300 < t < 900 s	**2 (50.73%)**
Unknown (handguns	FPSO (critical	Good visibility	50 < d < 200 m	300 < t < 900 s	900 s < t	**3 (45.21%)**

detected)	importance)					
Inconnu (handguns detected)	FPSO (critical importance)	Good visibility Dawn-dusk	d < 50 m	t < 300 s	t < 300 s	**3 (56.40%)**

Table 2-3 : Test scenarios developed in collaboration with experts

Figure 2-8 shows in detail the results of the insertion of parameters modelling an attack on an FPSO unit by an unknown assailant (scenario 1).

This example shows that the danger level of the situation is 2 with a 64.68% probability of occurrence. In this case, counter-measures to be applied are: inform the crew master, request the intervention of the security vessel, broadcast a loud, clear message using the long-range loudspeaker, activate searchlights, engage the safety post and activate repulsion equipment.

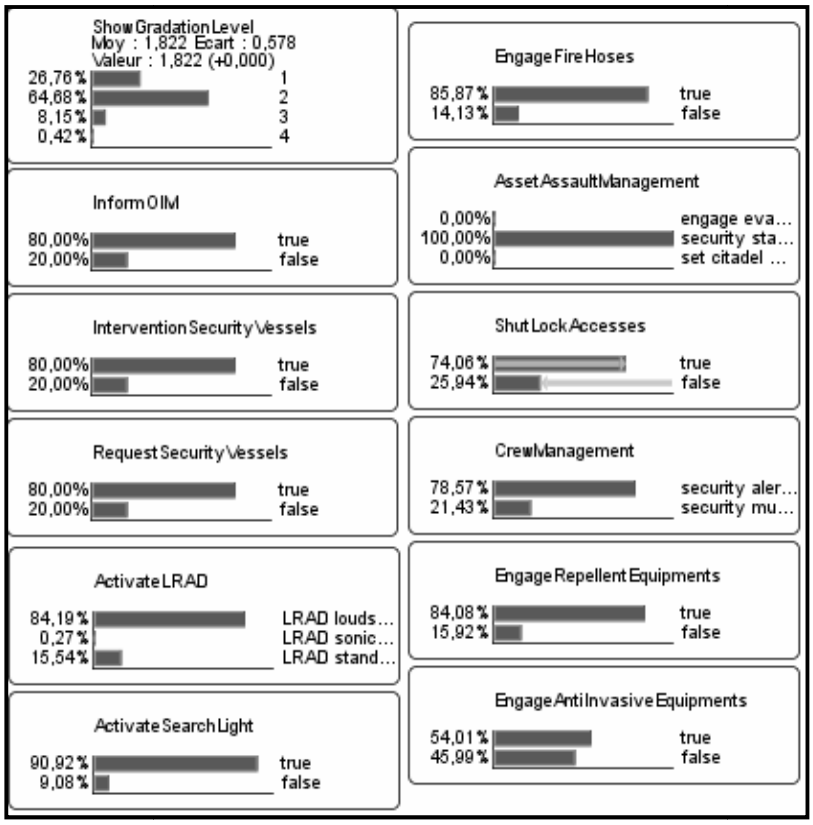


Figure 2-8 : Response planning following the insertion of an attack on an FPSO unit from an unknown source

Planning can be tailored to the danger level of the situation and is adapted as threat and target parameters change.

The generation of attack scenarios makes it possible to refine probabilities and test the reaction of the Bayesian network by varying threat, target and environment parameters. These scenarios made it possible to assess the relevance and consistency of the counter-measures proposed by the network, which can be iteratively improved.

4.2 Integration of the Bayesian network into the SARGOS system

The SARGOS[16] system [Bouejla and al., 2012] is designed to meet the emerging need for security on offshore civilian infrastructure that is vulnerable to malicious acts of piracy or terrorism conducted at sea. The aim is to develop a system that ensures a coordinated, global protection chain (Figure 2-9). It includes:

- Monitoring and automated monitoring. The combination of a specialised radar (FMCW technology) and conventional sensors helps to detect intrusions from small boats and commonly-used vessels.
- Assessment of the danger level. An intelligent analysis of the characteristics of the detected object makes it possible to classify and assess the danger level. When the level exceeds the pre-set alarm threshold, an alarm is generated and the operator is alerted via a message sent to a mobile terminal.
- Development of a graduated response plan that can be controlled in real time. A situation analysis automatically creates, from the Bayesian networks, response plans tailored to the nature of the detected intrusion. The plan takes into account the infrastructure's operating modes and the regulatory and legal context of the oil field.

One of the key capabilities of the SARGOS system is a comprehensive threat response strategy that can ensure personnel safety, raise the alarm, coordinate external means of assistance and recommend non-lethal deterrents. It was implemented using a transverse system approach and is based on innovative technologies that were developed using the complementary skills of project partners[17]. It can ensure the automatic

[16] Système d'Alerte et de Réponse Graduée OffShore. ProjetANR-09-SECU-009 - Programme CSOSG 2009

[17] SARGOS project partners are :

SOFRESUD, 777 av. de Bruxelles, 83500 La Seyne sur Mer

ARMINES/CRC, Rue Claude Daunesse, 06904 Sophia Antipolis

CDMT, 3 avenue Robert Schuman, 13628 Aix en Provence Cedex 1

protection of offshore infrastructure faced with new forms of piracy by triggering the relevant actions at the appropriate time.

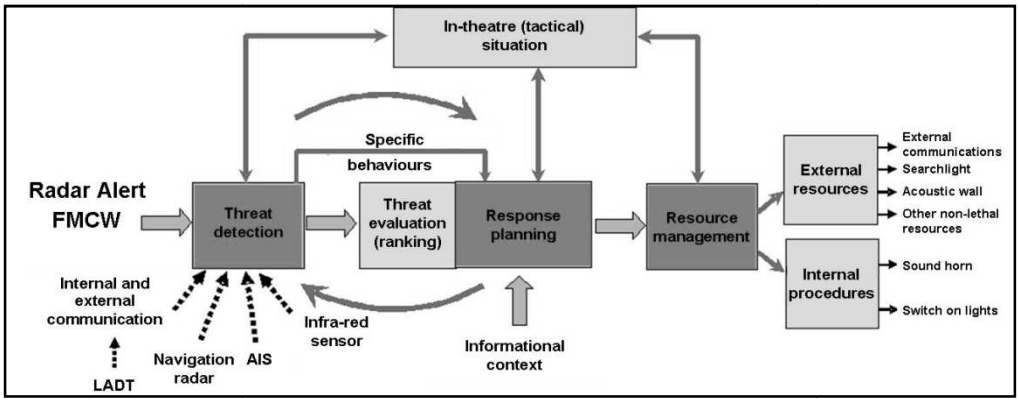


Figure 2-9 : The architecture of the SARGOS system

We have developed a prototype that integrates the Bayesian network into the SARGOS system. The prototype takes an alert report as input and generates a planning report as output. The output report contains all the counter-measures to be applied either manually by the crew or automatically by the system.

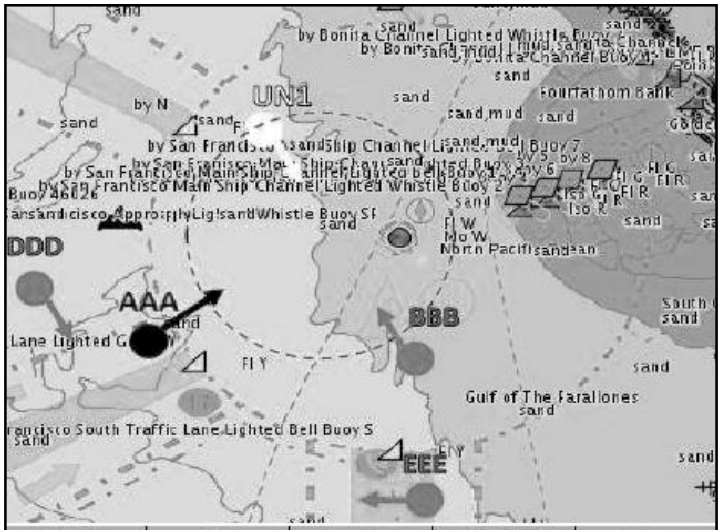
The results of intermediate calculations are fed into the Bayesian expert knowledge network. BayesiaEngine software provides an application programming (API) interface and a Java library. Through this module, attack parameters can be inserted into the network.

The selection of counter-measures varies according to the situation. It is therefore possible to set an activation threshold in order to only include those counter-measures that are most appropriate at a particular time, in a given situation. We decided to set this threshold at 70%. This means only those counter-measures where the probability of one of its states is greater than 70% are integrated into the planning report. This threshold was selected by domain experts as it is actually the case in more than two-thirds of incidents encountered in real life. After numerous trials and adjustments, the output of the network corresponded to realistic and reliable responses.

Once appropriate counter-measures have been selected they are included in the planning report, where they are displayed in a specific order. The main factors affecting the priority are: the action mode of the counter-measure, its ease of implementation, whether it can be activated automatically or manually, the time required before it becomes effective, and any additional functions.

The SARGOS system can handle multiple threats in one alert report. The first threat to be processed is always that which has the shortest response time for the most exposed potential target. Figure 2-10 demonstrates the interface of the SARGOS system and shows the simultaneous processing of multiple threats.

In this example, the system has detected a set of entities that are heading towards an oil field. It has classified them as “Enemy”, “Unknown”, or “Friend”. An alert is only generated for entities classified as “Enemy” and “Unknown”. Following this initial processing, the planning report is divided into two parts. The first applies to the whole oil field and concerns communication and a request for support (left-hand side of Figure 2-11); the second relates to the specific target in danger and displays a prioritised list of the countermeasures to be activated (right-hand side of Figure 2-11).



Class	ID	CPA	TCPA	Type
Enemy	AAA	2. 3 m	3. 30 mn	Small Boat
Unknown	UN1	1.5 m	2.20 mn	
Friend	BBB	2.8 m	4.15mn	Tanker
Friend	CCC	0		Tanker
Friend	DDD	0		Small boat

Figure 2-10 : The SARGOS man-machine interface showing threat classifications

On the left-hand side of Figure 2-11, the vertical division visible in the request for the intervention of the security vessel represents the resulting probability.

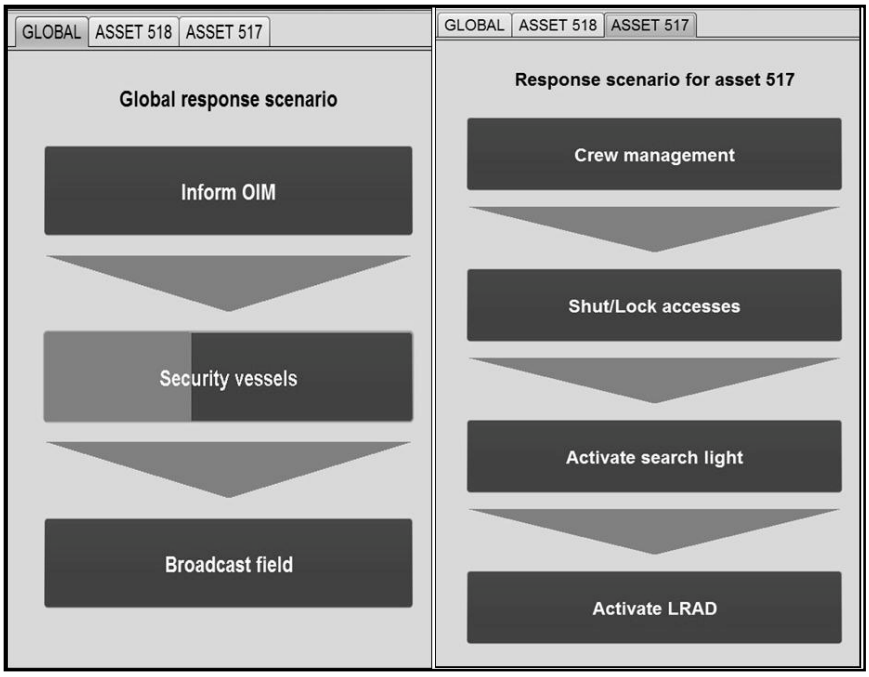


Figure 2-11 : The SARGOS man-machine interface showing global (left-hand side) and local (right-hand side) counter-measures to be applied.

5. Conclusions and future work

The problem of acts of piracy against oil infrastructure is complex. In an open space that is subject to many environmental constraints, the difficulty of assessing a potential threat, the constant evolution of a dangerous situation, as well as the need to manage a large number of parameters weaken the effectiveness of protection measures.

The use of a Bayesian network for planning the response to a threat therefore represents real progress. The network can manage potential interactions between threat characteristics, the target under attack, the environment, and crew and facility management. Most importantly, it can adapt in real-time to changes in the danger level of the situation. The proposed response is translated into a planning report, which is the output of the intelligent processing of successive warning reports that reflect the evolution of the situation. The network can be scaled through the integration of feedback from previous attacks managed by the system. Through this mechanism, the planning module is progressively better adapted and iteratively improved.

Dynamic Bayesian networks [Dean and Knazawa, 1989] provide another avenue for exploration. Interest in these networks has seen significant growth as a way to generalize Hidden Markov Models or Kalman Filters in applications such as speech recognition, state estimation in dynamic models, etc. A dynamic Bayesian network is a factored representation of a Bayesian network where the nodes are time-indexed on a discrete scale. The nodes are indexed over adjacent time steps and there are two types of links: classic Bayesian network links and so-called temporal relationships. The latter make it possible to define conditional probability tables for a node depending on the state of its parents at an earlier point in time. The application of a dynamic Bayesian network to the SARGOS system makes it possible to integrate notions of time into the decisions to be taken in response to an attack and its influence on the evolution of the threat.

Finally, another interesting approach would be to drawn upon a tailored ontology [Vandecasteele and Napoli, 2012]. This would potentially improve the model of knowledge integrated into the Bayesian network. It would make it possible to formalize knowledge upstream and consolidate threat detection and identification steps.

References

Becker A. and Naïm, P. (1999). Les réseaux bayésiens. Modèles graphiques de connaissances. Editions Eyrolles.

Bouejla A., Chaze X., Guarnieri F. and Napoli A. (2012). Bayesian networks in the management of oil field piracy risk. 8th International Conference on Risk Analysis and Hazard Mitigation, Island of Brac, Croatia.

Brown N. (2006). Taking the Fight to the Pirates. Jane's Information Group.

Burnett J.S. (2002). Dangerous Waters: Modern Piracy and Terror on the High Seas. New York: Dutton.

Chaze X., Bouejla A., Guarnieri F. and Napoli A. (2012). The contribution of Bayesian networks to risk management in oil field piracy. ITEMS2012, Busan, South Korea.

Dean T. and Knazawa K. (1989). A model for reasoning about persistence and causation. Computational Intelligence, pp. 142–150.

Dillon D.R. (2000). Piracy in Asia: A Growing Barrier to Maritime Trade. Heritage Foundation Backgrounder, volume 1379, www.heritage.org.

Giraud M.A., Alhadef B., Guarnieri F., Napoli A., Bottala-Gambetta M., Chaumarin D., Philips M., Morel M., Imbert C., Itcia E., Bonacci D. and Michel P. (2011). SARGOS : Système d'Alerte et Réponse Graduée OffShore. WISG 2011, Troyes, France.

Harris B. (2011). Graph theory and its applications: proccedings. Academic Press, University of Michigan.

Hudson L.D., Bryan S.W., Mahoney S. and Blackmond K. (2002). An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners.

International Maritime Organization. (2008). Reports on Acts of Piracy and Armed Robbery Against Ships. www.imo.org.

Jenkins B.M. (1988). Potential threats of offshore platforms. Rand Corporation.

Kalev K. and Dechter R. (1999). Stochastic local search for Bayesian networks. 7th International Workshop on Artificial Intelligence and Statistics.

Kashubsky M. (2008). Offshore energy force majeure: Nigeria's local problem with global consequences. Maritime studies.

Lee C. and Lee K.J. (2006). Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal. Reliability Engineering & System Safety, volume 91, n°5, pp. 515–532.

Martín J.E., Rivas T., Matías J.M., Taboada J. and Argüelles A. (2009). A Bayesian network analysis of workplace accidents caused by falls from a height. Safety Science, volume 47, n°2, pp. 206–214.

Morel M. and Broussolle J. (2011). I2C, Interoperable sensors and Information sources for Common Detection of abnormal vessel behaviours and Collaborative suspect events analysis. MAST 2011, Marseille, France.

Nincic D.J. (2009). Maritime Security as Energy Security: Current Threats and Challenges. In Luft, G., and Konin, A., eds. Energy Security: Challenges for the 21st Century. Washington DC: Greenwood Publishing in collaboration with the Institute for the Analysis of Global Security (IAGS).

Ryan M.(2006). Captain counts the cost of piracy. BBC News, news.bbc.co.uk.

United Nations. United Nations Convention on the Law of the Sea. www.un.org.

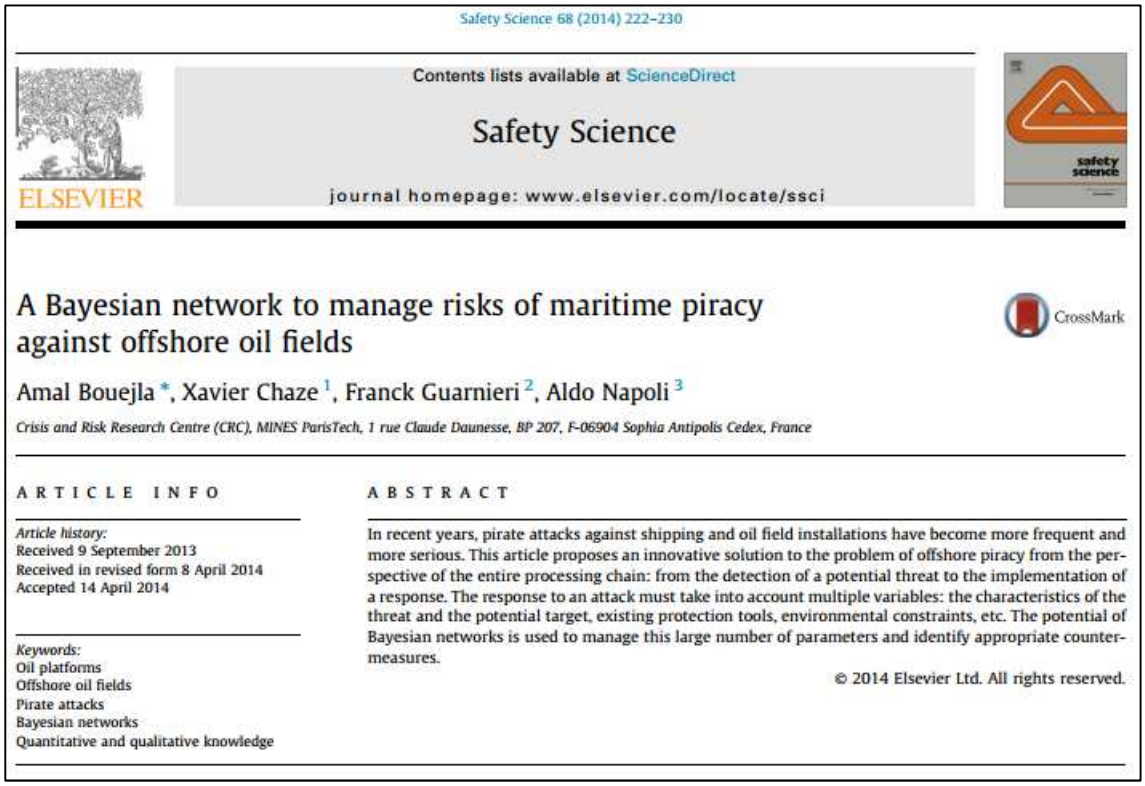
Vandecasteele A. and Napoli A. (2012). Spatial ontologies for detecting abnormal maritime behaviour. OCEANS2012, Yeosu, South Korea.

Chapitre 3 : Article 2 : Un Réseau Bayésien pour manager le risque de Piraterie Maritime contre les Champs Pétroliers Offshores

3.1. Présentation de l’article

L’article a été publié en octobre 2014 dans la revue Safety Science. Cet article est centré sur le management et l’analyse des risques de piraterie maritime.

3.2. Version anglaise de l'article



Safety Science 68 (2014) 222–230

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

A Bayesian network to manage risks of maritime piracy against offshore oil fields

Amal Bouejla *, Xavier Chaze [1], Franck Guarnieri [2], Aldo Napoli [3]

Crisis and Risk Research Centre (CRC), MINES ParisTech, 1 rue Claude Daunesse, BP 207, F-06904 Sophia Antipolis Cedex, France

ARTICLE INFO

Article history:
Received 9 September 2013
Received in revised form 8 April 2014
Accepted 14 April 2014

Keywords:
Oil platforms
Offshore oil fields
Pirate attacks
Bayesian networks
Quantitative and qualitative knowledge

ABSTRACT

In recent years, pirate attacks against shipping and oil field installations have become more frequent and more serious. This article proposes an innovative solution to the problem of offshore piracy from the perspective of the entire processing chain: from the detection of a potential threat to the implementation of a response. The response to an attack must take into account multiple variables: the characteristics of the threat and the potential target, existing protection tools, environmental constraints, etc. The potential of Bayesian networks is used to manage this large number of parameters and identify appropriate countermeasures.

© 2014 Elsevier Ltd. All rights reserved.

1. Introduction

Currently there are over seven thousand oil platforms scattered throughout the world, each of which requires on the one hand, equipment for the extraction, processing and temporary storage of petroleum, and on the other hand shipping capable of transporting crude oil between production and consumption sites.

Modern piracy is currently the major threat to the security of these energy production sites and maritime crude oil transport. In 2011, 552 attacks on ships and platforms were registered with the International Maritime Bureau[18] compared to 487 reports in 2010. At production sites, monitoring methods are a major weakness in the detection of a threat, and the procedures to be applied in the event of an attack are often inefficient and inappropriate. It is therefore essential to have a system that ensures the security of oil fields and offers them appropriate protection and effective crisis management.

[18] International Chamber of Commerce International Maritime Bureau's Piracy Reporting Centre (http://www.icc-ccs.org)

The SARGOS[19] system, funded by the National French Research Agency[20] (L'Agence Nationale de la Recherche) and recognised by regional organisations addresses this need by offering a global protection system in the fight against oil infrastructure piracy.

This article is organised into three parts. It first addresses the issue of acts of piracy against oil fields. Next the method used for the planning of counter-measures is described in detail. This includes notably, the construction of Bayesian networks from two datasets: the "Piracy and Armed Robbery" database of the International Maritime Organization (IMO) and the collection and formalisation of the knowledge of domain experts. Finally, the article describes how the model was tested using realistic and comprehensive pirate attack scenarios and the results are discussed.

2. Piracy against Oil Installations: a Serious Threat and Limited Defences

Offshore oil infrastructure is subject to a constantly increasing risk of piracy. The consequences of these actions have repercussions as much at a local level (on operations) as globally (on distribution). This section highlights both the economic and the political implications of pirate attacks and describes an increasingly insecure context where actors in the offshore oil and gas industry, without effective tools to protect themselves, find themselves helpless. Finally, it presents the SARGOS system and describes the contribution that this new system is expected to make to dealing with the problem of maritime piracy.

2.1 Economic and political issues

Offshore oil exploration is expanding rapidly. The exploitation of offshore oil resources currently represents about a third of global petroleum production. This energy resource, despite its scarcity, is being explored in many areas some of which are located

[19] The Offshore Warning and Graduated Response System (*Système d'Alerte et de Réponse Graduée OffShore*).

[20] The SARGOS project includes participants from private sector organisations such as DCNS (a French naval shipbuilder) and SOFRESUD (a supplier of high-tech equipment to the defence industry), and public research centres including ARMINES (a French contract research organisation) and TéSA (Telecommunications for Space and Aeronautics).

in dangerous territorial waters, notably the Gulf of Guinea. In the offshore waters of politically unstable countries, attacks on oil field infrastructure generate significant additional costs – caused by, for example the payment of ransoms, increased insurance premiums and the installation of security equipment. The annual cost of piracy is estimated at 7-12 billion United States dollars [BMI, 2011]. These additional costs directly affect the international price of oil.

Moreover, oil fields form the interface between the maritime world and the oil and gas industry. The heterogeneity of applicable regulation (rather than the absence of law) makes the status of installations a legal headache. Moreover, this complexity can lead to political conflicts between nations; when the nationality of the company operating the platform does not correspond to physical location of the installation, the problem arises of who has responsibility for the protection of the area [Schroeder and al., 2004].

The importance of oil installations in the global economy and industry and the potential political consequences of piracy therefore require that such assets are better protected.

2.2 Violent attacks

Although attacks against oil fields are infrequent and mostly low-profile, they are extremely disturbing because of the severe impact on the crew and infrastructure.

The following examples demonstrate the point:

- On 22nd September, 2010 the tug Bourbon Alexandre located in the Addax oil field off the Nigerian coast was attacked by four speedboats; three French sailors were taken hostage. This was the fourth attack against the Bourbon Company since 2009.
- The attack on the Exxon Mobil platform off the coast of Nigeria, led to the kidnapping of nineteen of its employees and significant damage to the oil facility caused by explosive devices used by the pirates.
- Finally, on 17th November, 2010 pirates aboard a speedboat attacked a ship owned by the French company Perenco that was carrying Cameroonian security forces near an oil platform in the Gulf of Guinea. The attack killed six people.

Infrastructure managers, employees and safety officers do not want to continue to see their ships or other assets become the subject of substantial ransoms, nor crewmen injured, killed or kept in extreme conditions for days or even weeks. At the same time insurers are unwilling to continue to provide cover for such high risks indefinitely. Finally, nations do not want to continue to see the price of oil affected by such events.

2.3 Emerging operational requirements

The attacks described above are a perfect illustration of the weakness of current anti-piracy tools. At the present time, there is no comprehensive system capable of managing the entire threat processing chain. Current systems treat the detection of a threat and the response to it as independent operations. Among the available detection tools, radar-based (pulse) systems[21] can spot large or medium-sized cooperative mobile objects but perform poorly in the detection of small craft (e.g. fishing boats and motor boats) in a rough sea; moreover the analysis of a large domain is relatively slow. There are also optronics surveillance systems[22] that, despite their ability to detect small targets at long-range, are handicapped by the problem of solar reflection from the sea and are very sensitive to weather conditions. As for the tools used to counter an attack, they are often inadequate or incorrectly used (e.g. water jets, Ship Security Alert System).

In terms of the threat response, the targets in danger can currently send alert messages to other units in the area but this diffusion is restricted to a very small geographic area. Moreover, even if a security vessel is alerted to a threat, it cannot be assumed that it will be able to intervene, particularly if it is not close to the location of the attack.

Therefore, the aim of the SARGOS system is to offer a new method that is able to both detect threats and plan a response. The response implements a graduated series of non-lethal counter-measures (sonic cannons, barring infrastructure access, etc.) that can be applied in order to eliminate the danger.

[21] In these systems, a radar antenna emits microwave pulses towards the target. These signals are reflected back, and then intercepted by the radar receiver, which collects an electrical signal called the echo.

[22] These electronic and electrical systems generally consist of an optical sensor, an image processing system and a data storage, or display device.

2.4 The contribution of the SARGOS system

The SARGOS system addresses the need to protect civilian infrastructure that is vulnerable to acts of piracy or terrorism at sea. It is a global system that takes into account the whole threat processing chain, from the detection of a potential danger to the implementation of the response. It can be integrated into the operations of the installation and takes into account regulatory and legal frameworks at both national and international level. The creation of the system, which involved the development of an overall protection method, automatic threat detection and identification, risk assessment and management of an appropriate response, required professional skills from many domains.

The functional diagram of the SARGOS system (Figure 1) describes the threat processing cycle. The overall system operates as follows: when the detection module instruments (Frequency Modulated Continuous Wave radar, infrared cameras, etc.) identify a vessel in an area near to the oil field, the system evaluates the threat and the potential danger and generates an alert report containing comprehensive data describing the scenario. This information includes details such as visibility, time of day, the speed, longitude and latitude of the detected vessel and its potential target, etc. The distance between the two entities and the theoretical response time of the security vessel is also calculated from this data. If the threat is identified as suspicious or hostile, the system generates an alert report every second. The alert report is used in the planning stage where external and internal means to respond to the attack are mobilised. This paper particularly addresses this aspect of response planning and the management of internal and external resources available on the installation (such as searchlights or sonar alarms).

Figure 3-1: from the information detected by the FMCW radar, the system identifies the threat and then calculates the ranking and generates an alert report containing all the information necessary to assess the situation in order to use internal and external resources to manage the threat. The ranking is calculated in corresponding to the time required (in seconds) to the threat to go the distance to CPA asset considered taking into account the assumption that at any time the threat may change course and coming in on the target constant radial. The terms are: [ranking <300 s], [300 <ranking <900 s] or [s 900 <ranking <1800 s].

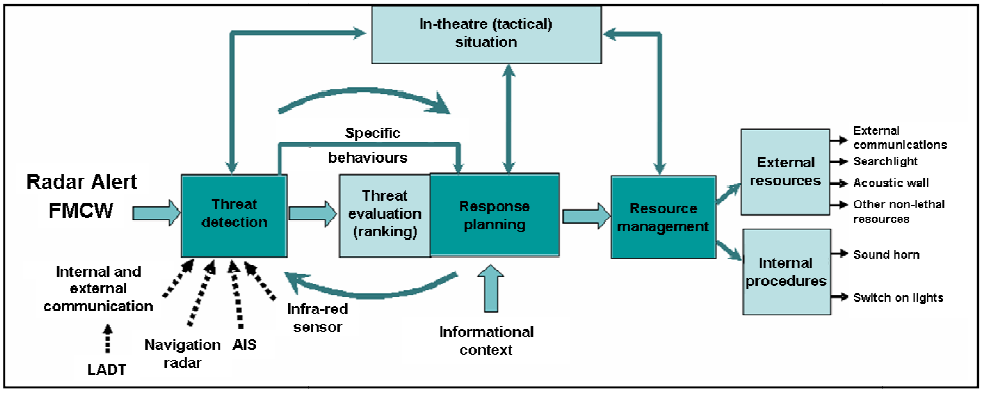


Figure 3-1 : Functional diagram of the SARGOS system

2.5 Elements of threat analysis and principles for resource management

There are significant obstacles inherent in addressing the problem of maritime piracy. An initial difficulty concerns how to manage the large number of parameters necessary to describe an attack. These parameters, which form the inputs and outputs of the system, characterise the asset in danger (type, criticality, vulnerability, on-board safety tools, etc.), the threat (the type of ship used by the attackers, its speed, their weapons, etc.) and the environment (the time of day, visibility, sea state, etc.). A second problem lies in the fact that these parameters may interact with each other. For example, whether it is relevant to request the intervention of the security vessel will depend not only on the time required for it to reach the asset under attack but also how well armed the attackers are and how fast they are moving. Therefore, the management of the multiple interrelations between system variables presents another major challenge. These first two constraints suggest that the system be based on graph theory, which would make it possible to translate and exploit, using a graph, the large number of variables, their interdependencies and interrelationships, etc.

However, an additional concern is uncertainty in the information describing the threat. The SARGOS system generates an alert report that contains on the one hand, data issuing from various detection instruments (type of ship detected, number of crew, potential weapons, etc.) and on the other hand, mathematical calculations based on dynamic variables (the distance between the target and its attackers, time available before the attackers are able to board the asset, etc.). Despite the improving performance of

radars, this data is known to be unreliable. This situation is only made worse as the distance between the target and the threat increases, or if the sea state deteriorates, etc. This uncertainty is a constraint that emphasises the need to use a system based on probability theory and probabilistic calculations.

With these constraints in mind, a solution based on Bayesian networks was explored [Leray and al., 2008]. A Bayesian network is a system for the representation of knowledge and the calculation of conditional probabilities [Naïm and al., 2007]. The tool is based on Thomas Bayes' theorem, which is one of the foundations of probability theory [Nielsen and al., 2009]. Widely used in medical and industrial diagnosis [Lee and Lee, 2006], Bayesian networks make it possible to capitalise on, and exploit knowledge and are particularly suitable when uncertainty must be taken into account [Hudson and al., 2002], [Martín and al., 2009].

The aim was to automate the preparation of response plans that are tailored to the nature of the detected intrusion and can provide an appropriate, graduated and progressive response to a threat. Information concerning attacks on shipping and petroleum installations was gathered from a specialist database, and experts in the maritime domain who offered their knowledge and expertise. The data from each of these two sources was modelled with Bayesian networks. The network was built using BayesiaLab[23] software; this powerful network modelling tool provides an intuitive graphical interface.

Recently, Bayesian networks are used in risk assessment because the model can perform forward or predictive analyses as well as backward or diagnostic analyses. Some methodologies have been proposed to structure Bayesian networks and perform risk assessment.

Several authors have already used Bayesian networks in order to solve problems in offshore. Among these authors, [Baoping and al., 2012] who modeled a Bayesian network for the quantitative evaluation of the preventive operation underwater eruption wells. The choice of using Bayesian networks has been done because they are models to perform predictive analytics and diagnostics systems. Another application described in

[23]BayesiaLab software is developed by the French company Bayesia (http://www.bayesia.com/).

the article of [Eleye-Datubo and al., 2008] is the use of a Bayesian network to provide an intuitive and vital representation that mimics the real world. The integration of the human element in a model based on probabilistic risk requires integrated appropriate technical and essential contributions of the linguistic nature. For this reason, the author proposed a Fuzzy Bayesian network as fuzzy logic is an excellent tool for such integration and Bayesian networks can make a probabilistic framework and cross the boundaries of possibility theory. The implementation of this method was demonstrated in a study of human performance at sea.

[Khakzad and al., 2013] looked at preventing the risk of blowouts during drilling operations. The authors demonstrate the application of both the “bow-tie” and Bayesian network methods. In the first method, fault trees and an event tree are developed for potential accident scenarios. In the second method, individual Bayesian networks are created for accident scenarios and an object-oriented Bayesian network is constructed by connecting the individual networks. The dynamic Bayesian network method is a better approach than the “bow-tie” model because it can take into account common cause failures and conditional dependencies along with performing probability updates and sequential learning based on accident precursors.

[Ren and al., 2007] also addressed the contribution of Bayesian networks when taking into account human factors. The authors designed and developed a methodology based on the “Swiss cheese” model developed by James Reason [Reason, 1990]. Reason’s model provides a generic framework for risk assessment linked to human factors. Five levels are used to characterize latent failures within the causal chain of events: root causes, trigger events, incidents, accidents and consequences. The detailed characterization of each level made it possible to build the Bayesian network. A range of events was specified, and the prior and conditional probabilities of the model were assigned based on the inherent characteristics of each event.

[Trucco and al., 2008] presented an approach to integrate human and organizational factors into risk analysis. This approach has been developed and applied to a case study in the maritime industry, but it can be also be utilized in others sectors. A Bayesian Belief Network has been developed to model the maritime transport system, by taking into account its different actors ship-owner, shipyard, port and regulator and their mutual influences.

[Vinnem and al., 2012] addressed the issue of hydrocarbon releases at sea during the exploitation or maintenance phases of a platform. A generic model, based on risk influencing human factors was developed and adapted to specific failure scenarios. The authors describe a full Bayesian network model and two implementations are outlined. The probability of human error, importance measurement of consequences and common causes and interactions are analysed. The authors demonstrate that the model is able to reflect human and organizational factors and safety culture.

These references highlight the wealth of work that has been carried out into both the assessment of technical risks and human and organizational factors in order to prevent the threats that face platforms at sea.

3. Coupling of quantitative and qualitative knowledge for the construction of a Bayesian network for response planning

The creation of the Bayesian network used for response planning relied on the coupling of quantitative information from the IMO's "Piracy and Armed Robbery" database and qualitative knowledge offered by experts in the maritime domain. Development was divided into two stages. The first step was to construct a Bayesian network from database records of attacks against shipping and oil installations across the globe, while the second step was to exploit the knowledge of experts in order to refine the results and to add counter-measures.

3.1 Construction of a Bayesian network from quantitative data

This first step involved the extraction of data from the IMO's "Piracy and Armed Robbery" database. This is the only database currently in existence that contains historic data (dating from 1994) of pirate attacks at sea. On 15th July, 2011 the database contained records of 5,502 attacks and provided detailed information on the name of the asset under

attack, the number of attackers, the weapons used, the measures taken by the crew to protect themselves, the impact on the crew and the pirates, etc.

In the table below are listed some examples of recent attacks and armed robberies.

Date	Ship name	Ship type	Incident details
2012-12-23	ASSO VENTUNO	Supply ship	Pirates armed with guns attacked and boarded the offshore supply ship underway and kidnapped four crew members. The ship sailed to a safe port after the incident. The other crew members did not sustain any injuries.
2012-12-29	SANKO MERCURY	Bulk carrier	Robbers boarded the anchored ship while waiting to commence loading operations. They broke into the forward bosun store, stole the ship's stores and property and escaped unnoticed. The incident occurred between 29.12.2012, 2300 LT and 30.12.2012, 0400 LT and was reported to the local agent and the port authorities.
2012-12-29	NORD DISCOVERY	Bulk carrier	Duty crew onboard the anchored bulk carrier found that the lock of the forward store had been broken. After checking, he saw the ship's stores lying on the deck and the robbers escaping in their two boats empty-handed.

Table 3-1 : Examples of recent attacks and armed robberies

To classify this information, we applied a method of textmining to the database using the software RapidMiner[24].

The BayesiaLab software made it possible to automatically generate a bayesian network and describe the interdependencies between the principal basic elements. Among the unsupervised learning methods available (data segmentation algorithms or characterisation of the target node for examples), an algorithm for finding associations was chosen as it offered the most appropriate modelling.

The Bayesian network constructed from data related to attacks held in the International Maritime Organization's database lacks many values related to the modalities of the different nodes because of a lack of detail in the description of pirate attacks. BayesiaLab makes it possible to impute missing values by adding a state to the variable. Moreover, the k-means algorithm applied to the data made it possible to estimate the independence relations between database variables and thus to obtain the best “cause and effect” structure. For each attack scenario, the network performs a statistical calculation by applying the parameters given as input to simulations of similar

[24] RapidMiner is unquestionably the world-leading open-source system for data mining. It is available as a stand-alone application for data analysis and as a data mining engine for the integration into own products

cases. The large amount of missing data in the database therefore does not impact any of the parameters for the simulation of attack scenarios.

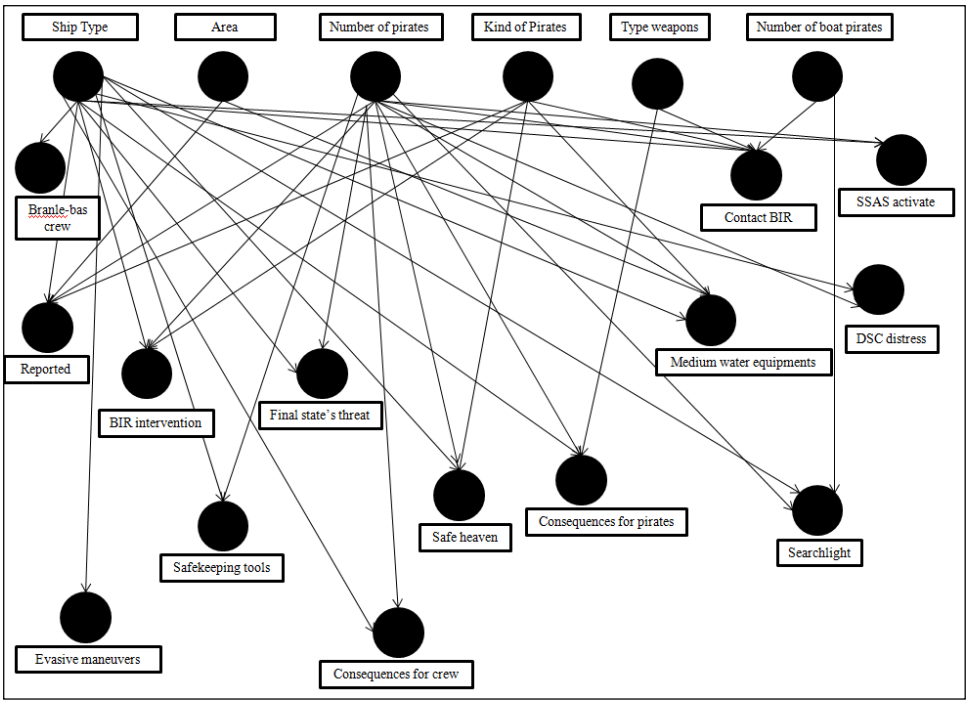


Figure 3-2 : The Bayesian network based on IMO data

Figure 3-2 shows the Bayesian network constructed from the information contained in the IMO database. Some information, such as the longitude, latitude, name of the asset attacked, etc. is not included. This is due to the fact that this data was not specified for all attacks. The network contained around twenty nodes that described the type of vessel under attack, the location of the attack, the type of weapons used by the pirates, their numbers, etc. The interrelationships between these variables were also identified through a machine learning process.

A classical statistical analysis of this data provided some initial findings, which included the observation that most ships coming under attack are bulk carriers or tankers; 48% of attacks take place in international waters (due to the absence of security patrols); and pirates prefer to attack in numbers (68% of attacks are organised by teams of more than five pirates). The network therefore provides a very clear view of the tactics of pirates, the weapons they use, and above all the number of individuals involved.

In the example below, specific modalities were set for nodes that characterise the threat in order to identify the counter-measures used by the crew of the asset under attack. Figure 3-3 illustrates the following assumptions:

- The asset under attack: a tanker
- The location of the accident: international waters
- The type of attackers: thieves
- Type of weapons: armed personnel

The Bayesian network indicates that in this case (as in most cases) the assailants fired shots at the potential target and that the crew, to protect themselves from the threat, tried to apply evasive manoeuvres and aimed water hoses at the attackers.

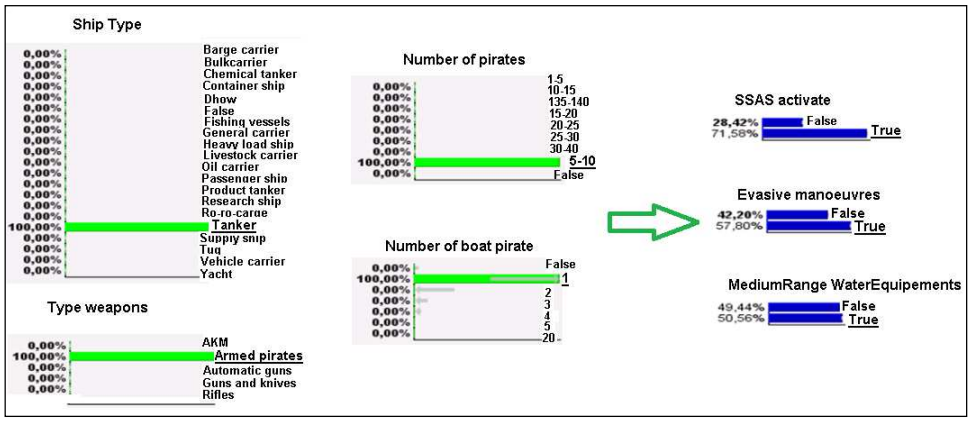


Figure 3-3 : Hypothetical attack against a tanker

The network created from the IMO database therefore helped to define the principal steps taken by the crew of attacked entities in order to protect themselves, namely: initiate evasive manoeuvres, activate the Ship Security Alarm System (SSAS), contact the security vessel, secure the crew, turn on searchlights, etc. It also made it possible to assess the effectiveness of these tools and to define the probability of occurrence of certain types of attacks.

It is necessary to carry out an initial analysis of the IMO database to establish the challenges posed by these threats to the crew, the platform, the economy and national security. It makes it possible, in a second step, to identify the frequency of attacks, risk zones, types of ships used to carry out attacks, etc. and to list the most commonly used and effective counter-measures.

3.2 Coupling the Bayesian network based on IMO data with the qualitative knowledge of marine experts

The Bayesian network created from the modalities and conditional probabilities found in the IMO database provided an initial formal framework. Domain experts were then able to enrich this initial network by integrating their knowledge and expertise in order to create the final SARGOS network [Hudson, 2002].

The second step of the approach was for experts in the maritime and petroleum industries to analyse the information provided by the Bayesian network that had been constructed from the IMO data. As the information contained in the IMO database related primarily to attacks on shipping, experts were able to contribute their knowledge of attacks on oil fields in order to extend the results: nodes and arcs were added to the model in order to make it as versatile as possible. Consequently, the Bayesian network was able to model both main target categories (shipping and fixed installations). While the inputs to the network (type of vessel used by the attackers, its movements, etc.) are identical regardless of the nature of the target, the counter-measures recommended by the Bayesian network are tailored to the type of target under attack (for example, evasive manoeuvres are not proposed when a fixed installation is the subject of the attack).

The design of this enhanced Bayesian network, adapted to the constraints and conditions associated with fixed installations came about as a result of many brainstorming sessions during which various maritime security experts shared their experiences and discussed the modalities and probabilities of the network.

The combination of information from the IMO database and the knowledge and experience of experts in marine and offshore safety made it possible to create the SARGOS response planning network, which consisted of four modules and five sub-modules (Figure 3-4).

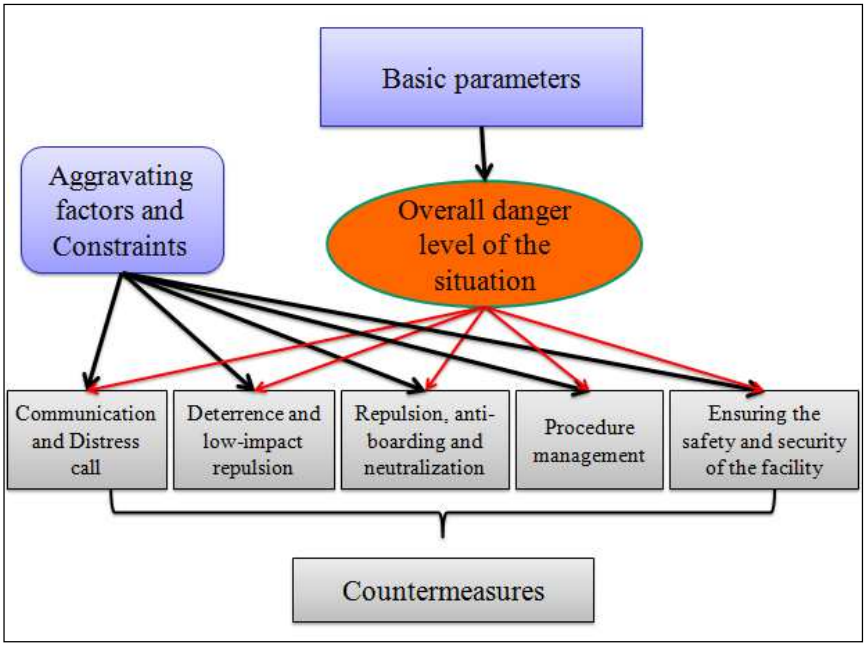


Figure 3-4 : Structure of the SARGOS Bayesian Network

In the SARGOS Bayesian network, each module or sub-module consists of one or more nodes that receive input from and/or output to other nodes. Each node is a matrix of conditional probabilities that are calculated from an assessment of the interactions between nodes and the reality represented by the node itself. For example, the probability distribution of the node to activate searchlights (‘ActivateSearchlight’) is the direct result of interactions with other nodes that describe visibility, time of day and technical constraints such as availability and remote control. The probabilities of the basic nodes are initially standardised as no specific attack characteristics are set.

The definition of the scope of each module is directly related to the composition of its constituent nodes. The module classification included: basic parameters, the overall danger level of the situation, aggravating factors and constraints, counter-measures and nodes related to communication and the request for assistance. These modules are described in detail below.

3.3 Basic parameters

The basic parameters module comprises static or dynamic physical data that characterise the threat and the target. These data are the direct result of, or are derived

from the intermediate calculations of the alert report. Basic parameters represent the minimum, but sufficiently detailed level of modelling required for a full understanding of the threat and the target when assessing potential responses to an attack. They include, for example, threat identification (the node ‘IdentityClass’ which has two values: suspicious or hostile), the distance between the threat and the target (the node ‘DTGThreat/Asset’), and the criticality of the target (the node ‘AssetAssessment’ that takes four values: critical, major, significant or otherwise).

In the Bayesian network, we take into account the longitude and latitude of the pirate ship for the calculation of the kinematics of the vessel to determine the distance between the graft vessel and the platform. These two variables are passed in the alert report but not included in the network nodes.

3.4 The overall level of danger of the situation

The overall danger level of the situation is arrived from the basic parameters. The node ‘ShowGradationLevel’ is used to formalise this module in the Bayesian network. The grading system runs from level 1 (least serious) to 4 (most serious). This level and the planning of counter-measures are constantly adapted to the situation.

3.5 Aggravating factors and constraints

The aggravating factors and constraints module consists of elements that are both internal and external to the system. Aggravating factors make it possible to take into account a potential deterioration in the situation and thus to anticipate potential planning options. The nodes in this module represent the environment, for example visibility (the node ‘Visibility’) and time of day (‘PeriodOfDay’). Constraints are represented by parameters which reflect the effectiveness of the response both technically and operationally. Technical constraints are directly related to the use of counter-measures, and include nodes that represent their availability (‘ImmediateReadiness’) or the potential for remote control (‘RemoteControlled’).

3.6 Counter-measures

Counter-measures include all defences that are mobilised by a target under attack in order to protect itself against an identified threat. They are the concrete realisation of the response plan and constitute the set of means and actions intended to normalise, as quickly as possible, the situation. Counter-measures are divided into five sub-modules, which reflect the concept of a graduated response through increasingly forceful measures that correspond to the nature of the detected threat. Measures range from communication and a request for assistance, through deterrence and small-scale repulsion, repulsion, anti-boarding measures and neutralisation, to procedure management and securing the facility. They are described in detail below.

Communication and the request for assistance are two key responses to a threat. Internal communication can be used to alert all relevant personnel on the target (e.g., the node 'InformOIM' which represents informing the crew master), while external communication makes it possible at various levels to alert the different actors involved in maritime security – for example to request the intervention of the security vessel (represented by the node 'RequestSecurityVessel') or to activate the Ship Security Alarm System (represented by the node 'RaiseSSAS') etc. Both of these types of communication enable fixed installations and shipping to prepare their response plan and to establish if external intervention is available.

From the position of the ship security (BIR), the system calculates the time required for the intervention on the location of the threat. If the estimated response time is greater than 300 seconds, the ship security may be required, in which case a request must be sent.

Deterrence and small-scale repulsion measures are intended to inform the attacker that the target is aware of the attacker's intentions, can follow the attacker and that it is not in the attackers' interest to continue. These measures include the ability of the target to repel an attack with low-impact devices such as searchlights, fire hoses or sonic cannons (Long Range Acoustic Devices), represented by the node 'ActivateLRAD'.

Repulsion, anti-boarding and neutralisation are high-impact counter-measures whose main function is at least to mitigate an attack, if not neutralise the attackers. The node

‘EngageRepellentEquipment’ represents a growing number of tools available on the anti-piracy market that are designed for the repulsion of an assault at long-range (while remaining within the bounds of legitimate, non-lethal defence). Like repulsion equipment, the main function of anti-boarding tools is to prevent attackers from gaining access to the facility or vessel. The function of the ‘SetCrowdControlMunition’ node is to delay the progress of the attackers in order to exhaust or even neutralise them and thereby provide the crew with maximum time to mobilise other safety measures.

Procedure management is composed of two counter-measures. On the one hand, the node ‘CrewManagement’ represents the sounding of crew Action Stations and the reporting of crew to their pre-assigned post or station. On the other hand, the ‘AssetAssaultManagement’ node represents activities related to securing the target of the attack. The modalities of this node are: activate the Citadel, engage evasive manoeuvres (for mobile units and shipping), and declare the security post (a set of individual procedures to be applied by each crew member as necessary). Like procedure management, the SARGOS system offers a way to secure the installation through the planning of actions designed to safely stop production and prevent access to sensitive areas.

4. Demonstration of the contribution of the Bayesian network and discussion

Once the probability distribution of the various modalities has been established, an interesting exercise is to test the Bayesian network by using it to simulate different attack scenarios through the selection of certain criteria. An examination of these scenarios made it possible to finalise the network before integrating it into the SARGOS system.

The integrated data that provides the input to the network is interpreted from images captured by cameras and various sensors. The uncertainty of this information increases with the distance between the target to be protected and the pirate ship. In its current form, the Bayesian network cannot handle the temporal evolution of the attack and there is no connection between response reports generated for the same attack. This issue is addressed in other research based on dynamic Bayesian networks (Dabrowski and al, 2013).

4.1 Attack scenarios

The example below (Figure 3-5) shows the results of setting parameters to simulate an attack on a Floating Production, Storage and Offloading (FPSO) unit by an unknown vessel. In this example the danger level of the situation is 2 with a 64.68% probability of occurrence and the counter-measures to be applied are: inform the crew master; request the intervention of the security vessel; broadcast a strong, clear message by loudspeaker; activate the searchlight; activate the security post; and engage repulsion equipment. Figure 3-5 shows that the planning of the response corresponds to the danger level of the situation and is able to adapt to changes in parameters representing the threat and the target. Setting parameters to represent the threat, the target, the environment, etc. creates different attack scenarios that make it possible to refine the probability of an attack and test the response of the Bayesian network.

In this case it is necessary to inform the master of the crew of the FPSO, request the intervention of ship safety and security since the probability of their action is equal to 80% (close to the ship attacked infrastructure). Several counter-measures can be activated as the speakers, bright lights and water jets. Following the evolution of the situation a few moments later and the increased level of danger that follows, it should then alert the crew to use the security station.

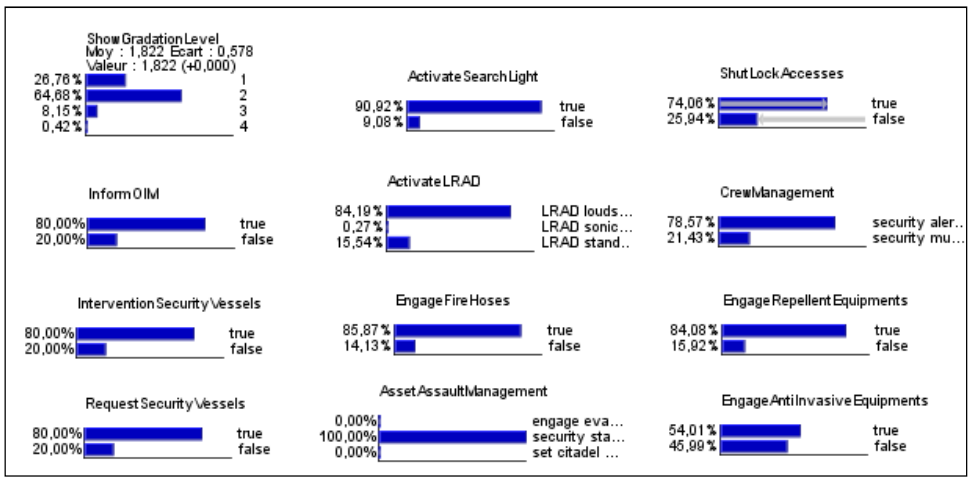


Figure 3-5 : Result of response planning using the scenario of an attack from an unknown vessel

4.2 Integration of the Bayesian network into the SARGOS system

In order to integrate the Bayesian network into the SARGOS system, a prototype was developed that included an alert report as input and a planning report (which listed all the counter-measures to be applied either by the crew or automatically by the system) as output. The BayesiaEngine software provides a module that makes it possible to select and set attack parameters. This module consists of an application programming interface (API) and a Java library. Intermediate calculations are carried out on the basis of these parameters and the results are fed into the enhanced Bayesian network created from expert knowledge.

The resulting list of counter-measures varies according to the attack scenario. Consequently, a threshold must be set in order to only activate those measures that provide the most relevant response at a particular time, and in a particular situation. This threshold was set at 70%. In other words, only those counter-measures where one of the modalities had a probability greater than 70% were selected for further processing. This threshold was arrived at by domain experts as it reflects actual events in more than two-thirds of real-life cases. Following an extensive period of testing, the selected counter-measures were found to correspond to realistic and reliable responses.

Once the counter-measures had been selected, they were added to the planning report in a specific order. The main factors determining this order of priority were: the action mode of the counter-measure, its ease of implementation, the degree of automation or the need for a large number of crew members to activate it, the time required for it to become effective and its potential additional functions.

The SARGOS system can handle multiple threats contained in a single alert report. Consequently, priorities must be established. In the system, the first threat to be treated is always the one where time available to react is the shortest for the target that is most exposed.

The system detected several potential threats heading towards the oil field and has classed them into ‘Enemy’, ‘Unknown’ or ‘Friend’. An alert is only generated following a classification of Enemy or Unknown. Once a threat has been detected and analysed, the response planning report is prepared. It is divided into two parts: the first concerns

communication and a general request for assistance directed at the entire oil field; the second concerns the specific asset at risk. The response planning report also displays the counter-measures to be activated in chronological order (Figure 3-6).

The representation of the probability that a particular measure will be implemented can be seen in the counter-measure 'Security Vessels', where the proportion of the blue segment suggests a 60-70% probability that this method will be called upon.

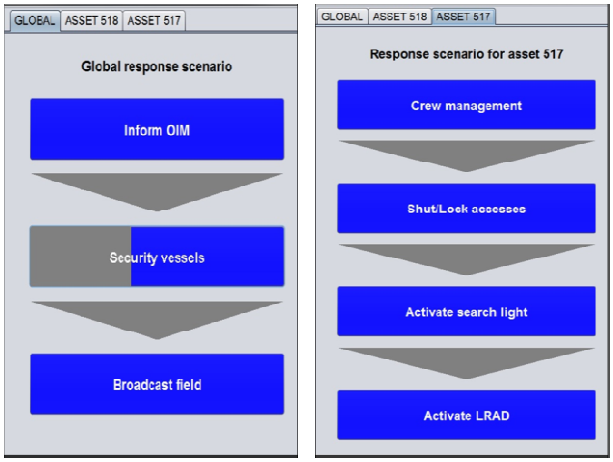


Figure 3-6 : The user interface of the SARGOS system showing global counter-measures on the left (in order: inform the crew master, request the intervention of the security vessel and inform other installations in the field) and specific counter-measures on the right (assemble crew, block access to infrastructure, activate searchlights and activate the sonar cannon).

5. Conclusion

Acts of maritime piracy against oil field infrastructure present a complex problem. The effectiveness of current measures designed to protect infrastructure is significantly affected by the vast terrain and environmental constraints. Moreover, it is difficult to assess a potential threat given the constantly changing nature of a dangerous situation and the huge number of parameters that must be managed.

The implementation of a Bayesian network therefore offers a significant advantage for the SARGOS system as this type of network is able to handle all possible combinations of parameters. These include not only the characteristics of the threat and the target under attack, but also the environment and variables related to crew and facility management. Most importantly, the system is able to adapt in real-time to changes in the

danger level of the situation. The SARGOS system offers a response planning solution that manifests in the preparation of a planning report created from an intelligent assessment of successive alert reports, and which can react to an evolving situation.

The activation threshold of counter-measures has been determined by experts. Most counter-measures are against-enabled manually by the crew. Some of them are not systematically exploited if their activation requires setting a crew danger. The Bayesian network was developed specifically for the protection of static targets (platforms) and is therefore not suitable for ensuring the safety of ships.

The network can be continuously improved through the integration of feedback from attacks that have already been managed. It is therefore possible to continue to enhance and tailor the planning module iteratively.

Finally, an interesting approach that may improve the modelling of knowledge embedded in the Bayesian network could be to establish an appropriate ontology. The use of a suitable ontology would make it possible to formalise knowledge upstream of the Bayesian network in order to consolidate the threat detection and identification steps.

The use of dynamic Bayesian networks is a way to explore. These networks have been an interesting development as a generalization of models hidden Markov models or Kalman filters for applications such as speech recognition, state estimation of a dynamic system, etc. A dynamic Bayesian network is a factored representation of a Bayesian network whose nodes are indexed by time on a discrete scale. The Bayesian network is represented by nodes and indexed by generic no time and two types of links: links classical Bayesian networks and so-called temporal relationships that define the conditional probability tables of the nodes according to their parents located to lower time indices. The application of a dynamic Bayesian network would integrate the notion of time on decisions to be taken in case of attack and its influence on the evolution of the threat.

References

Baoping C., Yonghong L., Zengkai L., Xiaojie T., Yanzhen Z. and Renjie J. (2012). Application of BayesianNetworks in Quantitative Risk Assessment of Subsea Blowout Preventer Operations. Society for Risk Analysis, pp. 1-20.

BMI. 2011. Study: Piracy Costs World Up to $12 Billion Annually, Bureau International Maritime, 14 juillet 2011. http://www.voanews.com/english/news/africa/Study-Piracy-Costs-World-up-to-12-Billion-Annually-113609239.html.

Dabrowski J.J. and Pieter de Villiers J.(2013). Maritime piracy situation modelling with dynamic Bayesian networks. Information fusion.

Eleye-Datubo A.G., Wall A. and Wang J. (2008). Marine and offshore Safety Assessment by Incorporative Risk Modelling in a Fuzzy-Bayesian Network of an Induced Mass Assignment Paradigm. Society for Risk Analysis, pp. 95-112.

Hudson L.D., Ware B.S., Mahoney S.M. and Laskey K.B. (2002). An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners. 8p, August 2002.

Khakzad N., Khan F. and Amyotte P. (2013). Quantitative risk analysis of offshore drilling operations: A Bayesian approach. Safety Science, 57, pp. 108-117.

Lee C.J. and Lee K.J. (2006). Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal. Reliability Engineering and System Safety, volume 91, n°5, pp. 515-532, Mai 2006.

Leray P., Meganck S., Maes S., and Manderick B. (2008). Causal graphical models with latent variables : learning and inference. In Holmes D. E. and Jain L., editors, Innovations in Bayesian Networks: Theory and Applications, Studies in Computational Intelligence, vol.156, pp. 219-249. Germany, Springer.

Martín J.E., Rivas T., Matías J.M., Taboada J. and Argüelles A. (2009). A Bayesian network analysis of workplace accidents caused by falls from a height. Safety Science, volume 47, n°2, pp. 206-214, février 2009.

Naïm P., Wuillemin P.H., Leray P., Pourret O., and Becker A. (2007). Réseaux bayésiens. Eyrolles, Paris, 3 edition.

Nielsen T.D. and Finn V.J. (2009). Bayesian networks and decision graphs. Springer, pp. 463.

Reason J. (1990). Human Error. Cambridge University Press, pp. 320.

Ren J., Jenkinson I., Wang J., Xu D.L. and Yang J.B. (2008). A methodology to model causal relationships on offshore safety assessment focusing on human and organizational factors. Journal of Safety Research 39, pp. 87-100.

Schroeder D.M., and Love M.S. (2004). Ecological and political issues surrounding decommissioning of offshore oil facilities in the Southern California Bight. Ocean and Coastel Management, volume 47, 2004, pp. 21-48.

Trucco P., Cagno E., Ruggeri F. and Grande O. (2008). A Bayesian Belief Network modelling of organisational factors in risk analysis : A case study in maritime transportation, Reliability Engineering and System Safety, pp. 823-834.

Vinnem J.E., Bye R., Gran B.A., Kongsvik T., Nyheim O.M., Okstad E.H., Seljelid J. and Vatn J. (2012). Risk modeling of maintenance work on major process equipment on offshore petroleum installations. Journal of Loss Prevention in the Process Industries 25, pp. 274-292.

Chapitre 4 : Article 3 : Contribution des Réseaux Bayésiens Dynamiques pour la Protection des Infrastructures Critiques : Plateformes Pétrolières Offshores

4.1. Présentation de l’article

L’article a été soumis à la revue Internationale Journal of Critical Infrastructure Protection. Il décrit le système de management de la piraterie maritime basé sur les réseaux bayésiens dynamiques et présente la vulnérabilité des infrastructures pétrolières.

4.2. Version anglaise de l’article

Contribution of dynamic Bayesian networks to the protection of critical infrastructure: offshore oil platforms

Abstract

Offshore oil platforms face an increasing threat of piracy. This paper describes the design and development of a prototype decision support tool to help operators respond. The decision-making process is based on probabilistic analysis models, in particular “dynamic” Bayesian networks. The resulting prototype is a graphical decision support model of an uncertain universe. The Bayesian network incorporates information from knowledge bases, databases, specialist expertise, and probability distributions that can help in predicting the future given the past. We describe the methodological approach to the design of this prototype for the diagnosis of pirate attacks and the planning of appropriate countermeasures.

Keywords

Dynamic Bayesian networks, Maritime piracy, Offshore oil platforms, Expert knowledge.

1. Introduction

Offshore oil and gas production plays an important role in the energy supply in modern society [Aleklett and al., 2010]. While most production is carried out a depths of less than 500 meters, recent years have seen the expansion of “deep” offshore production (at depths of more than 1,000 meters) as a result of significant technological advances, particularly in the field of seismic and subsea installations. Oil production in waters more than 1,000 meters deep rose by 12% between 2006 and 2008. Gas production at more than 1,000 meters represents about 2% of global production and reserves are estimated at 2.7 Tm3 (trillion cubic meters).

Oil companies are interested in offshore production because of the high levels of resources and the protection it offers from land-based conflicts (e.g. in the Gulf of

Guinea, where it is safer to produce offshore than onshore). Production is expected to continue to expand and around 30 new fields operating in depths of more than 1,000 meters are expected to be brought into production every year until 2020, more than double the number for the decade 2000–2010.

Oil and gas provide most of the energy needed to run modern societies. Global dependence on oil is huge; it provides fuel for transport, heating and cooling of buildings and it is used in the manufacture of industrial and household chemicals. Sixty percent of oil production is used for transport, primarily cars and heavy vehicles. Oil is a non-renewable source of energy and current global consumption is around 70 million barrels per day, which is expected to double by 2025.

Overall, offshore activity accounts for 30% of global oil production (25 million barrels per day) and 27% of gas production. It also represents 20% of global oil reserves and 30% of gas reserves. Approximately 450 fields have been discovered at more than 1,000 meters: 38% of these are in the Gulf of Mexico (the United States), 26% in the Gulf of Guinea (Africa) and 18% in Brazil. Although these deep reserves currently only account for 3% of global oil production, this figure is only expected to grow in future years, and reserves are estimated at 72 Giga barrels.

The construction, transportation and operation of a platform generate various risks. Incidents and accidents can have a major impact on the environment, mariners and property. Risks include seismic movements, toxic waste, fire or explosion (the most hazardous risk) and pollution that can affect marine life. Memories of pollution due to the extraction and transport of hydrocarbons are still fresh. Examples include the accident in 2010 at the Deepwater Horizon oil rig in the Gulf of Mexico that caused the loss of 4.9 million barrels of oil, eleven members of staff, injuries to 17 others and widespread pollution to coastal areas of Louisiana, the Mississippi, Alabama and Florida. This catastrophe was preceded by the explosion of the Piper Alpha oil platform in 1988 and the sinking of the Erika off the French coast in 1999.

Not only is there a risk of accidents or disaster [Gordon and al., 1996] there is also, since the early 2000s, a significant risk of piracy [Hansen, 2009]. This risk is very real in strategic areas such as the Gulf of Aden or the Gulf of Guinea (the worldwide Mecca for offshore oil production). Given the economic importance of hydrocarbons, offshore fields

have become a target for pirates and even terrorists [Anifowose and al., 2012]. While oil platforms and their supply vessels form a productive industrial network, they are powerless against deliberate malicious acts and their isolation makes them very vulnerable prime targets.

These proven threats are characterized by high levels of uncertainty. Bayesian networks have been shown to provide effective help in decision making in an uncertain world that is subject to time constraints. Of the various forms of Bayesian networks, we selected dynamic networks as the basis for our work as they offer many benefits. In this article we describe the design and development of a prototype decision support tool. The results produced by the model are tested and discussed in realistic pirate attack scenarios.

2. The exploration, production and transportation of offshore oil

Oil and gas are vital sources of energy for the world and are likely to remain so for many decades to come. Offshore oil production currently represents about one third of global oil production. Oil and gas production are a strategic challenge for both countries and multinational corporations that are facing increasing global demand for energy.

"*All industrial activities present safety problems, but the offshore petroleum industry does so more than most others*". This quote from [Kaasen, 1984], a Norwegian professor who is a leading expert on the offshore industry, highlights that offshore oil and gas fields have a higher level of risk than other, land-based industries. The explosion of the Deepwater Horizon oil platform on 20 April 2010 [White and al., 2011], which caused the death of eleven people, and was one of the biggest ecological disasters in the history of mankind, is a telling example. The disaster highlighted how critical this type of infrastructure is, and the catastrophic consequences that can unfold if it is put in danger.

In addition to the human and environmental losses, a platform exposed to the risk of piracy or fire endangers the global economy. An example is the pirate attack against the Bonga oil field on 19 June 2008, which resulted in several injuries and the closure of a field that accounted for 10% of Nigerian production (about 225,000 barrels/ day). The impact of this attack was seen in the international price of oil. "*Energy security is one of the most serious economic and security challenges, both today and in the future. The*

growth of world economies and societies goes hand-in-hand with the growth of energy and the associated infrastructure that produces and supply this energy. Critical energy infrastructure provides the fuel that enables the global economy to progress and society to function[25]".

Various disasters have demonstrated the vulnerability of such infrastructure and the urgent need for rigorous compliance with procedures and system design. The construction, transportation and operation of an oil platform generate various risks [Flin and al., 1996]. Technological accidents or incidents can exacerbate impacts on the environment, mariners and property. The risk of seismic movement, toxic releases, fire or explosion completes the threat panorama. Of these, the risk of explosion is most feared, although the risk of pollution can seriously damage marine life. An example is the case of the Pasha Bulker, a cargo ship that was carrying 40,000 tonnes of coal, shipwrecked on 8 June 2007 off the Australian coast with 700 tons of oil still on board. The 21 crew members were airlifted from the ship. However, the question of how to handle the environmental pollution remained. Given the economic importance of the price of oil, offshore fields have become an increasingly attractive target for pirates and terrorists. While oil platforms and their supply vessels form a productive industrial network, they are powerless against deliberate malicious acts, which makes them highly-sensitive critical infrastructure [Yergin, 2006].

The offshore oil industry already provides about a third of global supply, and is growing rapidly. Oil companies now focus most of their efforts on offshore exploration and production: in the medium term more than half of oil and gas extraction will be based offshore and particularly in deep waters (soon reaching up to 2000–3000 meters).

In 2010, about 3,300 offshore wells and around 420 floating and fixed offshore platforms had been constructed. The drilling market contributed about 40 billion dollars to the global economy, and engineering, equipment and other offshore structures about 50 billion dollars. However, although these facilities are designed to withstand extreme natural environments, they are not well-protected against deliberate malicious acts. While offshore platforms represent a success in terms of industrial production, from the point of view of safety, they are isolated targets that can be easily attacked from the sea.

[25] Extract from an address at the opening of the Organization for Security and Cooperation in Europe (OSCE), at a meeting of the NATO Economic Committee on 22 September 2008 in Brussels.

The safety of offshore oil facilities is therefore a major issue worldwide and raises questions about the consequences of both piracy and terrorism, which have become active issues both for ships travelling in open water and for the security of the energy supply. Oil and gas platforms lie at an interface between the maritime world and the oil industry. This creates conditions where their judicial status is very uncertain [Wright, 1994]. Although they are located at sea, fixed oil platforms can have a very special status because of nature of their activities. When non-operational, they are subject to the usual risks encountered at sea and consequently conventional maritime law. When operational, the framework changes, and international law as embodied in the national law of the coastal state applies. In addition to this already complex context, there is the question of the employment legislation applicable to personnel, which can differ depending on their status.

It is therefore essential to increase the level of protection for this infrastructure and develop systems that can generate an alarm and trigger a defensive response should the installation be attacked by pirates.

3. Pirate attacks: a very serious threat

World oil production is spread over more than 10,000 offshore fields. Each of these consists of facilities to extract, treat and temporarily store oil and vessels that transport hydrocarbons between production and consumption facilities. Modern piracy is currently the major threat to these energy production sites and maritime oil transport systems.

Although attacks against offshore infrastructure are less frequent and less publicized than attacks against shipping, they are nonetheless extremely worrying in that they highlight the vulnerability of this type of infrastructure.

Attacks on ships carrying hydrocarbons represent a significant percentage of all attacks against shipping [Kashubsky, 2008]. In 2006 they accounted for close to 12% of attacks, and reached more than 24% in 2007. Most attacks aim to steal anything of value. They occur in ports, or using very fast speedboats. The number of hijackings and hostage-taking situations has also risen sharply. In August 2003, the Malaysian tanker Penrider was seized off the coast of Indonesia and the hijackers demanded a ransom of $100,000.

Vessels transporting goods are clearly a target for pirates. In 1998, the Petro Ranger was attacked outside the territorial waters of Singapore. It was carrying nearly 12,000 tonnes of petroleum products. The pirates renamed it the Wilby and raised a Honduran flag. The Petro Ranger became, for a time, a ghost ship [Nincic, 2009].

The vast majority of attacks against shipping carrying hydrocarbons concern oil tankers and vessels transporting liquid gas. Out of the total number of tankers in the fleet (about 120,000), 4,000 (3%) are energy tankers. In 2007, pirates began to take an interest in mobile oil rigs and liquid gas carriers: there were two attacks, one in Indonesia and another off the coast of Singapore. Three fixed drilling platforms have also been attacked: two in Nigeria (including a kidnapping and ransom) and one in India. These events show that pirates are now able to tackle all sorts of target.

Since 2008, pirate attacks against offshore oil installations have increased considerably. [Kashubsky, 2008] carried out a detailed study of Nigeria. Some of the most significant events are shown in Table 4-1.

Date	**Description of the attack**	**Aftermath**
June 12, 2005	An armed group attacked the FPSO Jamestown (floating production, storage and offloading unit).	Forty-five people were taken hostage and released when a ransom was paid three days later.
January 11, 2006	A Shell platform was attacked.	Four people were taken hostage from the maintenance vessel anchored to the platform.
January 15, 2006	A very violent attack against a Shell facility led to a fire.	Extensive damage and 17 people killed.
February 18, 2006	A speedboat attack against an installation.	Nine personnel are injured.
October 2, 2006	Shell barges are attacked.	Three soldiers were killed protecting the vessel.
April 1, 2007	The facility suffered a second attack.	The maintenance vessel was hijacked by pirates, which was able to dock.
April 19, 2007	A patrol vessel was attacked.	It was stripped of its own weapons.
May 3, 2007	The FPSO Mystras was attacked; the attackers used the anchor chain to board.	Eight employees were kidnapped.
October 21, 2007	An armed group simultaneously attacked two maintenance ships.	
June 19, 2008	The FPSO Bonga was attacked and damaged.	Production was halted, with an estimated loss of more than 200,000 barrels per day.
September 14, 2008	Two Shell and Chevron platforms are attacked simultaneously.	
September 16, 2008	Eight speedboats loaded with dynamite and hand grenades attacked a Shell pumping station (Orubiri).	The pirates caused extensive damage.
September 22, 2010	The tug Bourbon Alexandre lying offshore in the Addax oil field of Nigeria was attacked by four speedboats.	Three French sailors were taken hostage. This was the fourth attack against the Bourbon since 2000.
November 17, 2010	Pirates using a speedboat attacked a ship belonging to the French company Perenco that was carrying Cameroonian security forces near an oil rig in the Gulf of Guinea.	This attack killed six soldiers.

Table 4-1 : Illustration of pirate attacks against oil installations

These events highlight the extent of the damage (human, material and economic) caused by pirate attacks. They also highlight the actions and strategies they deploy: surprise, extreme mobility, rapid action, a small number of attackers and a significant level of weaponry.

4. The use and benefits of dynamic Bayesian networks

Piracy reveals the shortcomings of currently-available systems implemented on offshore oil infrastructure to protect against hostile intrusions.

Safety on offshore installations is currently ensured by traditional methods: the watch, radio identification, automatic identification systems (AIS), radar monitoring of traffic and patrol boats generally operated by contractors. The priority for radar monitoring is to detect friendly large or medium-sized mobile vessels. They do not perform well in the detection of small marine targets with a small radar or optronic signature that are, of course, unfriendly (no radar or AIS reflector), operating in heavy seas (sea clutter). Moreover, they suffer from a blind spot at distances close to the carrier. Vessel Traffic Services (VTS) provide significant help to commercial navigation by offering a real-time picture of vessel movements in a given surveillance zone. Although they are widely used, they are typically tailored to the detection of “friendly” vessels and they are designed for the management of maritime traffic, which is far from the idea of protection against hostile intruders using small boats [Giraud and al., 2011].

As for the response to a threat, victims of an attack against an oil platform are able to alert patrol vessels deployed in the area but the diffusion of this alert is geographically restricted. Moreover, even if the patrol vessel is alerted, its ability to intervene is limited depending on its distance from the scene of the attack.

These limitations of current systems provided the motivation for the design and development of a decision support tool based on Bayesian networks.

4.1 Bayesian networks

Our research primarily aims to improve the detection of vessels and the development of alert mechanisms to enhance safety in response to a proven threat. In these conditions, there are significant constraints. On the one hand, there are a large number of attack parameters to be managed. They include input and outputs of system parameters related to the target (the platform) in danger (type, criticality, vulnerability, on-board safety equipment, etc.), the threat (type of vessel used by the attackers, its speed, their weapons, etc.) and the environment (time of day, visibility, sea state, etc.). Moreover, these parameters may interact. For example, whether it is relevant to request the intervention of the patrol vessel depends, in particular, on the time required to reach the installation, the attackers' weapons and their speed. The second constraint is related to the management of the many dependent relationships between different system variables.

A further constraint is the uncertainty of threat-related information. The generation of an alert report, which brings together information from various sensors including frequency modulated continuous wave (FMCW) radar (the type of vessel, number of occupants, potential weapons, etc.), and on the other hand, the mathematical calculations derived from dynamic variables (the distance between the target and the attackers, the time before they can board the platform, etc.) necessarily leads to the issue of the management of errors and false alarms. Although the performance of this type of radar has seen huge improvements, the uncertainty of the information increases with the distance of the threat, sea state, etc.

The constraints described above therefore suggest the design and development of a decision support system that is based on graph theory. The graph makes it possible to translate and exploit a large number of variables, their dependencies, incidences, etc. The uncertainty that is inherent in the data emphasizes the need for a solution based on probability theory and probabilistic calculations. The proposed model forms the basis for a tool that automatically creates a response plan adapted to the nature of the detected intrusion. The tool is based on Bayesian networks.

The question of knowledge representation and reasoning from representations has led to the development of many models. Probabilistic graph models (specifically Bayesian networks) were first developed in the 1980s by Judea Pearl to facilitate prediction

systems and abduction in Artificial Intelligence. This formalism for probabilistic reasoning was introduced by [Kim and Pearl, 1983], [Lauritzen and Speigelhalter, 1988] and [Jordan, 1998].

Bayesian networks form a set of probabilistic models for large collections of random variables where a sparse representation is necessary, both for numerical reasons (to avoid the manipulation of overly-large tables) and statistical reasons (to limit the number of parameters to be estimated). They are commonly used in Artificial Intelligence and machine learning [Jordan, 1999]. They are directed or acyclic graphs where the nodes represent random variables and arcs represent conditional independence between the various nodes [Pearl, 2000].

We selected a dynamic Bayesian network to form the basis for our model. This is a type of Bayesian network used to model dynamic stochastic processes ([Darwiche, 2000] and [Murphy, 2002]). Each variable X in a dynamic Bayesian network is associated with a time slice T and is denoted X_t. A key feature of these networks is the number of time slices T necessary to model a particular problem. This period of time is unlimited. While the number of variables associated with each time slice is unchangeable, the dimension n of the slice may change.

Our decision to use dynamic Bayesian networks relates to the processing of attack scenarios at various time intervals and thus the need to be able to create a structured, evolving plan.

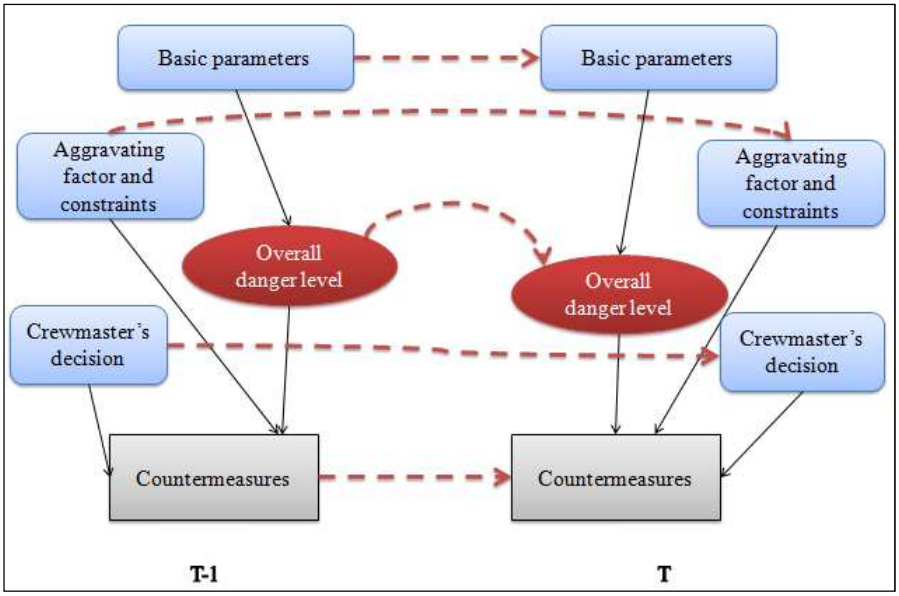


Figure 4-1 : Structure of the dynamic Bayesian network

The architecture of the dynamic Bayesian network shown in Figure 4-1 is defined by a part (B_1, $B_{->}$), where B1 defines the a priori $P(Z_T)$ and $B_{->}$ is the time slice of the Bayesian network which is used to define $P(Z_T \backslash Z_{T-1})$ where Z is a random variable described by $Z_t = (U_t, X_t, Y_t)$ to represent the nodes of the model. The dotted arcs represent temporal arcs between time slices. These arcs run from left to right and reflect the progress of time. There is a dynamic discrete stochastic process where the time index T is increased by one each time new data is collected by the system.

4.2 Bayesian network overall architecture

The structure of the Bayesian network includes basic parameters, the overall danger level of the situation, aggravating factors and constraints, nodes related to communication and requests for assistance, and countermeasures. These are explained in detail below.

Basic parameters are static or dynamic data that characterize the physical threat (the pirates) and the target (the oil platform). They are received directly or are derived from intermediate calculations contained an alert report that is produced by a detection module which consists of a series of sensors (radar, optronics, radio, etc.) [Giraud and al., 2011]. Although at this stage the model is minimal, it provides a full understanding of the relationship between the threat and the target with the aim of providing a response to an attack. Parameters include, for example, the identity of the threat IdentityClass

(suspicious or hostile), the distance between the threat and the target DTG Threat/Asset, the criticality of the asset AssetAssesment, etc. The AssetAssesment node has four modalities (critical, major, important and other).

The overall level of danger of the situation is derived from the basic parameters. The ShowGradationLevel node is the formalization of this module in the Bayesian network. The system offers four levels of danger, ranging from 1 for the least risk to a maximum of 4. The level and planning of countermeasures are continuously adapted as the situation develops. Aggravating factors and constraints are elements that are internal and external to the system. Aggravating factors make it possible to take into account a potential deterioration in the situation and anticipate future plans. They represent the environment: visibility (Visibility) and time of day (PeriodOfDay). Constraints are represented by parameters which reflect the effectiveness of the response both technically and operationally. Technical constraints are directly related to the use of countermeasures such as availability (ImmediateReadiness) or the ability to remotely control equipment (RemoteControlled).

There is also a module that can take into account decisions by the crewmaster regarding the manual activation of countermeasures that are usually activated automatically and remotely, should they fail. These nodes are directly linked to countermeasures by intra-slice arcs using static parameter learning. Each decision node has two modalities (true or false).

Communication and requests for help are two key responses in the event of an attack. Internal communication makes it possible to alert all personnel (e.g. inform the crewmaster, InformOIM) while different levels of external communication make it possible to warn the various actors concerned (request the intervention of the patrol vessel, RequestSecurityVessel, activate the Ship Security Alert System, RaiseSSAS, etc.). This enables the various facilities and shipping in the oil field to prepare their response plan and request outside intervention if possible.

Countermeasures are the defences that are implemented when the target is attacked. They are the physical materialization of the response plan and provide a set of means and actions to normalize the situation as soon as possible. Countermeasures are divided into five sub-modules, which form a graduated response. The force of the countermeasure

depends on the threat that has been detected. Measures range from deterrence and small-scale repulsion, to repulsion, anti-boarding and neutralization, procedure management, and securing the installation.

These countermeasures are described in detail below:

- Deterrence and small-scale repulsion: This informs the attackers that the platform is aware of their intentions, that they are being monitored and that it is not in their interests to launch an attack. Small-scale repulsion refers to the target's ability to repel an assault using small-scale measures such as searchlights, fire hoses or sound cannons ActivateLRAD (Long Range Acoustic Device).
- Repulsion, anti-boarding and neutralization: These are high-impact countermeasures whose main function is at least to mitigate an attack, if not neutralize assailants. The node EngageRepellentEquipment refers to equipment and technological devices that provide long-range repulsion while remaining within the framework of non-lethal self-defence measures. The same applies to repulsive, anti-boarding equipment where the aim is to prevent pirates from boarding when they approach the facility or ship. The role of SetCrowdControlMunition is to delay the progress of the attack and exhaust or neutralize the attackers, thus giving the crew as much time as possible to manage other safety measures.
- Procedure management: This consists of the following countermeasures:
    - The CrewManagement node refers to the sounding of action stations, then assembling the crew at designated stations.
    - The AssaultAssetManagement node refers to the management of the potential target to ensure its safety and security. The modes of this node are: activate citadel mode, perform evasive manoeuvres (for ships and mobile units), and activate the safety station, which consists of a set of individual procedures to be applied by each member of the crew.
- Ensuring the safety and security of the installation: Like procedure management, the action plan proposed by the Bayesian network includes measures related to the control of the production facilities in order to shut the unit down safety, or block access to sensitive areas.

The design of Bayesian network was divided into two stages:

- The first step consisted of the construction of a static Bayesian network. This coupled data and knowledge from the database maintained by the International Maritime Organization (IMO), which contains details of pirate attacks worldwide since 1994, with material from interviews with a panel of maritime experts including a first class Merchant Navy officer, a former Navy officer and a research engineer. The procedure for the acquisition and formalization of this knowledge is described in [Bouejla and al., 2014].
- The second step was to build a dynamic Bayesian network through the addition of a temporal dimension.

4.3 Modelling time in the Bayesian network

To improve the performance of the initial, static Bayesian network and integrate the temporal dimension, a second, dynamic Bayesian network was designed. In this network, the learning process took two forms:

- Links between intra-slice arcs: these are arcs that contain a single slice and these connections are identified in the initial static Bayesian network.
- Learning of connections between inter-slice arcs: these are arcs that connect the two time slices T−1 and T. They represent time arcs for the selected variables; therefore for each node in slice T its parents can be identified from the slice T−1.

In our prototype, the number of time slices varies from one attack to another and it is impossible to know in advance the number of slices to be processed for each attack. The prototype develops and learns as the attack unfolds. Various scenarios were tested and the experimental data was used to improve the calculation of conditional probabilities.

To meet the requirements of a dynamic Bayesian network, the network carries out the following checks: first, that the structure is invariant at every time step (time-invariance), and secondly, that each time arc links a time slice T−1 to a slice T. Finally, we assume that the variables in each slice are connected in the same way.

The dynamic Bayesian network is clearly useful in modelling a dynamic process. It makes it possible to make quantitative a posteriori calculations given a priori knowledge and current observations. This type of Bayesian network can interpret the results of a

given time slice identified by connections between the nodes in the graphical models generated by the initial dynamic Bayesian network.

5. Implementation and evaluation

The (dual) Bayesian network was tested using various attack scenarios. The examination of these scenarios made it possible to assess, on the one hand, the effectiveness of the prototype to plan a response suited to the attack scenario, and on the other hand to demonstrate the benefits of coupling a static and dynamic Bayesian network.

5.1 Presentation and execution of an attack

The example shown in Figure 4-2 shows the results at time T−1 resulting from the addition of parameters that model an attack against a bulk oil tanker. This type of vessel (the target) collects oil from the production unit and delivers it to a port. These very large vessels usually visit the oil field at a frequency ranging from once per week to once per month.

This target is attacked by a merchant ship, the “Merchant Vessel”, which has itself been hijacked by a group of pirates. Merchant vessels include heavy, very slow-moving ships such as tankers and Very Large Crude Carriers (VLCC), faster, general cargo ships and container ships that can maneuver more rapidly.

The danger level of the situation is calculated from these two pieces of information (the type of target and the type of pirate ship). In this case, the value of each parameter is 2. The countermeasures proposed by the prototype are: inform the crewmaster, request the intervention of the patrol vessel, broadcast an alert and place sound guns on standby.

The processing of the attack continues and the fundamental parameters are augmented by the Bayesian network, which calculates kinematic parameters, together with the type of pirate ship and its classification as “hostile”. The distance between the target and the pirate ship is calculated to be 50–200 meters, the ranking[26] is 300–900

[26] The *RankingThreatAsset* is the time it will take the threat to cover the remaining distance to the nearest point of the target, assuming that it is able, at any moment, to change direction and circle towards the target.

seconds and the patrol vessel's response time is 300–900 seconds. These parameters increase the danger level of the situation and allow further countermeasures to be planned that respond to this new information. As new data about the attack is added (at T+3), such as reduced visibility, the failure of various countermeasures to activate automatically, the increasing proximity of the pirate ship (< 50 meters) and the decrease in the ranking (< 300 seconds), the danger level of the situation rises to 4 with a risk of boarding of approximately 67%.

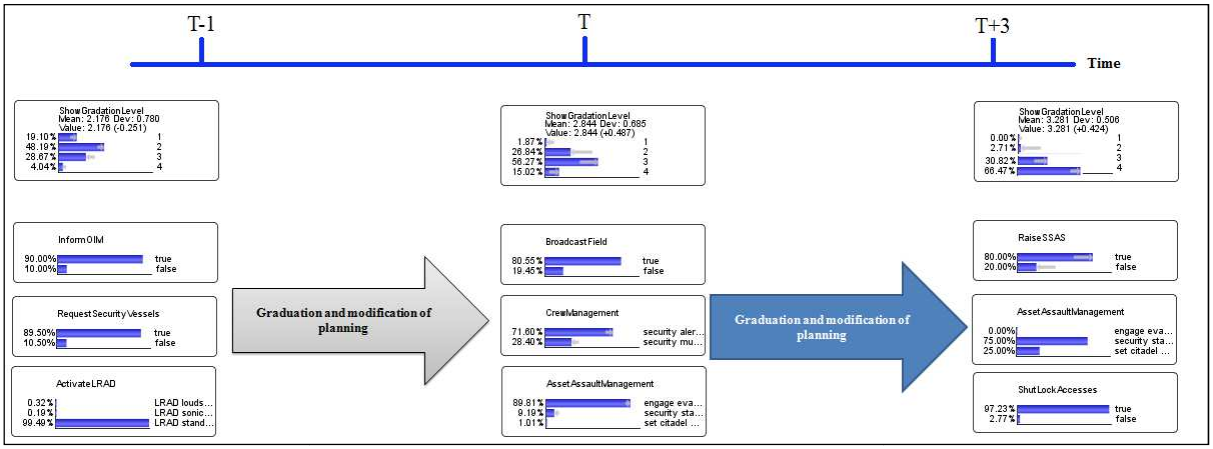


Figure 4-2 : Planning for three time slices (T−1, T and T+3) in an attack against a tanker

Our dynamic Bayesian network therefore makes it possible to launch appropriate countermeasures that are graded according to the increasing level of risk. As the scenario described above shows, the countermeasures to be applied at T−1 are the following:

- Inform the crewmaster
- Request the intervention of the patrol vessel
- Place sound cannons on standby

At time T, planned countermeasures are:

- Broadcast information about the attack by radio on an emergency or specific channel to warn other nearby targets
- Alert the crew
- Initiate evasive maneuver

Finally, the countermeasures at time T+3 are:

- Trigger the Ship Security Alert System
- Assemble the crew in the safe zone

- Block ship access

Not all countermeasures can be applied automatically and some may require the intervention of an operator. They include:

- EngageESDS: this secures the installation to prevent damage to production equipment, or limit any consequences if it is damaged
- FireHoses: this refers to the pressurization of the water circuit and the connection of fire hoses, which can be an initial dissuasive measure when the water jet is used as a repulsive weapon and if the attackers come within range (around twenty metres).
- SetCrowControlMunition: the main purpose of this type of equipment is to delay the progress of the pirates as much as possible, in order to exhaust or neutralize them, and give crewmembers time to improve barricades or implement other safety measures.

The example shown in Figure 4-3 includes an additional problem: the failure of a safety device. In this case, despite the extreme level of danger, the countermeasure that consists of blocking access to the platform cannot be activated due to a functional failure. Such a failure can endanger the lives of many people and threaten the entire production unit. The dynamic Bayesian network is able to propose a manual intervention to bring the countermeasure back into service, which improves the performance of the tool.

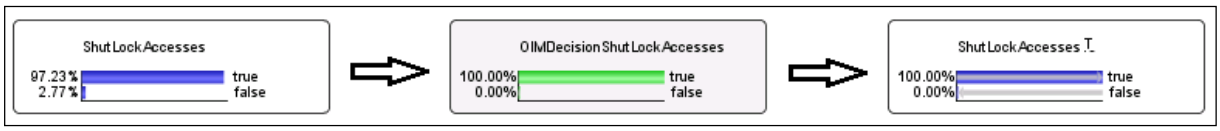


Figure 4-3 : Influence of manual intervention by the crew on the probability of the node ShutLockAccesses

5.2 Discussion

Our dynamic Bayesian network has three major advantages.

The planning of a response through the automatic production of a plan based on an intelligent analysis of the alert report. This report includes all the information necessary to prepare a physical response to the threat. The Bayesian network can manage all the interactions between threat characteristics and the target of the attack, the environment,

crew and facility management, and most importantly, it can adapt to changes in the level of danger of the situation.

On the other hand, the dynamic Bayesian network can disable countermeasures initiated in earlier processing of the attack that are no longer suited to the new level danger level. The system's man-machine interface consists of a dashboard showing the processing of the attack in two time slices, which makes it easy to compare the parameters in both situations and gives an overview of the evolution of the attack.

Finally, the network can take into account the need for operator intervention. The example shown in Figure 4-3 shows the inclusion of decisions taken by the crewmaster. Such decisions can exacerbate or reduce the danger level of the situation. This feature makes it possible to partially de-activate automatic defence measures and bring them under mechanical control taking into account the presence or absence of the crewmaster, their professional experience and the situation. This means that the operator is no longer a passive actor in the decision-making process. They can also assign probabilities to the countermeasures triggered by the system and/ or make them 100% manual. This option makes a large contribution to improving the diagnosis of the situation.

Despite these strengths, the network structure is still difficult to manipulate. An increase in the number of nodes and arcs is not a straightforward matter. The increase in the number of parents of a node automatically generates large probability matrices. In the case where the network is only constructed from database information, this problem can be easily handled by automatic learning. However, when expert knowledge is involved, the determination of probabilities requires a lot of work in order to establish credible scenarios and a long testing and validation phase based on various examples and attack scenarios.

6. Conclusion

Static and dynamic Bayesian networks are excellent tools for modelling uncertainty, due to their clear graphic representation and the associated conditional probability laws. The real advantage of dynamic Bayesian networks is that they can take account of the progress of time. They make it possible to carry out a qualitative and dynamic

interpretation of results through the analysis of interdependencies between variables in many time slices linked by connections between nodes in the initial graphical models.

In this article, we presented the design process for a diagnostic and response planning system to handle pirate attacks against oil fields based on a static Bayesian network. The limitations of this type of network led us to look at the contribution of dynamic Bayesian networks. This type of network can take account of changing situations through the incremental processing of data as it is collected. Consequently, we were able to design a system prototype that can be used by oil field operators to increase their decision capacity when faced with a pirate attack. The prototype makes it possible to plan reactions and responses at every moment as the attack unfolds.

Acknowledgments

The authors would like to thank the company Preventeo for their support for this research project.

References

Aleklett K., Hook M., Jakobsson K., Lardelli M., Snowden S. and Soderbergh B. (2010). The pick of the oil age – Analyzing the world oil production reference scenario in world energy outlook 2008. Energy Policy, Volume 38 Issue 3, pp. 1398–1414, March 2010.

Anifowose B., Damian M.L., Dan van Der H. and Lee C. (2012). Attacks on oil transport pipelines in Nigeria: A quantitative exploration and possible explanation of observed patterns. Applied Geography, Volume 32 Issue 2, pp. 636‑651, March 2012.

Bouejla A., Guarnieri F. and Napoli A. (2014). A Bayesian network to manage risks of maritime piracy against offshore oil fields. Safety Science, October 2014.

Darwiche A. (2000). A differential approach to inference in Bayesian networks. Proceedings of uncertainty in Artificial Intelligence, pp.123–132.

Flin R., Mearns K., Fleming M. and Gordon R. (1996). Risk perception and safety in the offshore oil and gas industry. Health and safety executive-offshore technology report.

Giraud M.A., Alhadef B., Guarnieri F., Napoli A., Bottala Gambetta M., Chaumartin D., Philips M., Morel M., Imbert C., Itcia E., Bonacci D. and Michel, P. (2011). SARGOS: Securing Offshore Infrastructures Through a Global Alert and Graded Response. System Workshop MAST Europe, pp. 27–29, 27 June 2011.

Gordon R.P.E., Flin R.H., Mearns K. and Fleming M.T. (1996). Assessing the human factors causes of accidents in the offshore oil industry. International conference on health, safety and

environment in oil and gas exploration and production, No 3, New Orleans, United States, pp. 635–644.

Hansen S.J. (2009). Piracy in the greater Gulf of Aden, Myths, Misconception and Remedies. Norwegian Institute for Urban and Regional Research.

Jordan M.I. (1998). Learning in Graphical Models, MIT Press.

Jordan M.I. (1999). An Introduction to Variational Methods for Graphical Models. Machine Learning, 37, pp. 183–233

Kaasen K. (1984). Safety Regulation of Offshore Petroleum Activities: a Study of the Legal Framework on the Norwegian Continental Shelf. Oslo University.

Kashubsky M. (2008). Offshore energy force majeure: Nigeria's local problem with global consequences. Maritime studies.

Kim J.H. and Pearl J. (1983). A computational model for causal and diagnostic reasoning in inference engines. Proc. 8th Int. Joint Conf. on Artificial Intelligence, pp.190–193.

Lauritzen S.L. and Spiegelhalter D.J. (1988). Local Computations with Probabilities on Graphical Structures and Their Application to Expert Systems, Journal of the Royal Statistical Society. Series B (Methodological), Volume 50, No 2, pp. 157–224.

Murphy K.P. (2002). Dynamic Bayesian networks: Presentation, Inference and Learning. Cambridge University.

Nincic D.J. (2009). Maritime Security as Energy Security: Current Threats and Challenges. In Luft G. and Konin A., (Eds.) Energy Security: Challenges for the 21st Century. Washington DC: Greenwood Publishing in collaboration with the Institute for the Analysis of Global Security (IAGS).

Pearl J. (2000). Causality: Models, Reasoning and Inference. Cambridge University Press, ISBN, 0-521-77362-8.

White H.K., Hsing P.Y., Cho W., Shank T.M., Cordes E.E., Quattrini A.M., Nelson R.K., Camilli R., Demopoulos A.W.J., German C.R., Brooks J.M., Roberts H.H., Shedd W., Reddy C.M. and Fisher C.R. (2011). Impact of the Deepwater Horizon oil spill on a deep-water coral community in the Gulf of Mexico, Cross Mark, Volume 109 No 50, November 2011.

Wright C. (1994). A fallible safety system: institutionalised irrationality in the offshore oil and gas industry. The sociological review, Volume 42 Issue 1, pp. 79–103

Yergin, D. (2006). Ensuring Energy Security, Foreign Affairs. Volume 85, No. 2.

Chapitre 5 : Article 4 : Couplage entre Réseau Bayésien Statique et Dynamique en mesure de répondre au risque de Piraterie Maritime contre les champs pétroliers Offshores

5.1 Présentation de l’article

Cet article a été soumis à la revue Ocean Engineering. Il décrit le couplage entre réseau bayésien statique et réseau bayésien dynamique et souligne les apports et les limites des deux systèmes.

5.2 Version anglaise de l'article

A coupled Static and Dynamic Bayesian Network able to respond to Maritime Piracy against Offshore Oil Fields

Abstract

This article describes a prototype decision support tool to be used in the fight against maritime piracy. A static and a dynamic Bayesian network were coupled in order to develop a graphical decision support model of an uncertain world. Not only does this type of coupled network make it possible to compare the respective and complementary inputs, it can also incorporate into knowledge bases, probability distributions that can predict the future, given the past. This article describes in detail the methodological approach to the design of a prototype for risk diagnosis and the planning of countermeasures to be applied in the case of a pirate attack against an offshore oil platform. The prototype provides supports for decision-making by taking into account the impact of a decision taken at time T−1 on a decision that must be taken at time T.

Keywords

Bayesian networks, Maritime piracy, Oil fields, Decision support systems.

1. Introduction

Far from the fictionalized images of piracy described in romantic novels set in the age of sail, modern piracy is a violent phenomenon whose upsurge is a concern to international maritime authorities.

"*Piracy consists of any of the following acts:*

(a) Any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private aircraft, and directed:

(i) On the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;

(ii) Against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;

(b) Any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;

(c) *Any act inciting or of intentionally facilitating an act described in sub-paragraph (a) or (b).*[27]"

This definition suggests that individuals and organizations that perform attacks against fishermen, commercial vessels, recreational sailors or oil platforms are particularly determined, and often well-equipped (with transport, communications, weapons, etc.). Their battle-hardened "captains" ensure the sustainability of this criminal activity and manage attacks as if they were a global business (Figure 5-1).

Pirates have at their disposal very powerful speedboats that can easily catch a heavy merchant ship. The latter can only slow down, and are unable to tack or increase speed in order to shake off a small boat. These "floating dollars" are easy prey as they cruise in waters that are not regularly patrolled by coastal authorities [Onuoha, 2010]. The pirate "mother ships" are stationed behind this field of "operations" and are equipped with the latest object-location technologies. This allows them to precisely identify their target and organize their attack. Their targets are taken by surprise, typically by speedboats that they are unable to detect.

Figure 5-1 : Distribution of maritime piracy in 2013 (Source: International Maritime Bureau)

Acts of piracy continue to multiply. In 2013, 264 attacks were identified by the International Maritime Bureau (IMB), including 141 in South-East Asia and 51 in West Africa. 85% of the attacks took place at night and the main targets were commercial vessels (tankers, bulk carriers and tugs with barges) at anchor or sailing at low speed. In

[27] This definition of piracy is contained in article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS).

most cases, the pirates attempted to steal cargo or equipment that could be easily resold, or pillage the ship itself. However, in other cases they also attempted to kidnap crew members. According to the IMB, one in four attacks, where there was no intervention by national naval forces, was successful.

In the early 2000s, pirates were armed with knives. Today, they attack with automatic weapons. This finding, although not surprising, is alarming. According to a report by the IMB, pirates carried out 85 attacks in the first half of 2014 (Figure 5-2).

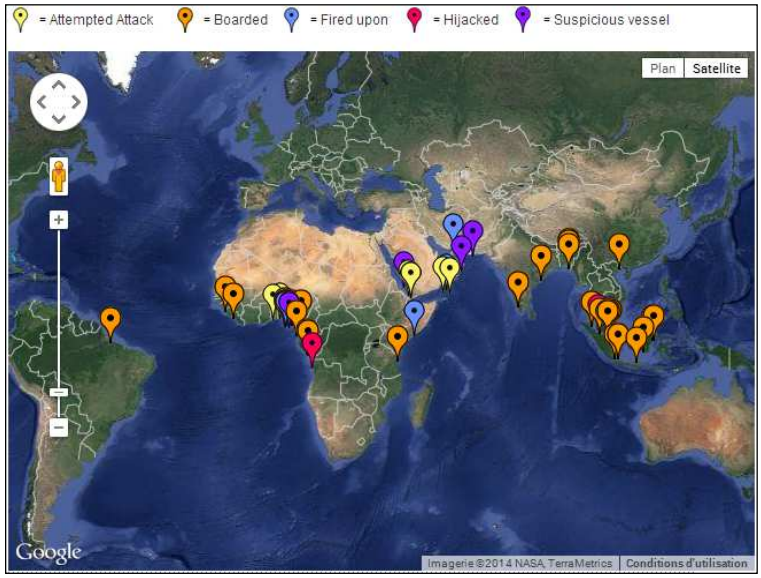


Figure 5-2 : Map of the distribution maritime piracy acts in the first half of 2014 (Source: IMB)

Although attacks on offshore energy infrastructure are less frequent and receive less publicity, they are no less worrying. They demonstrate the vulnerability of an economic sector where the stakes are very high. Given the scarcity of onshore resources, production has had to move offshore where it faces the new threat of piracy.

Acts of piracy have increased considerably since 1988. [Kashubsky, 2008] conducted a detailed study of Nigeria which showed that the reassuring hypothesis that offshore installations would be protected by virtue of their geographical distance was no longer true. The attack in June 2008 against Shell's offshore infrastructure 120 km off the coast of Nigeria (the Bonga oil field) which led to a production stoppage and losses estimated at over 200,000 barrels per day, or that on the French company Perenco's ship that was carrying Cameroonian security forces near to an oil rig in the Gulf of Guinea (leading to the death of six Cameroonian soldiers), show that distance is no longer a guarantee of safety [Nincic, 2009].

Faced with this known threat, various technological systems have been designed and developed, with mixed success. Two constraints must be taken into account: uncertainty and time. Bayesian networks have proved to be an effective way to overcome these constraints and provide support for decision making. Our research showed that a dynamic network offered many benefits as a complement to a so-called “static” network. Consequently, we have designed a model and developed a prototype which brings together these two types of network. The prototype has been tested and the results examined in realistic pirate attack scenarios.

2. Decisions support systems for maritime piracy against offshore oil platforms

Security on offshore installations is currently provided by conventional decision support tools: a lookout, radio identification, Automatic Identification Systems (AIS), radar monitoring of traffic, etc. These tools can be complemented at a national level by naval forces in certain countries, and at a local level by patrol boats operated by subcontractors [Giraud and al., 2011] who are employed by operating companies.

Nevertheless, resources are limited. Patrol vessels are few and far between, expensive and not necessarily located very close to the event. As for radar monitoring of sea traffic, the priority is to detect “friendly” large- or medium-sized mobile objects. Radar systems suffer from a blind spot at distances close to the origin and are not particularly suited to the detection of small marine targets such as speedboats or jet-skis that have a small radar or optronic signature (lack of reflective surfaces or AIS), operate in open waters (sea clutter) and are – of course – unfriendly. The only viable option is a human lookout; a system that does not perform well at night or in degraded visibility due to weather conditions.

In addition to the limitations (technological or physiological) of tools and resources (technical or human), threat characterization is not always straightforward in uncertain conditions. False alarms are a real problem and have discredited many of the solutions offered to oil companies [Mukundan, 2003].

A central issue for the resolution of the problem is how uncertainty is handled. Bayesian networks are one technique for the processing and analysis of data in conditions

of uncertainty [Nielsen and Verner Jensen, 2007], and this was the solution we selected. Our decision was supported by earlier work in the maritime domain.

[Ren and al., 2008] discussed the contribution of static Bayesian networks in modelling human factors in cause and effect relationships for the assessment of maritime security. They designed and developed a methodology based on James Reason's "Swiss cheese" model [Reason, 1990]. Reason's model provides a generic human factors risk assessment framework. Five levels are used to characterize latent failures within the causal chain of events: root causes, triggers, events, incidents, accidents and their consequences. In Ren's work, a detailed characterization of each level led to the construction of a Bayesian network. A series of events was specified, and the a priori conditional probabilities of the model were assigned based on characteristics intrinsic to each event.

[Trucco et al., 2008] presented an approach for the integration of human and organizational factors into risk analysis. Although the approach was developed and applied to a case study in the maritime industry, it can also be used in other economic sectors. A static Bayesian network was developed to model risk associated with maritime transport systems; it took into account various actors, such as ship-owners, ports and shipyards, and their mutual influences.

Finally, [Dabrowski et al., 2013] proposed a generic model to characterize the behaviour of pirate ships. The model was designed using dynamic Bayesian networks and derived exclusively from a summary of data taken from the "Piracy and Armed Robbery" database maintained by the IMO. Among the factors that can influence the model, kinematic data such as position and velocity is given the greatest weight. The model includes three classes of vessels: transport vessels, fishing boats and pirate ships. It was evaluated through a comparison of its predictions with actual records taken from the IMO database in the Gulf of Aden and the Indian Ocean. The model is limited to the prevention of the risk of pirate attack through an analysis of ship behavior.

These studies contributed to our solution to the problem as they supported the idea of designing and deploying Bayesian networks, which can provide decision support for the

protection of offshore oil installations. The aim of our work goes beyond a new field of application (offshore energy infrastructure) and addresses the entire decision-making process. It uses quantitative data and expert knowledge throughout the process; from the diagnosis to the processing of the threat though the implementation of various tools and defence mechanisms.

3. A static Bayesian network model of maritime piracy

Our proposed “system” is inherently complex. Several parameters characterize this complexity: the marine environment (principally the sea state), meteorology (and its impact on visibility and the mobility of attackers), the type of infrastructure to be protected, and of course, the ingenuity of the attackers. The asset to be protected takes many forms, for example a floating production, storage and offloading (FPSO) platform, speedboats used for crew transfers (crewboats), bulk oil tankers, etc. Pirates also have diverse means at their disposal: highly-maneuverable ships or small boats (High Manoeuvrability Boats), fishing or commercial vessels (themselves pirated), or simple dugout canoes. The attacker’s choice of mode of transport is a decisive factor as it influences kinematic parameters such as the speed and acceleration of the pirate ship, which is used to calculate the distance between the latter and the asset to be protected. These are both the basic parameters and the constraints that make it possible to clearly define the situation.

It is clear that in the face of a threat an immediate response is required, and various tools have been designed and developed. An oil platform is able to deploy an arsenal of countermeasures, such as the Ship Security Alert System (SSAS), sound cannons, searchlights, etc. [Morel and al., 2007]. These tools can be tailored to the type of attack and the danger level of the situation.

The representation and management of the parameters and response modes that characterize this complexity requires a graphical system. This system must enable interactions between attack parameters and response modes that help those responsible for an oil platform to take effective and appropriate decisions in an emergency situation. Given these constraints,

Bayesian networks appeared to offer the most appropriate solution (§ 2).

Bayesian network are based on Bayes inverse probability formula:

$$P(\mathbf{H}|\mathbf{e}) = P(\mathbf{e}|\mathbf{H}) \times \frac{P(\mathbf{H})}{P(\mathbf{e})}$$

Equation 5-1 : Bayes' theorem

For any hypothesis H and observation e.

A Bayesian network ([Pearl, 2000] and [Heckerman, 1999]) is a probabilistic model based on any n variables, X1, ..., Xn, defining the conjunction P (X1 ... Xn), by a satisfactory decomposition of the following property:

$$P(X_1 \dots X_n) = \prod_{i=1}^{n} P(X_i \mid Pa_i)$$

Equation 5-2 : Decomposition of Equation 1

Where Pa_i is a subset of $\{X_1, ..., X_{i-1}\}$.

This formula makes it possible to simplify the information necessary to calculate the joint probability of the set $\{X_1, \ldots, X_{i-1}\}$. Thus, rather than specifying the probability of X_i conditional on all the calculations of its predecessors $X_1, ..., X_{i-1}$, only those that are conditioned by the elements of Pai must be specified. This set is called the parents of X_i.

Bayesian networks are a marriage between probability theory and graph theory. Consequently, they provide tools that address two major problems commonly encountered in Intelligence Artificial, applied mathematics and engineering: uncertainty and complexity. In particular, they play an increasingly important role in the design and analysis of algorithms related to reasoning and learning ([Jordan, 1998]; [Naïm and al., 2004] and [Darwiche, 2000]).

3.1 The expected benefits of Bayesian networks

The use of Bayesian networks has many advantages that have been widely reported and discussed in the literature [Efron, 2010]. Table 1 is extracted from the work of [François, 2006] and describes the advantages of probabilistic graphical models.

The advantages of graphical models	The role of graphs in probabilistic models	The advantages of probabilistic models
A way to represent relationships between attributes clearly and intuitively	Provide a simple and effective way to express hypotheses	Probabilistic knowledge extraction (which variables are correlated, dependent or conditionally independent)
Can represent cause and effect relationships	Provide a compact representation of joint probability functions	Diagnosis: an evaluation of **P** (causes/symptoms) Prediction: an evaluation of **P** (symptoms/causes) and Classification: the calculation of max $P_{classes}$ (class /observations)
Graphical models are able to handle uncertainty and inaccuracy	Facilitate inference from observations	

Table 5-1 : The advantages of probabilistic graphical models (Source: [François, 2006])

One of the challenges in our research is the large amount of data to be processed. It is therefore useful to have one or more models that can link observations and reality in a specific context, including cases where observations are incomplete and/ or inaccurate. In the context of maritime piracy the volume of data is significant and includes the IMO's Piracy and Armed Robbery database, real-time data captured by radar and radio sensors, marine and meteorological data, etc. and expert knowledge. In this scenario it is crucial to establish relevant relationships between variables in the marine environment (time of day, meteorology, etc.), variables related to the oil platform (type, vulnerability, available countermeasures, etc.) and those concerning the pirate ship (type of vessel, level of armaments, etc.).

Bayesian networks provide a compact representation of these sets of dependencies through the concept of separation and the use of conditional probability tables. It is important not to confuse Bayesian networks with expert systems. A rule-based expert system is often defined as an application that can perform logical reasoning comparable to that of a human expert. It is based on databases of facts and knowledge and an inference engine, which can make logical deductions. In practice, an expert system models how an expert reasons and then attempts to reproduce this reasoning in response to new requests. On the other hand, a probabilistic model does not model how the expert reasons: rather it models the qualitative knowledge held by the expert. Consequently, such a model is not an expert system in the sense that the term is usually used, as the reasoning that is carried out is not logical, but probabilistic [Cowell and al., 1999].

With respect to conditional dependencies, the expressive power of directed graphical models (such as Bayesian networks) is neither better nor worse than undirected models,

but they do lend themselves to a causal interpretation. We selected directed models for our work as they are more intuitive and visual. Graphical models guide the interpretation of the structure, in the same way as they provide a guide during inference and learning. These models are also easier for domain experts (who often base their reasoning on cause and effect relationships) to construct [Langseth and Bangso, 2001].

Probabilistic networks also represent uncertain knowledge in ways that are more flexible than those conventionally found in rule-based systems. For example, different combinations of attack parameters are observed for different types of oil platform and strict rules cannot always be applied to diagnose the situation. In such a complex attack scenario requiring an appropriate response, a human expert is able to give an opinion even when some of the necessary data is missing. An expert system cannot do this, while a probabilistic model can.

Bayesian networks are more easily adapted and updated to the context than rule-based systems. Experience shows that it is now easier and faster to create graphical models; furthermore, as they are very intuitive, communication with experts becomes easier [Neapolitan, 2012].

Finally, although Bayesian networks can model the subjective knowledge of an expert, they do not model how the expert reasons. They therefore transform knowledge into an interpretable model that integrates quantitative and qualitative data. Once this compact probabilistic graphical model has been constructed it can be used to reason, without having to refer back to the original data [Darwiche, 2009].

3.2 The design and development of the model

This section outlines the development of our prototype decision support system, which is designed to reduce the vulnerability of oil and gas field operators to pirate attack. It is based on the coupling of a static and dynamic Bayesian network. A temporal or dynamic Bayesian network is a stochastic and statistical model which extends the concept of the Bayesian network. Unlike static networks, a dynamic Bayesian network can represent a discrete sequence of changes in random variables based on, for example, time steps. The dynamic term characterizes the system being modelled (here the oilfield and its actors – operators and pirates), and not the network, which does not change.

3.2.1 General architecture of the model

To the best of our knowledge there is no established methodology for the acquisition and formalization of knowledge that forms the basis for a Bayesian network. There are, however, two sets of techniques that can be grouped into categories that reflect the fundamental constituents of a Bayesian network: its structure and its parameters [Heckerman and al., 1997]. In this part of our work, we used BayesiaLab[28] software.

The first step was to create a static Bayesian network from the contents of the IMO's Piracy and Armed Robbery database. The database contains records of actual pirate attacks against ships and oil platforms. It includes details of 6,472 attacks since 1994. This data makes it possible to determine, on the one hand the tactics used by pirates and on the other the most frequently-used and effective countermeasures. Based on the network structure, the next step is to calculate probability tables (estimate a priori probability distributions or probability law parameters) from this data. In the case of the IMO database, two cases emerged: 30% of the records were complete (all variables had a value), while 70% were not. In the case of complete records, the statistical analysis consisted of calculating the probability of an event based on the frequency of occurrence of the event in the database. This is called the "maximum likelihood" approach [Meganck and al., 2006]. For incomplete records we used the statistical learning method, supplemented by an initial step that estimated missing parameters from their average [Friedman and Goldszmidt, 1998]. This is known as the "Expectation-Maximization" algorithm. It is a two-stage iterative algorithm; the first uses inference techniques to calculate missing network parameters, while the second calculates missing values, and then maximizes all parameters.

As a supplement to the knowledge base developed from the IMO database, a team of experts in the maritime domain was recruited, consisting of: a 1st class Merchant Navy officer, a former Navy officer and a research engineer. A probability scale was drawn up to enable these experts to estimate quantitatively (or qualitatively) the probability of a defined event. This was particularly effective as each parameter in the Bayesian network is a conditional probability law whose size increases exponentially with respect to the

[28] http://www.bayesia.com

number of its parents. As it is unrealistic to ask experts to provide values for each of these laws, the probability scale helped them to reach a decision.

The planning of potential responses to a pirate attack is determined by real-time knowledge about the various threats that are detected (behavioural criteria, identity class, and comparison with situations previously encountered and recorded in the system). Planning must also take into account possible limitations created by the physical location of the oil field or its legal status. Static Bayesian networks are able to manage all the possible interactions between the threat characteristics, the target and the environment in order to determine the best sequence of responses. Consequently, the action plan can constantly adapt to changes in the danger level. This plan is presented as a decision-making support to the operator who validates the various stages; proposed measures can range from the triggering of an alarm through to the activation of non-lethal repulsion devices. This recommendation includes basic parameters, the overall danger level of the situation, aggravating factors and constraints, and nodes related to communication, a request for help and countermeasures (Figure 5-3).

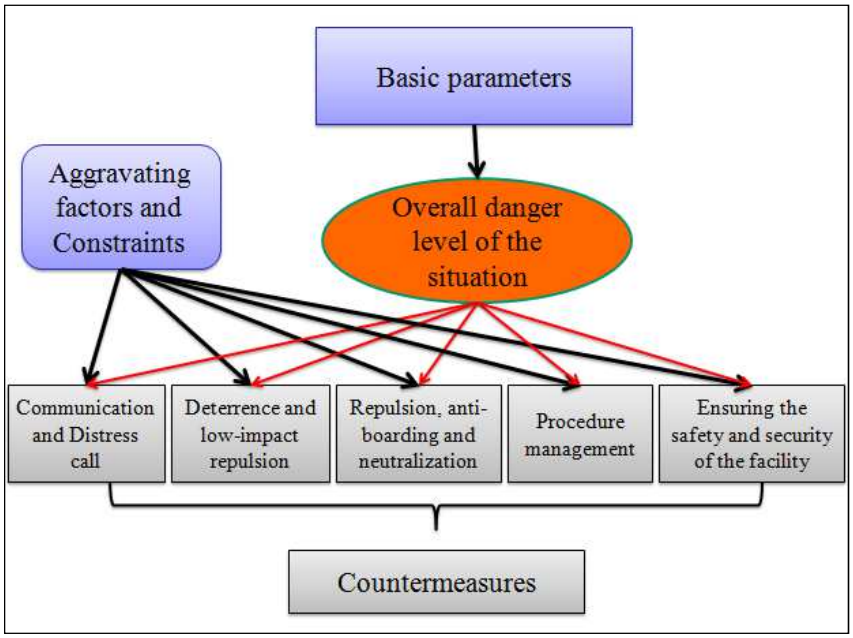


Figure 5-3 : Structure of the static Bayesian network for response planning to a piracy attack

3.2.2 The model parameters

The various parameters of the model are listed and detailed in Table 5-2.

Family	Description	Examples of parameters
Basic parameters	Static or dynamic physical data that characterize the threat and the target. They come directly from, or are derived from intermediate calculations and the alert report, produced by the system's detection module.	These parameters include the identity of the threat "*IdentityClass*" (suspicious or hostile), the distance between the threat and the target "*DTGThreat/Asset*", and the criticality of the target "*AssetAssessment*", etc.
Overall danger level of the situation	The overall danger level of the situation	The "*ShowGradationLevel*" node is the formalization of this module. The grading system ranges from 1 (for the lowest risk) to 4 (maximum risk).
Aggravating factors and constraints	Internal and external elements of the system.	They represent the environment: visibility "*Visibility*" and time of day "*PeriodOfDay*". Technical constraints are directly related to the use of countermeasures such as availability "*ImmediateReadiness*" or remote control "*RemoteControlled*".
Communication and distress call	Internal communication at the target makes it possible to alert all personnel, while external communication makes it possible, to varying degrees, to alert the various actors to survival-at-sea safety measures.	Examples: inform the crewmaster "*InformIOM*", request the intervention of the patrol vessel "*RequestSecurityVessel*", implement the Ship Security Alert System "*RaiseSSAS*", etc.)
Countermeasures	These are all the defences implemented when the target is attacked to protect it from an identified threat. They are divided into four sub-modules.	Deterrence and low-impact repulsion: this informs the attackers that the target is aware of their intentions. Example: activate fire hoses or sound cannons "*ActivateLRAD*" (Long-Range Acoustic Device).
		Repulsion, anti-boarding and neutralization: these are high-impact active countermeasures whose main function is to at least mitigate if not neutralize attackers. Example: "*Set CrowdControlMunition*" where the intention is to delay the progress of the attack.
		Procedure Management: the "*CrewManagement*" node concerns the sounding of action stations on the infrastructure, while the "*AssaultAsset Management*" node concerns the management of the potential target with a view to ensuring its safety and security.
		Ensuring the safety and security of the facility: this relates to maintaining control of production facilities in order to carry out a safe shutdown or deny access to sensitive areas.

Table 5-2 : Detailed description of the modules in the static Bayesian network

The countermeasures managed by the prototype take the form of an escalating scale that makes it possible to grade the response to an attack. In this way, the response can be

adapted to the nature of the threat and its development. A network of internal and external communication systems designed to broadcast warnings and coordinate the response and the request for assistance is also activated.

In the prototype Bayesian network, each module or sub-module consists of one or more nodes that receive and/ or transmit causal relationships to other nodes. Each node consists of a matrix of conditional probabilities that are calculated taking into account interactions with other nodes and the current situation. For example, the probability distribution for activating searchlights “ActivateSearchLight” interacts directly with visibility, time of day and technical constraints such as the availability and the ability to remotely control countermeasures.

4. Testing and verification of the model

Our static Bayesian network can formulate and trigger a set of countermeasures in an emergency situation. For each alert, the network determines a set of responses to activate depending on the basic attack parameters (type of pirate ship, vulnerability of the target, distance between the target and the pirate ship, etc.).

Whenever a suspect or hostile vessel appears, the system receives an alert report compiled from data collected by the various sensors present on the platform (radar, optronic reports, AIS, watch, etc.). This report calculates various parameters such as the distance between the target and the suspect ship, the time required for the patrol vessel to intervene, etc. It also defines basic parameters such as the type of suspect vessel, its level of armaments, and the presence of a patrol vessel, etc. These parameters are integrated into the Bayesian network in order to calculate the danger level of the situation and develop the set of countermeasures to be applied.

A probability scale (Figure 5-4) was used to determine the countermeasures and procedures to be triggered following the detection of an attack. The choice of countermeasures varies according to the situation, which gives rise to a need to establish a threshold for their activation (i.e. to select the response that is most relevant at a given time T). This threshold was chosen by the team of maritime experts and was set at 70%.

Consequently, only countermeasures for which one of the modalities has a probability strictly greater than 70% are recommended and triggered.

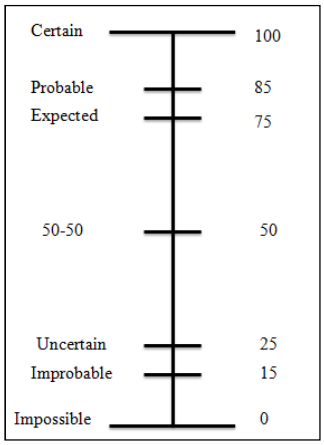


Figure 5-4 : Probability scale

The example below (Figure 5-5) shows the results related to the insertion of parameters related to an attack on a crewboat used to transport personnel or parcels between the various installations and/ or land by an unknown ship that is assumed to be a threat. The danger level of the situation is 2 with a percentage higher than 43%; in this case the countermeasures to be applied are:

- Inform the crewmaster
- Request the intervention of the patrol vessel
- Put sound cannons on standby
- Alert the entire crew

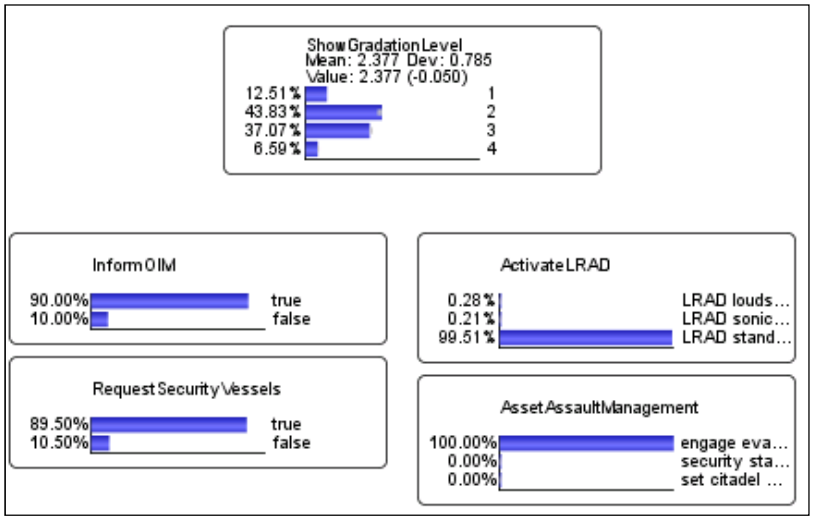


Figure 5-5 : Planning of the response to an attack against a crewboat (initial planning at time T)

The response plan proposed by the prototype is adapted to the level of danger of the situation and changes according to updates in the threat parameters (the unknown ship) and the target (the speedboat). Other attack parameters can be added, such as: a ranking[29] of less than 300 seconds, a distance less than 50 meters, pirates equipped with a highly-maneuverable ship or small boat (i.e. a vessel with a small turning circle, high maximum speed and fast acceleration that can quickly change direction) and who are armed. In this case, the vulnerability of the target is defined as "major". The danger level is now equal to 3 and the probability of the countermeasures that were recommended in the initial plan has increased (Figure 5-6).

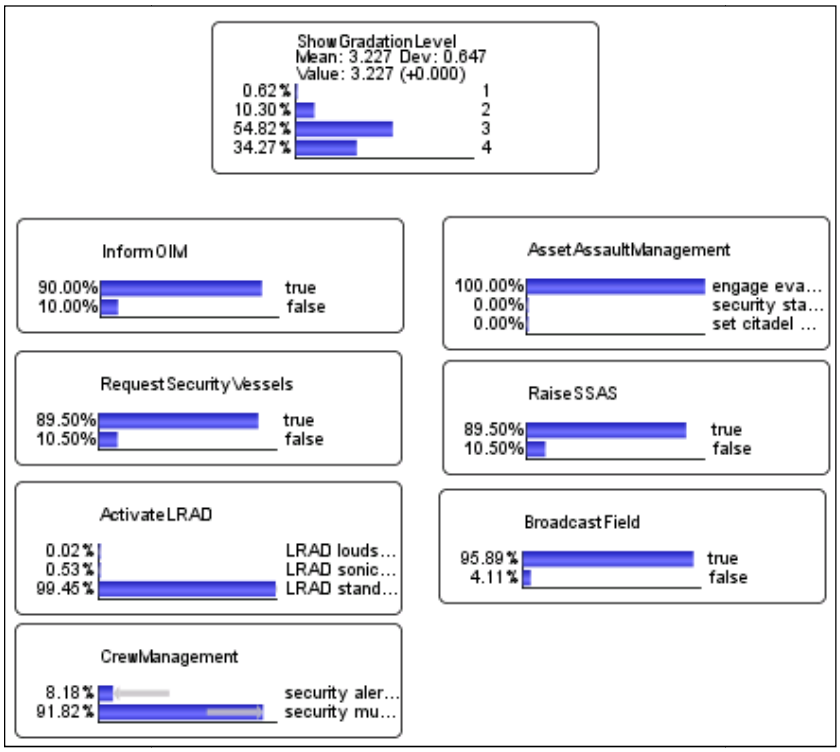


Figure 5-6 : Planning of the response to an attack against a crewboat (second plan at T+1)

The new countermeasures to be activated become:

- Initiate evasive manoeuvres,
- Trigger the Ship Security Alert System (SSAS),
- Prompt the operator to broadcast information about the attack to warn other nearby targets on VHF 16 or another specific channel.

[29] The "*RankingThreatAsset*" corresponds to the time necessary for the threat to cover the remaining distance to the nearest point of the target, taking into account the fact that at any moment the threat can change direction and circle around the target.

Despite the adaptability, scale and responsiveness of the static model presented above, there are several limitations that have an impact on the decision-making process. These limitations are explained and examined in the next section.

5. Application of the dynamic Bayesian network model

In the static model, each change in the attack parameters is processed as a new emergency (a new event); therefore this prototype is not able to dynamically process the attack from beginning to end.

Moreover, in the case of a pirate ship that is heading for a platform or an oil tanker, the basic parameters can change from one moment to another depending on the distance between the two objects. This change is generally influenced by improvements in detection. When this happens, the countermeasures that are recommended by the Bayesian network reflect changes in the captured information, but the model retains those countermeasures that were triggered during initial processing. As Figure 6 shows, the basic attack information available at time T puts the danger level of the situation at 2 with about a 44% probability. In this case, the prototype automatically sends a request for the intervention of the patrol vessel, broadcasts a warning by telephone, and sends an alert to the crewmaster. At time T+1, the attack parameters have changed: the distance between the target and the attacking vessel is less than 50 meters, and the ranking is less than 300 seconds, etc. In this case, the danger level of the situation is 3, which triggers other countermeasures such as evasive maneuvres. In Figure 5-7, (T+2), the time for the patrol vessel to respond is estimated to be above 900 seconds, the vessel is identified as “suspect” and visibility is reduced.

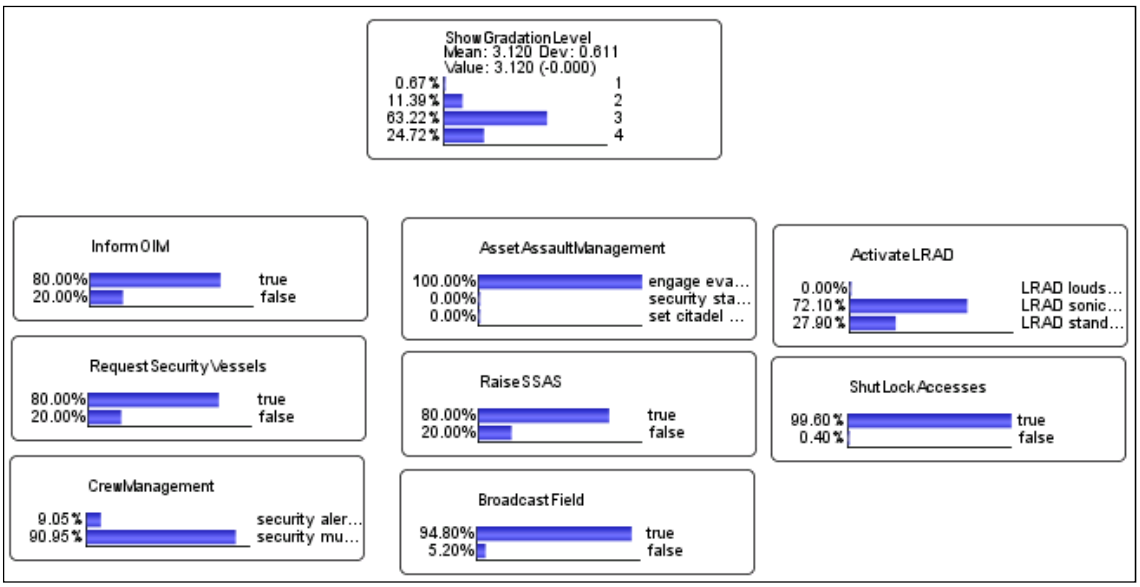


Figure 5-7 : Response planning for an attack against a crewboat (Third plan, T+2)

This example highlights a major drawback of the static model. It shows that most of the countermeasures activated at time T will still be active at time T+2 (probabilities are greater than 70%), although they are no longer appropriate in the new situation. This leads to excessive use of countermeasures as the attack develops and consequently leads to confusion in the choice of measures to be activated by crewmembers.

Not all countermeasures are deployed automatically and some require the intervention of an operator to trigger them. Examples include:

- “EngageESDS”: ensuring the safety of the installation in order to ensure as far as possible that the production unit is not damaged or, if it is, that the consequences are as limited as possible.
- “FireHoses”: this concerns the pressurization of the fire circuit and the connection of fire hoses, which can be an initial dissuasive measure. In this case, a water jet is used as a repulsion weapon if the attackers are within range (around twenty meters).
- “SetCrowdControlMunition”: the main function of this equipment is to delay the progress of attackers who have boarded the facility as much as possible, in order to exhaust or neutralize them and give the crew time to improve barricades or perform other safety actions.

These countermeasures must be deployed carefully as it is imperative that there is no confusion about their use. The all depend on the progress of time, which supports the idea that a dynamic Bayesian network is a valid approach for an optimal solution.

A dynamic Bayesian network was developed to compensate for the limitations of the static network described above. The methodological approach involved the addition of new nodes and a temporal dimension: nodes and arcs were introduced that could characterize a changing situation.

A dynamic Bayesian network is a factored representation of a Bayesian network where the nodes are indexed over a discrete time scale. As it is impossible to represent an infinite structure, a graphical notation is used in which nodes are indexed by generic time steps and two types of links: the conventional links found in static Bayesian networks and so-called temporal links that define the conditional probability tables of nodes conditional on their parents at an earlier time index [Bouissou and Bourreau, 2012].

The architecture of the dynamic Bayesian network shown in Figure 5-8 is characterized by the part (B_1, B->), where B_1 defines a priori P (Z_T) and B-> is the time slice of the Bayesian network which defines P ($Z_T \backslash Z_{T-1)}$, where Z is a random variable described by Z_t= (U_t, X_t, Y_t) representing the model's nodes. The dotted lines are temporal arcs between time slices. These arcs run from left to right and reflect the progress of time.

Next, we examine a discrete dynamic stochastic process. In this case, the index T is incremented by one each time new data is captured by the system.

The dynamic Bayesian network contains a "crewmaster decision" module. The nodes in this module take into account the crewmaster's decisions regarding the manual activation of countermeasures or those where automatic remote operation devices have failed. These nodes are directly connected to countermeasures by intra-slice arcs based on learning from static parameters. Each decision node has two modalities: true or false.

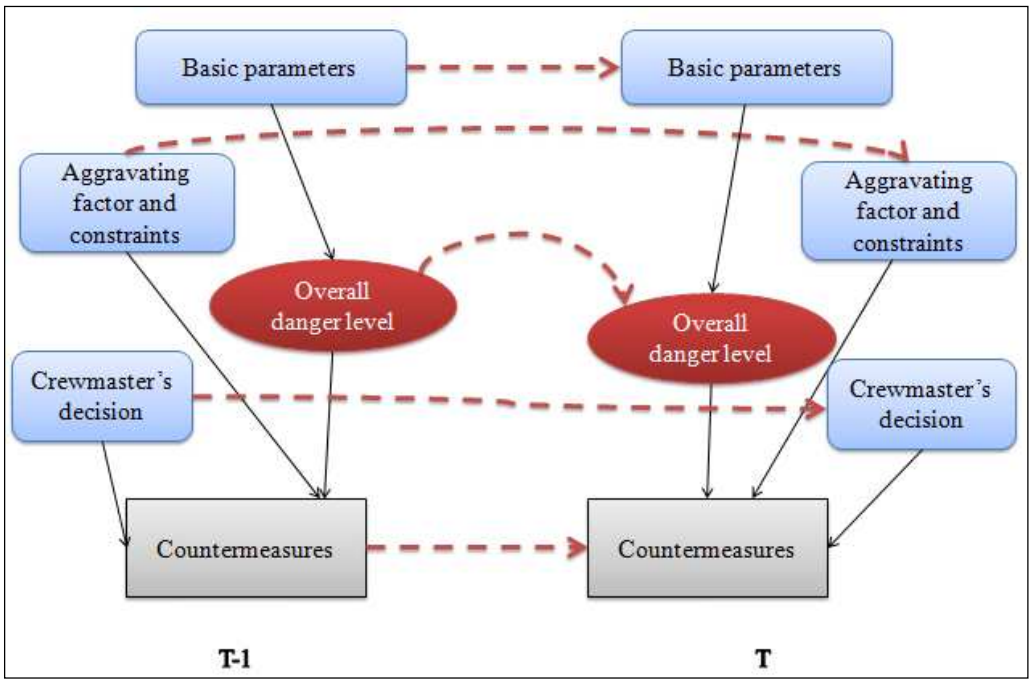


Figure 5-8 : Structure of the dynamic Bayesian network

Learning the structure of the dynamic Bayesian network highlights two principles:

- Links between intra-slice arcs are arcs that contain a single slice; these connections can be identified in the static Bayesian network.
- Links between inter-slices arcs are arcs that link two time slices T−1 and T. They represent arcs at the time of the variables were selected; for each node in slice T, it is necessary to identify its parents in the slice T−1.

In our prototype, the number of time series varies from one attack to another. We cannot therefore know in advance the number of slices that must be processed for each attack. The prototype develops and learns as the analysis of the attack develops. In the various scenarios we tested, conditional probabilities were calculated and improved on the basis of the experimental data. To meet the requirements of a dynamic Bayesian network, the network checks: first, that the structure is time-invariant at every time step, and secondly, that each arc of time extends from time slice T−1 to time slice T. Finally we assume that the variables in each slice are linked in the same way.

6. Contributions and limitations of the model

The example below (Figure 5-9) shows the results at time T−1 related to the insertion of attack parameters against a floating production, storage and offloading platform

(FPSO) by an unknown ship. The danger level of the situation is calculated from two pieces of information and is equal to 2. In this case, the prototype recommends informing the crewmaster, requesting the intervention of the patrol vessel, sending alerts by telephone and putting sound cannons on standby. Processing continues as the attack develops and the basic parameters are improved by calculating the distance between the target and the ship, the type of ship and its classification as “hostile”. These parameters increase the danger level and lead to response planning that includes new countermeasures which are appropriate to the developing situation.

However, unlike the static network, the dynamic Bayesian network disables countermeasures that were initiated earlier in the attack, which are no longer appropriate to the new level of danger. The prototype’s interface provides a dashboard that shows the progress of the attack in both time slices, which makes it easy to compare parameters in the two situations and provides a complete overview of the evolution of the attack over time.

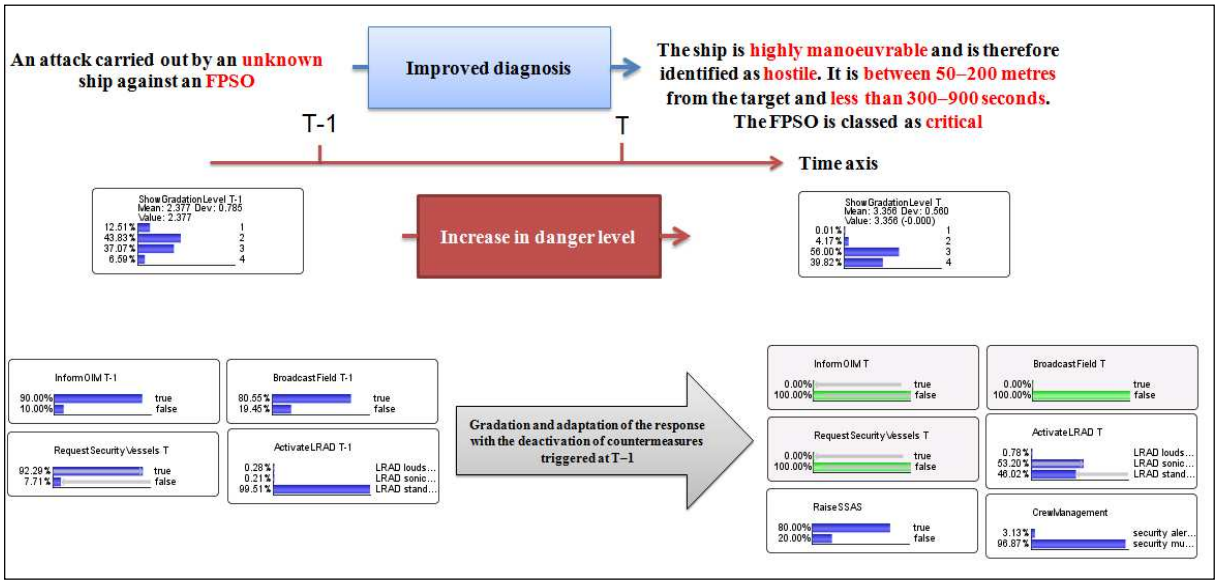


Figure 5-9 : Results of the planning for two time slices (T−1 and T) during an attack against an FPSO

The design of our dynamic Bayesian network also includes the need for operator intervention. Figure 5-10 shows how the decisions of the crewmaster can be taken into account. These decisions may exacerbate or reduce the danger level of the situation. This feature means that the system can be made semi-automatic depending on whether a crewmaster is present, their professional experience and the situation. Consequently, the operator becomes an active actor in the decisions that are made. The operator can also

assign probabilities to countermeasures triggered by the system and/ or decide that they are 100% manual; this feature significantly improves the diagnosis of the situation.

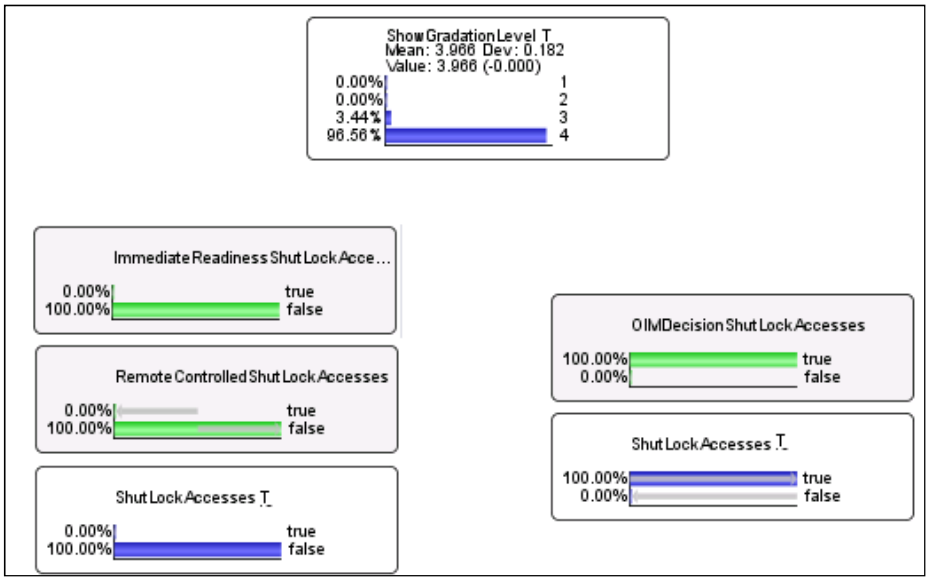


Figure 5-10 : Results of manual intervention by the crew on the probability of the node "ShutLockAccesses"

The example above shows that despite the extremely high danger level, access to the platform cannot be blocked due to functional constraints related to a failure of a countermeasure. Such a failure may endanger many lives and threaten the entire production unit. The addition of a manual intervention feature into the dynamic Bayesian network means that the countermeasure can be made functional and improves the tool's performance. On the one hand the dynamic Bayesian network offers the advantages of a static planning system; on the other it can account for the dynamic development of an emergency through the identification of effective countermeasures that are appropriate to a complex, changing environment.

7. Conclusion

Both static and dynamic Bayesian networks are excellent tools for modelling uncertainty. This is due to their clear graphic representation and the associated conditional probability laws. The particular value of dynamic Bayesian networks is that they are able to integrate a temporal dimension. This makes it possible to interpret results both qualitatively and dynamically through the analysis of the interdependencies between variables at various time slices via links between nodes in earlier graphical models.

This article presents an approach to the design of a system for response planning to pirate attacks against oil fields, based on a static Bayesian network. The limitations of the static network led us to study the contribution of so-called dynamic Bayesian networks. This type of network can take into account the development of situations through incremental processing of the data collected. Consequently, we designed a prototype system that improves the decision-making capabilities oil field operators in the face of a pirate attack. The prototype enables response planning at each moment of the progress of an attack.

References

Bouissou M. and Bourreau B. (2012). Revue des applications des réseaux bayésiens dynamiques en analyse des risques, 18ème Congrès de Maîtrise des Risques et Sûreté de Fonctionnement, pp. 16–18, October 2012.

Cowell R.G., Dawid P., Lauritzen S.L. and Spiegelhalter D.J. (1999). Probabilistic Networks and Expert Systems, Series Information Science and Statistics, XII, ISBN 978-0-387-98767-5, 323 p.

Dabrowski J.J. and Pieter de Villiers J. (2013). Maritime Piracy Situation Modelling with Dynamic Bayesian Networks. Papers submitted to Information Fusion, July 22 2013.

Darwiche A. (2000). A differential approach to inference in Bayesian networks. Proceedings of Uncertainty in Artificial Intelligence, pp. 123–132.

Darwiche A. (2009). Modeling and Reasoning with Bayesian Networks, ISBN 9780521884389, April 2009.

Efron, B. (2010). Large scale inference: Empirical Bayes methods for estimation, testing, and prediction. Cambridge University Press.

François O. (2006). De l'identification de structure de réseaux bayésiens à la reconnaissance des formes à partir d'informations complètes ou incomplètes. Institut national des sciences appliquées de Rouen, 28 November 2006.

Friedman N and Goldszmidt M. (1998). Learning Bayesian Networks with Local Structure. Learning in graphical models, NATO ASI Series, Volume 89, pp. 421-459.

Giraud M. A, Alhadef B, Guarnieri F, Napoli A, Bottala Gambetta M, Chaumartin D, Philips M, Morel M, Imbert C, Itcia E, Bonacci D,and Michel P. (2011). SARGOS: Securing Offshore Infrastructures Through a Global Alert and Graded Response, System Workshop MAST Europe, pp. 27–29, 27 June 2011.

Heckerman D., Meek C. and Cooper G. (1997). A Bayesian Approach to Causal Discovery. technical report, MSR-TR-97-05, February 1997.

Heckerman D. (1999). A tutorial on learning with Bayesian network, M.I Jordan, learning in graphical models, Kluwer Academic Publishers, Boston, pp. 301–351.

Jordan M.I. (1998). Learning in Graphical Models. The Netherlands: Kluwer Academic Publishers.

Kashubsky M. (2008). Offshore energy force majeure: Nigeria's local problem with global consequences. Maritime studies, May–June 2008.

Langseth H. and Bangso O. (2001). Parameter learning in object-oriented Bayesian networks, Annals of Mathematics and Artificial Intelligence, 32, pp. 221–243.

Little R.J. (2006). Calibrated Bayes : A bayes/ Frequentist roadmap. The American Statistician, volume 60, issue 3, pp. 213-223.

Meganck S., Laray P. and Manderick B. (2006). Learning causal Bayesian Networks from observations and experiments: A decision theoretic approach. Modeling decisions for artificial intelligence, lecture notes in computer science, volume 3885, pp. 58-69.

Morel M., Gleizes M.P., Napoli A., Littaye A., Bazin V., Alhadef B., Scapel C., Leroy B., Lebrevelec J. and Dejardin D. (2007). ScanMaris: an Adaptive and Integrative Approach for Wide Maritime Zone Surveillance, Cognitive Systems with Interactive Sensors.

Mukundan P. (2003). Piracy and Armed robbery against ship today. WMU journal Of Maritime Affairs, Volume 3, Issue 2, pp. 167–180, October 2003.

Naïm P., Wuillemin P.H., Leray P., Pourret O. and Becker A. (2004). Réseaux Bayésiens, Eyrolles, ISBN, 2-212-11137-1.

Neapolitan R.E. (2012). Probabilistic Reasoning In Expert Systems: Theory and Algorithms. ISBN 1477452540 9781477452547.

Nielsen T.D. and Verner J.F. (2007). Bayesian Networks and Decisions Graphs. Series Information Science and Statistics, 2nd edition, XVI, ISBN 978-0-387-68282-2, 447 p.

Nincic D.J. (2009). Maritime Security as Energy Security: Current Threats and Challenges. In Luft, G., and Konin, A., (eds). Energy Security: Challenges for the 21st Century. Washington DC: Greenwood Publishing in collaboration with the Institute for the Analysis of Global Security (IAGS).

Onuoha F. (2010). Sea piracy and maritime security in the Horn of Africa : The Somali coast and Gulf Of Aden in perspective. African Security Review, Volume 18, Issue 3, pp. 31–44, 22 July 2010.

Pearl J. (2000). Causality: Models, Reasoning and Inference. Cambridge, England: Cambridge University Press, ISBN, 0-521-77362-8.

Reason J. (1990). Human Error, Cambridge University Press, 320p.

Ren J., Jenkinson I., Wang J., Xu D.L. and Yang J.B. (2008). A methodology to model causal relationships on offshore safety assessment focusing on human and organizational factors, Journal of Safety Research 39, pp. 87–100.

Trucco P., Cagno E., Ruggeri F. and Grande O. (2008). A Bayesian Belief Network modelling of organizational factors in risk analysis: A case study in maritime transportation. Reliability Engineering and System Safety, pp. 823–834.

Chapitre 6 : Une approche bayésienne pour le management du risque de piraterie maritime à l'encontre des infrastructures pétrolières en mer

6.1 Introduction

Le pirate des temps modernes n'a plus de perroquet sur l'épaule et encore moins de drapeau noir à la tête de mort. Terminé les gallons chargés d'or, les cibles sont désormais des tankers et des plateformes en mer gorgées d'or noir. Autres temps, autres technologies, la réponse à la menace fait désormais appel à l'intelligence artificielle et aux réseaux bayésiens.

Les attaques de pirates à l'encontre des plateformes pétrolières en mer se multiplient. Afin de réduire la vulnérabilité de ces infrastructures critiques hautement stratégiques pour l'approvisionnement énergétique, les exploitants étudient et évaluent l'apport de nouvelles technologies de l'information et de la communication. Parmi elles, celles de l'intelligence artificielle et plus particulièrement les réseaux bayésiens offrent des potentiels à explorer.

6.2 Le contexte

6.2.1 Attaques de plateformes pétrolières, une réalité

Plus de sept mille plateformes pétrolières sont réparties à travers le monde. Installations de haute technologie, elles regroupent un ensemble d'équipements pour extraire, traiter et stocker provisoirement le pétrole et des navires chargés de transporter les hydrocarbures entre lieux de production et de consommation [Bouejla et al., WISG, 2012].

La piraterie maritime moderne représente sans conteste un risque majeur pour la sécurisation des sites de production énergétique et du transport maritime pétrolier.

Force est de constater que les moyens actuels de surveillance présentent des faiblesses majeures en matière de détection d'une menace et surtout de procédure de défense à mettre en œuvre face à l'agression. Il convient donc de disposer d'un dispositif efficace et efficient, garantissant la sécurité de l'ensemble des installations et parties

prenantes (exploitants, sous-traitants…) impliquées dans l'exploitation des champs pétroliers [Bouejla et al., Lambda mu 18, 2012].

Quelques exemples spectaculaires et parfois dramatiques illustrent le phénomène de piraterie :

- Le 15 janvier 2006, l'attaque d'une installation de Shell dégénère en incendie, au cours duquel 17 personnes périssent ;
- Le 19 avril 2007, un navire de sécurité, patrouillant dans un champ pétrolier, est attaqué et dépouillé de son propre armement ;
- Le 14 septembre 2008, deux plateformes de Shell et Chevron sont attaquées simultanément.

Le retour d'expérience de ces événements met en lumière l'ampleur des dommages (humains, matériels et économiques). Il souligne aussi les formes d'actions criminelles et les stratégies déployées par les pirates : la surprise, l'extrême mobilité, la rapidité de l'action, le petit nombre d'assaillants et des moyens armés conséquents [Chaze et al., *Radio Science Bulletin*, 2013].

6.2.2 Une protection peu efficace et forcément à améliorer

D'autre part, les autorités militaires considèrent qu'elles sont dans l'impossibilité de protéger l'ensemble de la flotte marchande mondiale. Les plateformes pétrolières n'échappent pas à ce constat. Le Bureau maritime international (BMI) a donc émis des recommandations à destination des armateurs et des équipages afin de garantir la sécurité des personnes, des biens et des équipements. Il n'est pas envisagé d'armer les navires et les plateformes pétrolières. Il s'agit d'éviter des affrontements violents avec des pirates souvent surarmés (fusils automatiques, grenades, lance-roquettes…). Les pirates semblent privilégier la prise d'otages et la demande de rançon. Cela conduit à espérer de leur part un traitement convenable des otages.

Les deux modes d'action dont disposent les navires marchands (éviter les pirates en modifiant les routes maritimes et/ou accroître la sécurité du navire) qu'il s'avère impossible de mettre en œuvre dans le cas desplateformes pétrolières, puisqu'elles sont ancrées. La détection et l'alerte restent donc essentielles.

Malgré les recommandations du BMI, certains armateurs et exploitants ont décidé de faire appel à des entreprises de sécurité. Ils ont donc recours à des moyens non létaux afin de repousser les attaques. En novembre 2008 dans le golfe d'Aden, une équipe de sécurité a mis en échec des pirates lourdement armés en ayant recours pendant 40 minutes à un canon à eau combiné à un dispositif émettant un bruit assourdissant.

Quant aux dispositifs utilisés pour contrer une attaque, ils sont souvent inappropriés ou mal employés (jet d'eau, canons sonores par exemple) [Bouejla et al., INFORSID, 2012].

Concernant la réponse face à une menace, les plateformes pétrolières victimes d'une attaque peuvent émettre des messages d'alerte aux unités de sécurité déployées dans la même zone mais cette diffusion est géographiquement très restreinte. De plus, même si le navire de sûreté et de sécurité est prévenu, son intervention reste d'autant plus incertaine qu'il se trouve éloigné du lieu de l'attaque.

6.2.3 L'intelligence artificielle et les réseaux bayésiens à la rescousse

L'utilisation pratique d'un réseau bayésien peut être envisagée au même titre que celle d'autres modèles : réseau de neurones, système expert, arbre de décision, modèle d'analyse de données (régression linéaire), arbre de défaillances, modèle logique. Naturellement, le choix de la méthode fait intervenir différents critères, comme la facilité, le coût et le délai de mise en œuvre d'une solution. En dehors de toute considération théorique, il est intéressant de disposer d'un modèle effectuant le lien entre les observations et la réalité pour un objectif précis, même lorsque les observations sont incomplètes et/ou imprécises [Bouejla et al., JFRB, 2012].

L piraterie maritime a conduit à rassembler une immense masse d'informations, résultant des enregistrements des attaques de piraterie survenues depuis des années. Face à cette profusion de données, l'enjeu est d'extraire de la connaissance. Il est donc intéressant de retrouver les relations pertinentes entre les variables ou des groupes de variables. L'utilisation des réseaux bayésiens permet dans ce cas d'obtenir une représentation compacte de ces ensembles de dépendances grâce à la notion de séparation et des tables de probabilités conditionnelles.

Les réseaux bayésiens permettent donc de transformer en modèle interprétable la connaissance contenue dans les enregistrements des attaques de piraterie.

D'autre part, avec l'aide des experts maritimes qui connaissent parfaitement les variables et les contraintes d'un champ pétrolier et du milieu maritime, il est possible de construire un modèle probabiliste qui ne modélise pas le mode de raisonnement de l'expert mais la connaissance qualitative que l'expert possède des paramètres influençant le système. Un tel modèle n'est donc pas un système expert mais un système avec des raisonnements probabilistes [Chaze et al., SOSE, 2012].

De plus, les réseaux bayésiens sont plus facilement adaptés et mis à jour en fonction du contexte que les systèmes à base de règles. Il est donc plus simple et rapide de créer des modèles graphiques qui, très intuitifs, facilitent la communication avec les experts [François, 2006].

Les réseaux bayésiens sont aussi capables de gérer l'incertain et l'imprécis et surtout de représenter des relations de cause à effet. De fait, ils sont incontournables face à un problème sujet à l'incertain comme la piraterie maritime.

Notre recherche a principalement pour ambition d'améliorer la phase d'alerte et de mise en sécurité de l'installation pétrolière face à une menace avérée. A ce niveau, il existe de fortes contraintes inhérentes à la problématique abordée. D'une part, on observe une première difficulté propre à l'exploitation du grand nombre de paramètres relatifs à une attaque. En effet, il existe en entrée et en sortie du système des paramètres liés à la fois à la cible (la plateforme) mise en danger (son type, sa criticité, sa vulnérabilité, les outils de sécurité disponibles à bord, etc.), à la menace (le type du navire des assaillants, la vitesse, leur niveau d'armement, etc.) et à l'environnement (la période de la journée, la visibilité, l'état de la mer, etc.). D'autre part, ces paramètres peuvent présenter des interactions. Par exemple, la pertinence de la demande d'intervention du navire de sécurité dépendra notamment du temps nécessaire pour qu'il rejoigne l'installation attaquée, du niveau d'armement et de la vitesse de la menace. La seconde contrainte réside donc dans la gestion de ces nombreuses relations de dépendances entre les différentes variables du système [Chaze et al., ITEMS, 2012].

Une contrainte supplémentaire doit être prise en compte : l'incertitude des informations relatives à une menace. Générer un rapport d'alerte qui contient des

informations résultant d'une part de la fusion des données issues des différents instruments de détection dont le radar FMCW[30] (type du navire détecté, nombre d'occupants, armement éventuel, etc.), et d'autre part de calculs mathématiques à partir des variables dynamiques (distance entre la cible et les attaquants, temps disponible avant que ces derniers soient à bord de la plateforme, etc.) conduit forcément à se questionner sur la gestion des erreurs et des fausses alertes. Malgré les performances croissantes de ce type de radar, ces informations revêtent un niveau d'incertitude qui augmente notamment avec l'éloignement de la menace, l'état de la mer, etc.

Les contraintes précédemment définies invitent donc à concevoir et développer un système d'aide à la décision s'appuyant sur la théorie des graphes, celle-ci permettant de traduire et exploiter au travers d'un graphe un grand nombre de variables, leurs relations de dépendance, leurs incidences, etc.

La prise en compte de l'incertitude inhérente aux données met l'accent sur la nécessité de mobiliser une solution s'appuyant sur la théorie des probabilités et les calculs probabilistes.

Un modèle et un outil d'élaboration automatique de plans de réaction adaptés à la nature de l'intrusion détectée, fondés sur les réseaux bayésiens, sont donc proposés.

6.3 Conception d'un réseau bayésien statique

La principale idée adoptée pour la construction du réseau bayésien statique de planification des réponses contre une menace de piraterie consiste à coupler les connaissances quantitatives issues de la base de données « Piraterie et vol à mains armées » de l'Organisation maritime internationale (OMI) et des connaissances qualitatives acquises auprès des experts du domaine maritime afin d'affiner les résultats et d'ajouter des contre-mesures de riposte.

6.3.1 Description du réseau bayésien

La figure 6-1 illustre le réseau bayésien construit à partir de la base de données. Certaines informations comme la longitude, la latitude, le nom du bien attaqué, etc. n'ont

[30] Frequency Modulated Continuous Wave. Radar à émission de fréquence modulée continue

pas été retenues. Ce choix est dû au fait que ces champs ne sont pas mentionnés pour toutes les attaques [Bouejla et al., Risk Analysis, 2012].

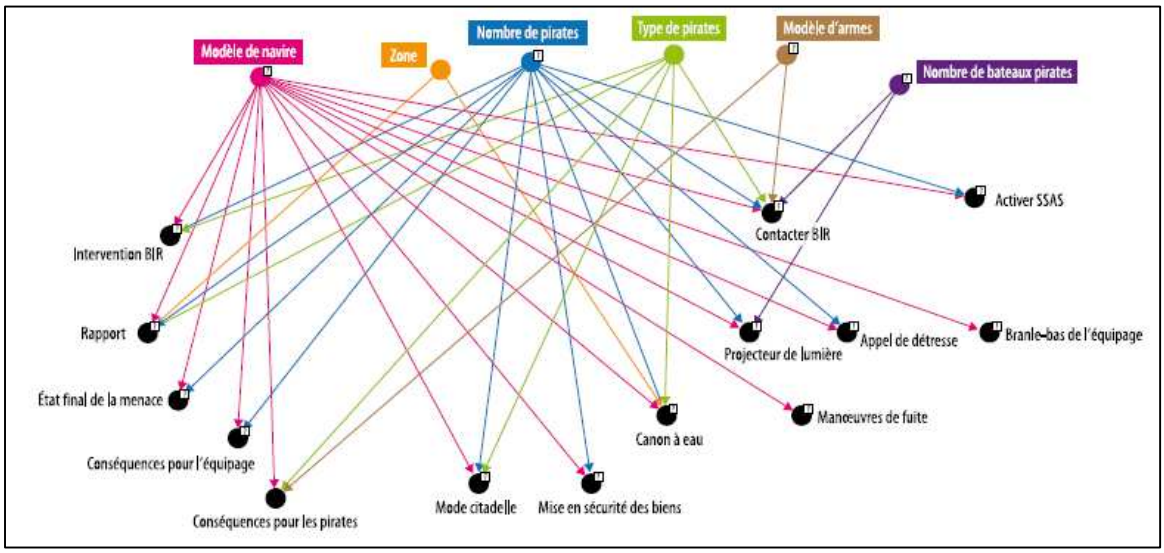


Figure 6-1 : Réseau Bayésien fondé sur les données OMI

Le réseau contient une vingtaine de nœuds relatifs notamment au type du navire attaqué, à la position de l'attaque, au type d'armement des pirates, leurs nombres, etc. ainsi que les relations entre ces variables qui ont été identifiées par un traitement d'apprentissage automatique.

Une analyse statistique classique de ces enregistrements livre une première série d'informations, notamment : la plupart des navires attaqués sont des vraquiers ou des navires-citernes ; 48 % des attaques se déroulent dans les eaux internationales, en raison de l'absence de contrôles de sécurité. Les pirates profitent aussi souvent de leurs nombre : 68 % des attaques sont organisées par des équipes de pirates composées de plus de 5 personnes.

Grâce à ce réseau bayésien, une vision très claire sur la tactique des pirates, la nature de l'armement et surtout le nombre des personnes impliquées est désormais disponible. Du fait de leurs connaissances du domaine maritime, les experts ont pu ensuite transposer ce premier réseau et le spécifier à la problématique des plateformes pétrolières.

La figure 6-2 illustre le réseau bayésien de planification des réactions contre une menace. Le principe de ce réseau est le suivant : lors de la détection d'une piste radar qui circule dans une zone proche du champ pétrolier, un ensemble de variables est déterminé

et calculé afin de l'identifier et d'évaluer sa potentielle dangerosité [Bouejla et al., *Safety Science*, 2014].

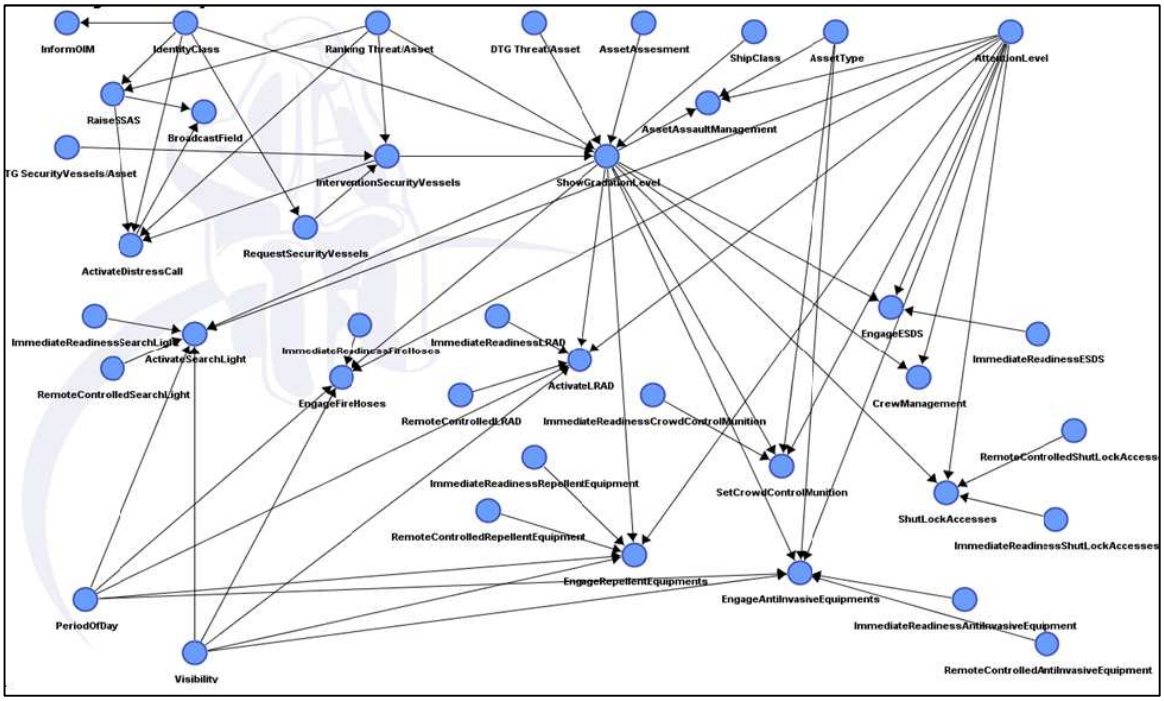


Figure 6-2 : Le réseau bayésien de planification de la réaction contre une menace

Parmi ces informations, citons par exemple la vitesse de la piste, la visibilité, la période de la journée, la longitude et la latitude de la piste détectée, etc. A partir de ces données, la distance entre la cible et la piste attaquante ainsi que le temps théorique d'intervention du navire de sûreté sont calculés.

Ces informations sont enregistrées dans un rapport d'alerte avec un identifiant unique pour chaque piste détectée. Le rapport n'est généré que lorsque la menace est identifiée comme suspecte ou hostile.

L'architecture fondamentale du réseau de planification de la réaction est constituée de cinq modules et quatre sous-modules (figure 6-3).

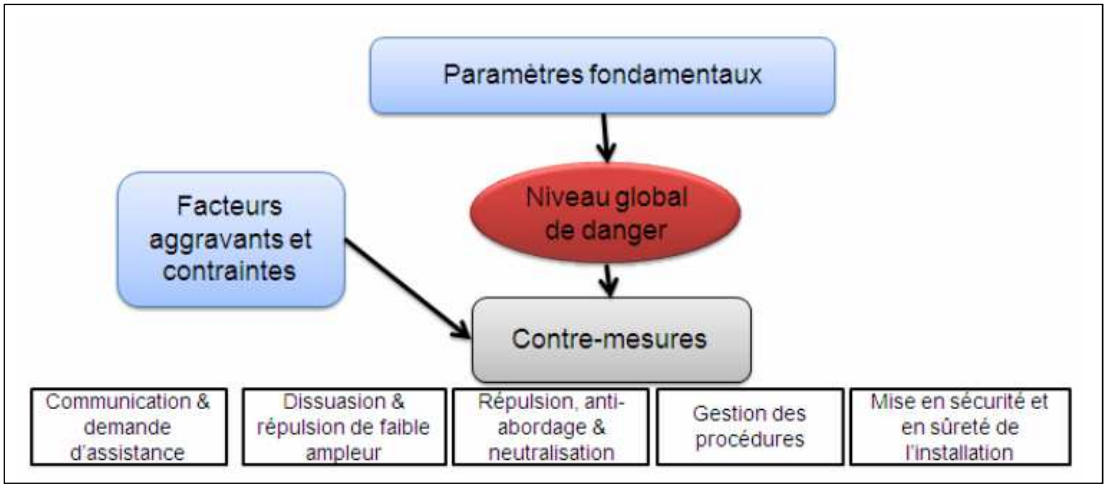


Figure 6-3 : Architecture global du réseau bayésien statique

Les différents paramètres du modèle ont été regroupés dans des « familles » et sont listés et détaillés dans le tableau 6-1.

Intitulé de la famille	**Description**	**Exemples de paramètres**
Paramètres fondamentaux	Ce sont des données physiques statiques ou dynamiques qui caractérisent la menace et la cible. Elles sont directement issues, ou déduites de calculs intermédiaires, du rapport d'alerte, produit par le module de détection du système.	Parmi ces paramètres, l'identité de la menace « *Identity Class* » suspecte ou hostile, la distance entre la menace et la cible « *DTG Threat/Asset* », la criticité de la cible « *Asset Assesment* », etc.
Niveau global de danger de la situation	Il définit la dangerosité globale de la situation.	Le nœud « *Show Gradation Level* » est la formalisation de ce module. Le système de gradation s'échelonne de 1 pour le moindre risque à 4 pour le risque maximal.
Facteurs aggravants et contraintes	Ce sont des éléments internes et externes au système.	Ils représentent l'environnement : la visibilité « *Visibility* » et la période de la journée « *PeriodOfDay* ». Les contraintes techniques sont directement liées à l'utilisation des contre-mesures comme la disponibilité « *ImmediateReadiness* » ou le contrôle à distance « *RemoteControlled* ».
Communication et demande d'assistance	La communication interne à la cible permet d'avertir tous les personnels concernés alors que la communication externe permet à différentes échelles d'avertir les différents acteurs concernés sur les mesures de sûreté en lien avec la survie en mer.	Exemples : informer le maître de l'équipage « *Inform OIM* », demander l'intervention du navire de sûreté « *Request Security Vessels* », mettre en œuvre the Ship Security Alert System « *Raise SSAS* », etc.).
Contre-mesures	Ce sont l'ensemble des moyens de défense mis en œuvre lorsque la cible est attaquée pour se protéger d'une menace identifiée. Ces contre-mesures sont partagées en quatre sous-	Dissuasion et répulsion de faible ampleur : Il s'agit de faire savoir aux attaquants que la cible connaît ses intentions. Exemple : Activer les lances à incendie ou les canons sonores « *Activate LRAD* » (Long-

	modules.	Rang Acoustic Device).
		Répulsion, anti-abordage et neutralisation : Ce sont les contre-mesures actives avec impact fort et dont la fonction principale est au moins l'atténuation si ce n'est la neutralisation des attaquants. Exemple : « *Set CrowControl Munition* » son rôle est de retarder la progression des attaquants.
		Gestion des procédures : Le nœud « Crew Mangement » propose pour chaque cas de sonner le branle-bas équipage de l'infrastructure et le nœud « Asset Assault Management » qui permet dans chaque cas une gestion de la cible potentielle en termes de mise en sécurité et sûreté.
		Mise en sécurité et en sûreté de l'installation : concerne le contrôle de l'outil de production afin de le stopper en toute sécurité ou l'interdiction d'accéder aux locaux sensibles.

Table 6-1 : Description détaillée des différents modules du réseau bayésien statique

Les contre-mesures gérées par le prototype s'articulent en un ensemble de contre-mesures d'ampleur croissante permettant de graduer la réponse face à l'agression. Ceci permet de s'adapter à la nature et à l'évolution de la menace. Un réseau de communication interne et externe permettant la diffusion de l'alerte, la coordination de la réponse et la demande d'assistance est aussi activé.

Dans le réseau bayésien conçu, chaque module ou sous-module est composé d'un ou plusieurs nœuds qui reçoivent et/ou émettent des relations de causalité vers d'autres nœuds. Chaque nœud est composé d'une matrice de probabilités conditionnelles calculées en tenant compte des différentes influences avec les autres nœuds et de la réalité afférente que lui-même présente. Par exemple, la distribution de probabilité d'activation des projecteurs lumineux « Activate Search Light » est directement soumise à des interactions avec la visibilité, la période de la journée et les contraintes techniques comme la disponibilité et le contrôle à distance des contre-mesures.

6.3.2 Discussion des apports et des limites du modèle conçu

Le réseau bayésien proposé permet la formulation et le déclenchement d'un ensemble de contre-mesures en situation d'urgence. A chaque alerte, le réseau détermine un ensemble de réactions à activer selon les paramètres fondamentaux de l'attaque (le type du navire pirate, la vulnérabilité de la cible à protéger, la distance entre la cible et le navire pirate, etc.).

Afin de déterminer les contre-mesures et les modalités qui seront déclenchées, une échelle de probabilité a été utilisée. Les résultats des contre-mesures varient selon les situations d'où la nécessité de fixer un seuil d'activation des dernières dont la réponse est la plus pertinente à un instant T donné. Il a été décidé que seules les contre-mesures dont une des modalités obtient une probabilité strictement supérieure à 70% seront préconisées et déclenchées. Ce seuil a été choisi par les experts maritimes.

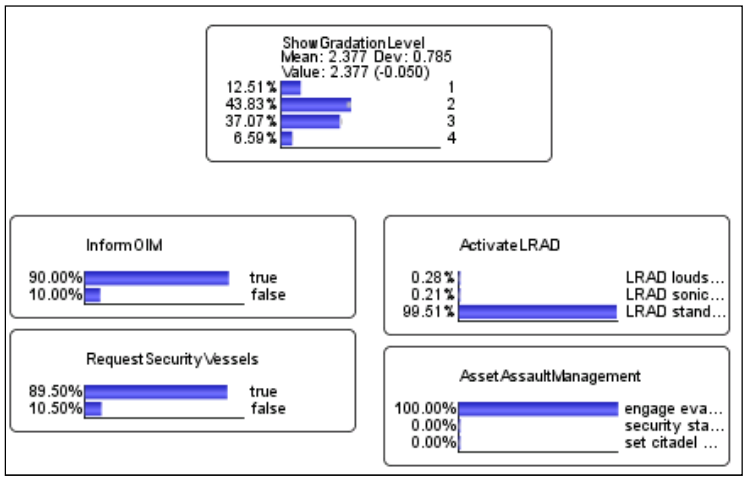


Figure 6-4 : Planification de réponse face à une attaque contre un Crewboat (première planification, T)

L'exemple ci-dessus (figure 6-4) présente les résultats liés à l'insertion des paramètres d'une attaque d'une vedette rapide servant au transport de personnel ou de petits colis entre les différentes installations et/ou la terre (Crewboat) par un navire inconnu. Le niveau de danger de la situation est égal à 2 avec un pourcentage supérieur à 43 %. Dans ce cas les contre-mesures à appliquer sont :

- Informer le maître de l'équipage
- Demander l'intervention du navire de sûreté et de sécurité
- Mettre les canons sonores en stand-by

- Alerter l’ensemble de l’équipage

La planification est adaptée au niveau de dangerosité de la situation et change selon l’actualisation des paramètres de la menace (le navire inconnu) et de la cible (la vedette rapide). D’autres paramètres à l’attaque peuvent être ajoutés, comme : un ranking[31] inférieur à 300 secondes, une distance inférieure à 50 mètres, des pirates qui utilisent un navire ou une embarcation disposant de fortes capacités de manœuvrabilité (c'est-à-dire d’un taux de giration et d’une vitesse de pointe élevée ainsi qu’une accélération importante lui permettant des évolutions brusques sur le plan d’eau) et qui possèdent des armes à feu. La vulnérabilité de la cible est définie comme « majeure ». Dès lors, le niveau de danger est égal à 3 et la probabilité des contre-mesures qui a été appliquée dans la première planification a augmenté (Figure 6-5).

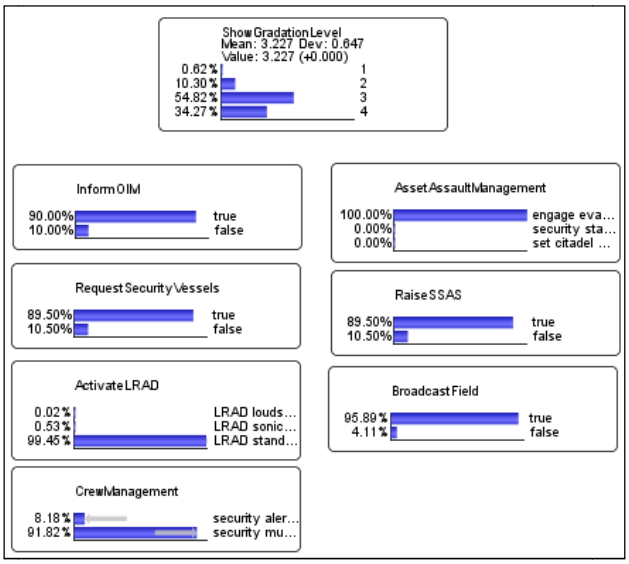


Figure 6-5 : Planification de réponse face à une attaque contre un Crewboat (deuxième planification, T+1)

Les nouvelles contre-mesures à appliquer sont désormais :

- Engager des manœuvres évasives
- Déclencher the Ship Security Alert System SSAS
- Proposer à l’opérateur d’effectuer une diffusion large par phonie (VHF 16) ou sur un canal déterminé l’information d’une attaque pour avertir toutes les autres cibles situées à proximité.

[31] Le "*Ranking Threat Asset*" est un temps calculé qui correspond au temps nécessaire à la menace pour parcourir la distance restante jusqu’au point le plus proche (même nul) de la cible considérée en prenant en compte l’hypothèse qu’à tout moment, la menace peut changer de cap et venir en radiale constante sur la cible.

Malgré l'adaptabilité, la graduation et l'évolutivité du modèle statique présenté ci-dessus, plusieurs limites pénalisent la performance du processus de prise de décision.

L'évolution dans le temps de l'attaque est considérée comme une nouvelle urgence (un nouvel évènement) à traiter et donc dans ce cas, le prototype proposé ne permet pas de disposer d'un suivi dynamique du traitement de l'attaque depuis sa détection jusqu'à sa mise en échec.

Par ailleurs, les paramètres fondamentaux d'un navire se dirigeant vers une plateforme ou un navire pétrolier peuvent changer d'un instant à l'autre suivant la distance entre les deux objets. Ce changement est influencé par l'amélioration de la détection. Dans ce cas et pour la même attaque, le prototype propose des contre-mesures adaptées à l'évolution des informations détectées et il conserve les contre-mesures déclenchées lors du premier traitement. Dans l'exemple illustré la figure 6-6, les informations fondamentales de l'attaque à l'instant T montrent que la vulnérabilité de la plateforme est critique avec une distance entre la cible et le navire pirate comprise entre 200 et 500 mètres[32] et un « ranking[33] » supérieur à 900 secondes. Le prototype qualifie les pirates d'« hostiles » avec un niveau d'armement inconnu. Le niveau de dangerosité de la situation calculé à partir de ces informations est égal à 2 avec environ 49 % de probabilité. Dans ce cas, le prototype envoie automatiquement une demande d'intervention du navire de sûreté, effectue une diffusion d'alerte large par téléphonie et adresse une alerte au maître d'équipage. A l'instant T + 3, les paramètres de l'attaque changent puisque la distance entre la cible et le navire agresseur devient inférieur à 50 mètres[34] et l'identité des pirates est devenue « suspecte ». Dans ce cas, le niveau de dangerosité de la situation est égal à 3, ce qui engendre l'activation d'autres contre-mesures comme l'activation des manœuvres évasives. Cet exemple souligne un inconvénient majeur du modèle « statique »puisque les contre-mesures activées à l'instant T restent activées jusqu'à l'instant T + 3 (les probabilités sont supérieures à 70 %) alors qu'elles ne sont plus adaptées à l'évolution de la situation. Ceci engendre une utilisation

[32] Les différents seuils et modalités des contre-mesures ont été définis par les experts du domaine maritime et à partir des statistiques des scénarios d'attaques enregistrées dans la base de données de l'organisation maritime internationale.

[33] Le "*Ranking Threat Asset*" est un temps calculé qui correspond au temps nécessaire à la menace pour parcourir la distance restante jusqu'au point le plus proche de la cible considérée en prenant en compte l'hypothèse qu'à tout moment, la menace peut changer de cap et venir en radiale constante sur la cible.

[34] Les paramètres d'une attaque (la distance entre le navire des pirates et la cible à protégée, le ranking, etc.) ont été calculé à partir des données capturés par les caméras de surveillance fixés dans le champ pétrolier.

excessive des contre-mesures pendant toutes les étapes du traitement d'une attaque et rend plus confus le choix des mesures à activer par les membres de l'équipage.

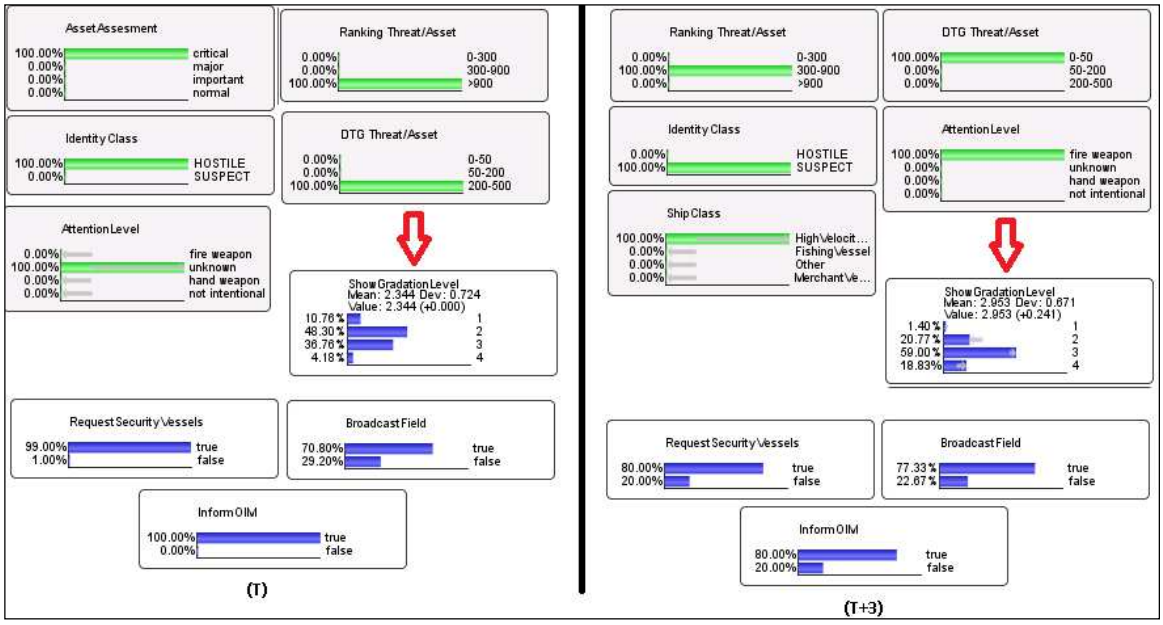


Figure 6-6 : Exemple d'un scénario d'attaque dans deux temps différents

Les contre-mesures ne se déploient pas toutes automatiquement. Leur déclenchement exige parfois l'intervention d'un opérateur. Parmi ces contre-mesures :

- « Engage ESDS » : la mise en sécurité de l'installation industrielle de façon à éviter au maximum que l'outil de production ne soit endommagé ou s'il venait à l'être, que les conséquences en soient le plus limitées possible.
- « FireHorses » : un nœud proposant de mettre en pression le circuit incendie et d'y brancher les lances à incendie, qui peuvent être en premier lieu dissuasives grâce au jet d'eau formé et utilisé en arme de répulsion si les assaillants venaient à se retrouver à portée de « tir » (aux alentours d'une vingtaine de mètres).
- « SetCrowControlMunition » : la fonction principale de ce type d'équipement est de retarder au maximum la progression des assaillants à bord de l'installation pour les fatiguer voire les neutraliser et laisser un répit à l'équipage afin de mieux se barricader ou effectuer d'autres actions de sûreté.

Ces contre-mesures doivent donc être considérées à bon escient. La confusion dans leur usage ne peut être tolérée. Ayant toutes en commun le rapport au temps, le recours à un réseau bayésien dynamique s'avère légitime pour un usage optimal.

Afin de lever les limites citées ci-dessus, la démarche méthodologique a consisté d'une part à améliorer le réseau bayésien statique par l'ajout de nouveaux nœuds et à l'enrichir d'une dimension temporelle par le recours à un réseau bayésien dynamique : des nœuds et des arcs ont ainsi été ajoutés afin de le rendre apte à caractériser une situation évolutive.

6.4 Conception d'un réseau bayésien dynamique

Un réseau bayésien dynamique est une représentation factorisée d'un réseau bayésien dont les nœuds sont indexés par le temps sur une échelle discrète. Comme il est impossible de représenter une structure infinie, on utilise une notation graphique dans laquelle les nœuds sont indexés par des pas de temps génériques et offrant deux types de liens : les liens classiques des réseaux bayésiens statiques et des liens dits temporels qui permettent de définir les tables de probabilités conditionnelles des nœuds en fonction de leurs parents situés à des indices de temps inférieurs [Bouissou et Bourreau, 2012].

6.4.1 Description du réseau bayésien dynamique

L'architecture du réseau bayésien dynamique présentée dans la figure 6-7 est caractérisée par une partie (B_1, B->), où B_1 qui définit l'a priori $P(Z_T)$ et B-> est la tranche temporelle du réseau bayésien par lequel on définit $P(Z_T \backslash Z_{T-1})$ où Z est une variable aléatoire décrit par $Z_t = (U_t, X_t, Y_t)$ pour représenter les nœuds du modèles. Les arcs en pointillés présentent les arcs temporels entre les tranches de temps. Ces arcs vont de gauche à droite et reflètent l'avancement du temps.

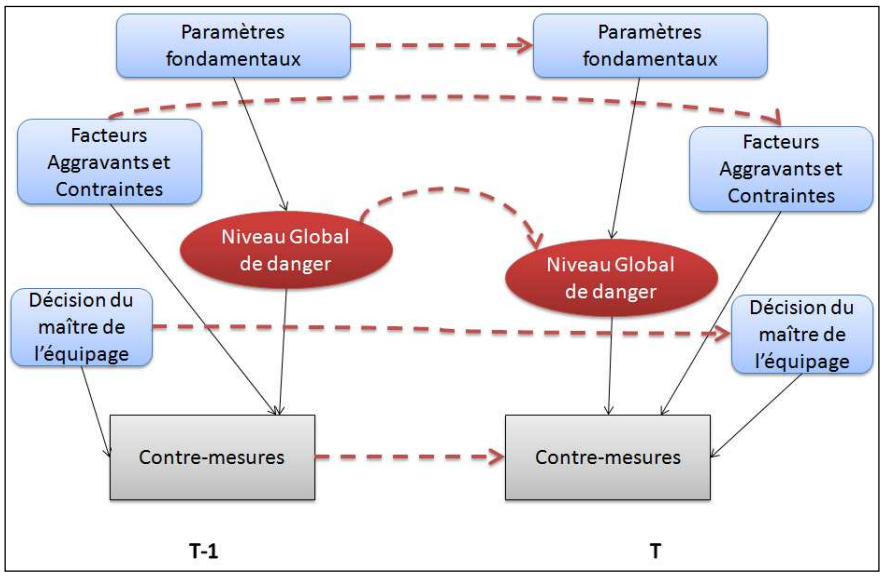


Figure 6-7 : Structure du réseau bayésien dynamique

Nous considérons un processus stochastique dynamique de temps discret, l'index T est donc augmenté d'un pas de temps à chaque nouvelle donnée collectée par le système.

Le réseau bayésien dynamique contient un module « Décision du maître d'équipage ». Ce sont des nœuds permettant de prendre en compte les décisions du maître d'équipage pour les contre-mesures qui demandent une activation manuelle et pour les contre-mesures où l'activation automatique à distance est, le cas échéant, en panne. Ces nœuds sont directement reliés aux contre-mesures par des arcs intra-tranches en utilisant l'apprentissage des paramètres statiques. Chaque nœud de décision est constitué de deux modalités : vrai ou faux.

L'apprentissage de la structure du réseau bayésien dynamique relève de deux principes :

- Des connexions entre les arcs intra-tranches, constituant elles-mêmes des arcs ne contenant qu'une seule tranche, ces connexions étant déterminées dans le réseau bayésien statique existant.
- Des connexions des arcs inter-tranches, constituant des arcs reliant deux tranches de temps $T-1$ et T. Elles représentent les arcs de temps de sélection des variables ; ainsi pour chaque nœud dans la tranche T, il convient de rechercher les parents à partir de la tranche $T-1$.

Dans le cas de notre prototype, le nombre de séries de temps varie d'une attaque à l'autre. On ne peut donc pas connaître à l'avance le nombre de tranches de traitement pour chaque attaque. Le prototype se développe et apprend avec l'analyse de l'évolution de l'état des différentes attaques. Les probabilités conditionnelles sont calculées et améliorées à partir des données expérimentales des différents scénarios testés. Afin de satisfaire les conditions d'un réseau bayésien dynamique, le réseau conçu vérifie : premièrement que la structure est invariante à tout pas de temps (*time-invariant*), deuxièmement que chaque arc de temps est étendu d'une tranche de temps T – 1 vers une tranche temps T. Enfin nous supposons que les variables de chaque tranche sont connectées de la même manière [Bouejla et al., Lambda mu 19, 2014].

6.4.2 Discussion des apports et des limites du modèle conçu

L'exemple ci-dessous (Figure 6-8) présente les résultats dans un temps T – 1 liés à l'insertion des paramètres d'une attaque contre une unité flottante de production, de stockage et de déchargement (FPSO, *flotating production storage and offloading*) par un navire inconnu. Le niveau de danger de la situation est calculé à partir de deux informations détectées égales à 2. Le prototype propose d'informer le maître d'équipage, de demander l'intervention du navire de sûreté, d'envoyer des alertes par téléphonie et de mettre les canons sonores en attente. Le traitement de l'attaque se poursuit et les paramètres fondamentaux ont été améliorés en calculant la distance entre la cible et le navire, le type du navire pirate et sa qualification comme « hostile ». Ces paramètres augmentent le niveau de dangerosité de la situation et permettent la planification d'une réaction avec des nouvelles contre-mesures adaptées à la situation rencontrée.

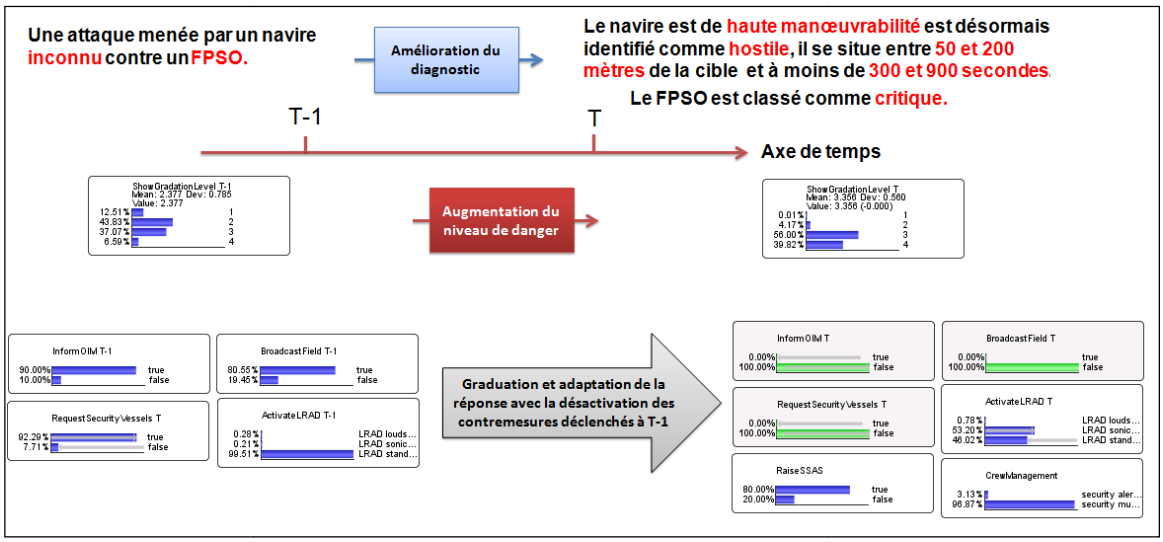


Figure 6-8 : Résultats de la planification dans deux tranches de temps (T – 1 et T) lors d'une attaque contre un FPSO.

Le réseau bayésien dynamique, à l'inverse du réseau statique, désactive les contre-mesures déclenchées lors des précédents traitements de l'attaque et qui ne sont plus adaptées au nouveau niveau de dangerosité. L'interface homme-machine du système permet de présenter un tableau de bord de traitement de l'attaque dans les deux tranches de temps, ce qui facilite la comparaison des paramètres des deux situations et de disposer d'une vision complète de l'évolution de l'attaque dans le temps.

Le réseau bayésien dynamique conçu considère aussi les interventions des opérateurs. La figure 6-9 montre la prise en compte du système de décisions du maître d'équipage. Cette décision peut aggraver ou diminuer la dangerosité de la situation. Cet aspect permet de modifier l'automatisation complète du système et de le rendre partiellement automatique en prenant en compte la présence ou pas du maître d'équipage, son expérience professionnelle du domaine et de la situation. De cette façon l'opérateur n'est plus un acteur passif dans la séquence de décisions. L'opérateur peut aussi attribuer des probabilités aux contre-mesures déclenchées par le système et/ou manuellement à 100 %, cette possibilité participe pleinement à l'amélioration du diagnostic de la situation.

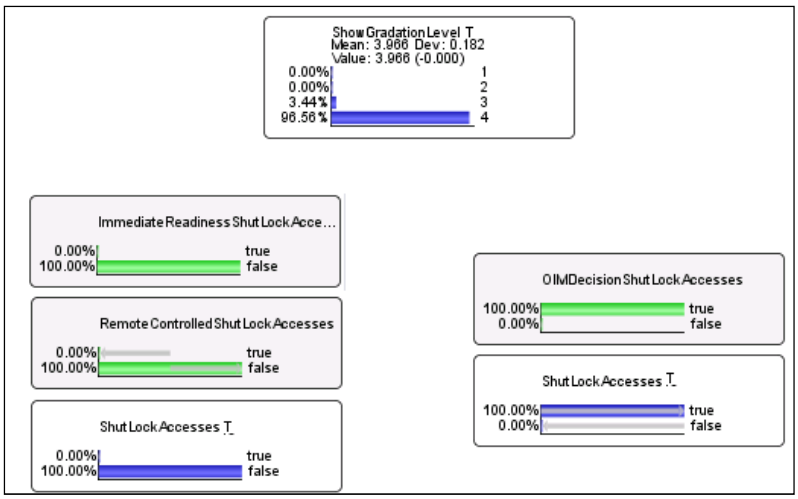


Figure 6-9 : Résultats de la possibilité d'intervention manuelle de l'équipage sur la probabilité du nœud « ShutLockAccesses ».

L'exemple ci-dessous montre que malgré la dangerosité extrême du niveau de la situation, la contre-mesure de verrouillage de l'accès à la plateforme ne peut pas être activée puisque les contraintes fonctionnelles liées à la contre-mesure sont en panne. Cette panne peut mettre en danger la vie de plusieurs personnes et menacer l'unité de production dans son ensemble. L'usage d'un réseau bayésien dynamique, en autorisant l'intervention manuelle, rend cette contre-mesure à nouveau fonctionnelle et renforce ainsi la performance du dispositif. Le réseau bayésien dynamique proposé à ce stade offre d'une part les atouts acquis par le recours à un système de planification statique et permet d'autre part la prise en compte de la dynamique d'évolution d'une situation d'urgence en déterminant des contre-mesures efficaces et adaptées à un contexte complexe et changeant.

6.5 Le couplage entre réseau bayésien statique et réseau bayésien dynamique

Dans cette thèse, nous avons présenté la synthèse d'un travail déjà effectué portant sur la conception d'un système de planification des réactions contre une attaque de piraterie à l'encontre des champs pétroliers basé sur l'usage d'un réseau bayésien statique. Les limites de ce type de réseaux nous ont conduits à étudier les apports des réseaux bayésiens dits dynamiques. Ce type de réseau bayésien permet de considérer des situations évolutives par le traitement incrémental des données collectées. Ainsi, nous

avons pu concevoir un prototype de système permettant à l'exploitant d'un champ pétrolier d'accroître sa capacité de prise de décision face à une attaque de piraterie. Le prototype permet de planifier des réactions et des ripostes pour chaque instant de l'évolution d'une attaque.

Le couplage entre les deux systèmes a permis d'une part de conserver le potentiel de la structure du réseau statique et l'adaptation avec chaque type de menace et d'autre part de disposer d'un rapport de planification séquentielle avec l'intégration de l'intervention humaine en cas de disfonctionnement de l'un des équipements du système, grâce au réseau bayésien dynamique.

Malgré les atouts de ce couplage au niveau des résultats, la structure du réseau bayésien dynamique en rend la manipulation malaisée lorsqu'augmente le nombre des nœuds et des arcs d'indépendance. De plus, l'augmentation du nombre des parents d'un nœud engendre des grandes matrices de probabilités. Lorsque le réseau n'est construit qu'à partir d'une base de données, l'apprentissage automatique rend facile la résolution de ce problème. Dans le cas des connaissances expertes, qui englobe le modèle que nous avons conçu, la détermination des probabilités requiert plusieurs sessions de travail et une phase importante de test et de validation à partir des différents exemples et scénarios d'attaque.

6.6 Conclusion

La problématique de la piraterie maritime à l'encontre des infrastructures pétrolières est complexe. Dans un espace ouvert et soumis à de fortes contraintes environnementales, la difficulté à évaluer une menace potentielle, l'évolutivité constante d'une situation de danger ainsi que la gestion de très nombreux paramètres affaiblissent actuellement l'efficacité de la protection de ces infrastructures.

L'utilisation d'un réseau bayésien pour la planification de la réaction face à une menace est donc un atout majeur puisque le réseau gère les interactions possibles entre les caractéristiques de la menace et de la cible attaquée, l'environnement, la gestion de

l’équipage et des installations et surtout, il s’adapte en temps réel à l’évolution du niveau de danger de la situation.

Les réseaux bayésiens, statiques comme dynamiques, constituent d’excellents outils de modélisation de l’incertain grâce à leur représentation graphique claire et aux lois de probabilités conditionnelles associées. L’intérêt des réseaux bayésiens dynamiques est la prise en compte du temps. Ils permettent l’interprétation de résultats de manière qualitative et dynamique par l’analyse des interdépendances entre les variables de plusieurs tranches de temps opérées par des connexions entre les nœuds de modèles graphiques préalablement générés.

Notre modèle peut être amélioré, car il nécessite des probabilités dont la détermination requiert typiquement de grandes quantités de données ou plusieurs connaissances a priori, dont dépend la fiabilité des résultats. Une des perspectives est d’intégrer des retours d’expériences relatifs aux traitements des attaques réelles contre les champs pétroliers. Le modèle sera ainsi adapté et amélioré de manière itérative.

Conclusion et perspectives

Conclusion

Nous nous sommes intéressés dans cette thèse à la construction d'un système d'aide à la décision en situation de crise. Les méthodes actuelles utilisées en amont de management du risque de piraterie maritime sont majoritairement des méthodes de détection. Les résultats issus de ces méthodes ne sont pas totalement efficaces et dépendent de la présence de plusieurs paramètres (la météo, la distance entre la menace et la cible potentiel, la présence des navires de sécurité et de sûreté, etc.). Dans ce travail de recherche, nous avons proposé une méthode originale d'aide à la planification des réactions contre une menace potentielle à l'encontre des champs pétroliers basée sur les réseaux bayésiens. Cette proposition a permis de générer automatiquement des plans de réponses adaptable et évolutif à chaque type de cible à protéger à partir de l'exploration de données détectées et calculées dans un rapport d'alerte.

La contribution de cette thèse peut être décrite en six points, qui sont :

- **Proposition d'une nouvelle méthodologie de construction d'un système de planification**

La méthodologie proposée dans cette thèse est basée sur les réseaux bayésiens pour acquérir les connaissances en donnant la possibilité de rassembler et de fusionner des connaissances de diverses natures dans un même modèle : retour d'expérience, expertise, observations. La méthodologie permet aussi de représenter graphiquement ces connaissances. Le recours à un réseau bayésien facilite une représentation explicite, intuitive et compréhensible par un ou non spécialiste, ce qui favorise à la fois la validation du modèle, ses évolutions éventuelles et surtout son utilisation (évaluer, prévoir, diagnostiquer, ou optimiser des décisions).

- **Identification d'un outil de conception des réseaux bayésiens permettant l'extraction des connaissances à partir des données brutes et leur couplage à des connaissances expertes**

La recherche a permis de démontrer que les connaissances issues de l'apprentissage automatique des données de la base de l'Organisation maritime internationale sont efficaces et peuvent être utilisées dans le contexte des champs pétroliers. L'idée de

coupler ces résultats avec les connaissances des experts maritimes a permis de concevoir un réseau bayésien d'une part fréquentiste grâce aux données réelles des attaques, d'autre partprobabiliste grâce à l'expertise maritime.

Le logiciel BayesiaLab a présenté un atout majeur pour la facilité de conception du réseau bayésien.

- **Constitution d'un environnement de modélisation d'une attaque contre une plateforme**

Le réseau bayésien est composé de l'ensemble des variables jugées nécessaires et indispensables pour définir une attaque. Les paramètres fondamentaux du réseau permettent de définir les éléments décrivant la cible à protéger et le navire des assaillants.

Ces paramètres permettent aussi de calculer un niveau de danger de la situation qui donne une information efficace sur l'évolution temporelle de la menace.

Plusieurs équipements et contremesures peuvent être présents sur les infrastructures pétrolières. Ces équipements sont létaux ou pas et mis en œuvre selon des contraintes fonctionnelles et environnementales.

Le potentiel des réseaux bayésiens grâce en particulier aux arcs de dépendance a permis de gérer les relations et le fonctionnement de ces équipements en les adaptant à chaque type de menace.

- **Découverte des apports et des limites décrivant des situations à risques**

Le réseau bayésien élaboré permet de proposer des réponses adaptées et graduées à chaque menace détectée. L'établissement de plusieurs scénarios d'attaque a permis de découvrir deux limites du système : d'une part, l'automatisation complète de la plupart des équipements et l'appréhension de l'équipage comme un acteur passif ; d'autre part, l'indépendance entre les plans de planification d'une même attaque et ce, selon des pas de temps différents.

- **Conception d'un réseau bayésien dynamique à partir de la structure du réseau bayésien statique**

Le couplage d'un réseau bayésien dynamique au réseau bayésien statique déjà conçu a permis de profiter des potentiels des deux systèmes. Le réseau statique nous a donné une structure efficace afin de modéliser la planification des contre-mesures. Le réseau dynamique a, de son côté, favorisé l'insertion de la variable temporelle dans le système, ce qui a permis des planifications séquentielles reliées.

La structure du système a été enrichie par des nouveaux nœuds permettant l'intervention humaine en cas de panne des systèmes automatiques de fonctionnement des équipements de contre-attaque.

- **Constat sur le prototype conçu et développé**

Le système global proposé présente un prototype de système innovant, « intelligent » et certainement efficace pour le management du risque de piraterie maritime à l'encontre des plateformes pétrolières. Ce prototype permet la gestion d'une crise avec la prise en compte de l'ensemble des variables d'une menace, du milieu marin et des caractéristiques de la cible à protéger.

En terme opérationnels, les résultats obtenus lors de l'établissement des différents scénarios d'attaque sont satisfaisants. Cependant, force est de constater que la structure globale du réseau bayésien reste de manipulation difficile en raison du nombre important des nœuds et des arcs d'indépendance. De plus, l'augmentation du nombre des parents des nœuds a engendré la création de matrices de probabilités particulièrement volumineuses.

Perspectives de la thèse

Au terme de cette thèse, nous proposons trois perspectives de recherche.

- **En amont du réseau bayésien, concevoir une ontologie du domaine**

A court terme, il serait utile en s'adossant à des travaux conduits au sein de Centre de recherche sur les Risques et les Crises d'évaluer l'apport du concept d'ontologie. L'ontologie est utilisée, depuis plusieurs années, dans l'Ingénierie des connaissances (IC) et l'Intelligence artificielle (IA) pour structurer les concepts d'un domaine. Les concepts sont rassemblés et ces derniers sont considérés comme des briques élémentaires permettant d'exprimer les connaissances du domaine qu'il recouvre [Bachimont, 2006].

Les ontologies sont utiles pour partager des connaissances, créer un consensus, construire des systèmes à base de connaissances. La création d'une ontologie en lien avec la question de la piraterie maritime et, plus globalement, avec toute menace en mer serait donc pertinente.

Une ontologie serait ainsi utile pour décrire les scénarios d'attaque et ainsi mieux connaître l'analyse des comportements à risque de navires en mer. [Vandecasteele et Napoli, 2013] ont proposé un modèle utile à notre travail. Pour ce faire, la méthode demanderait de disposer d'une base de données d'apprentissage où les attaques seraient étiquetées comme menace « à risques » ou « non à risques ». Cette méthode serait ainsi mise en œuvre une fois que les attaques traitées seraient enregistrées dans une base de données. Ce dispositif existe déjà au stade de prototype [Idiri et Napoli, 2014].

- **Convoquer plus largement des connaissances expertes**

Dans le cadre de notre recherche, nous avons eu l'honneur de pouvoir collaborer avec des experts du domaine maritime et de la sécurité maritime. Cette collaboration s'est établie dans le cadre du projet de recherche SARGOS [Giraud et al., 2013]. Elle s'est révélée essentielle pour notre travail. La qualité des expertises mobilisées a permis de crédibiliser notre démarche et de valider pour partie nos résultats. Cette collaboration a été, par essence, limitée dans le temps. Les domaines de questionnement et de fait d'expertise nous apparaissent nombreux. Citons par exemple : le besoin de disposer d'un retour d'expérience détaillé des attaques subies qu'elles aient connu ou pas une issue favorable

pour les pirates ; une meilleure connaissance des stratégies mises en œuvre par les infrastructures pour se défendre d'une agression, et en particulier l'efficacité des ripostes, qu'elles soient létales ou pas ; la possibilité de tester, évaluer et valider les modèles conçus et développés auprès d'un panel d'experts du domaine… Naturellement, la possibilité d'une expérimentation de nos travaux à une grande échelle et en conditions « réalistes » serait un plus indéniable tant dans l'acquisition de connaissance que dans la validation de nos travaux de modélisation.

- **Aller vers un réseau bayésien « spatial »**

A notre connaissance, les modèles prédictifs produits à ce jour à l'aide des réseaux bayésiens n'ont pas intégré directement des règles d'interaction spatiale entre variables. Ainsi, [Dabrowski et al., 2013] présentent le résultat de simulations d'attaque sur des cartes en se fondant sur des données préalablement acquises (2011) dans le golfe d'Aden. [Castaldo et al., 2014] proposent eux aussi une représentation spatialisée d'inférences bayésiennes en ayant recours à une représentation topologique qui permet avantageusement de mettre en évidence des relations de voisinages. [Riviero et al., 2009] décrivent VISAD, un outil interactif pour la détection de comportement anormaux en mer. Le concept de « *visual data mining* » est avancé. Une perspective serait donc de disposer d'une description détaillée des modalités d'interaction spatiale entre de nombreuses variables territoriales, permettant par la suite de jouer sur l'ensemble de ces variables dans la construction des scénarios d'attaque et de défense. Pour qu'un tel modèle puisse voir le jour, il devrait s'appuyer sur une description « simple » de l'espace maritime étudié. Le recours à des polygones serait certainement opportun [Vandecasteele et al., 2014] tout en nécessitant une évaluation approfondie.

Bibliographie

Anifowose B., Damian M.L., Dan van Der H. and Lee C. (2012). Attacks on oil transport pipelines in Nigeria: A quantitative exploration and possible explanation of observed patterns, Applied Geography, Vol. 32 Iss.2, pp. 636‑651, March 2012.

Aleklett K., Hook M., Jakobsson K., Lardelli M., Snowden S. and Soderbergh B. (2010). The pick of the oil age – Analyzing the world oil production reference scenario in world energy outlook 2008. Energy Policy, Volume 38 Issue 3, pp. 1398–1414, March 2010.

Antonucci A. And Zaffalon M. (2008). Decision-theoretic specification of creedal networks : A unified language for uncertain modelling with sets of bayesian networks; international journal of approximate reasoning, volume 49, pp. 345-361.

Bachimont B. (2006). Qu'est-ce qu'une ontologie?. Technolangue.net, 3 juillet 2006. http://www.technolangue.net/imprimer.php3?id_article=280.

Baoping C., Yonghong L., Zengkai L., Xiaojie T., Yanzhen Z. and Renjie J. (2012). Application of BayesianNetworks in Quantitative Risk Assessment of Subsea Blowout Preventer Operations. Society for Risk Analysis, pp. 1-20.

Bayes T. (1763). An essay towards solving a problem in the doctrine of chances. Philosiphical Transactions of the Royal Society, volume 53, pp. 370-418.

Becker A. and Naïm, P. (1999). Les réseaux bayésiens. Modèles graphiques de connaissances. Editions Eyrolles.

BMI. 2011. Study: Piracy Costs World Up to $12 Billion Annually, Bureau International Maritime, 14 juillet 2011. http://www.voanews.com/english/news/africa/Study-Piracy-Costs-World-up-to-12-Billion-Annually-113609239.html.

Bouejla A., Chaze X., Napoli A., Guarnieri F., Eude T. and Alhadef B. (2012). Contribution des réseaux bayésiens à la gestion du risque de piraterie contre les champs pétroliers. Workshop Interdisciplinaire sur la sécurité globale, Université de technologies de Troyes, Janvier 2012.

Bouejla A., Chaze X., Guarnieri F. and Napoli A. (2012). Conception d'un réseau bayésien pour la prévention du risque de piraterie contre les champs pétroliers. Journées francophones sur les réseaux bayésiens, îles Kerkennah, Tunisie, 11 au 13 mai 2012.

Bouejla A., Chaze X., Napoli A. and Guarnieri F. (2012). Application des réseaux bayésiens à la planification de la réponse à une attaque de pirates contre un champ pétrolier. Informatique des organisations et Systèmes d'Information et de Décision, Université Montpellier 2, 29 au 31 mai 2012.

Bouejla A., Chaze X., Guarnieri F. and Napoli A. (2012). Bayesian networks in the management of oil field piracy risk. Risk analysis, International Conference on Risk Analysis and Hazard Mitigation, Wessex institute, Brac, Croatie, 19 au 21 septembre 2012.

Bouejla A., Chaze X., Guarnieri F. and Napoli A. (2012). Apports des réseaux bayésiens pour la sûreté et la mise en sécurité des infrastructures pétrolières offshore. Lambda mu 18, Institut pour la maîtrise des risques, Tours, Octobre 2012.

Bouejla A., Guarnieri F. and Napoli A. (2014). Apports des réseaux bayésiens « dynamiques » à la lutte contre la piraterie maritime. Lambda mu 19, Institut pour la maîtrise des risques, Dijon, Octobre 2014.

Bouejla A., Chaze X., Guarnieri F. and Napoli A. (2014). A Bayesian network to manage risks of maritime piracy against offshore oil fields. Safety Science, Volume 68, pp. 222-230, Elsevier, 31 octobre 2014.

Bouissou M. and Bourreau B. (2012). Revue des applications des réseaux bayésiens dynamiques en analyse des risques, 18ème Congrès de Maîtrise des Risques et Sûreté de Fonctionnement, pp. 16–18, October 2012.

Brown N. (2006). Taking the Fight to the Pirates. Jane's Information Group.

Burnett J.S. (2002). Dangerous Waters: Modern Piracy and Terror on the High Seas. New York: Dutton.

Castaldo F., Palmieri F.A.N., Bastani V., Marcenaro L. and Regazzoni C. (2014). Abnormal vessel behavior detection in port areas based on dynamic bayesian network. 17th IEEE International Conference on Information Fusion, juillet 2014.

Chaze X., Bouejla A., Napoli A., Guarnieri F., Eude T. and Alhadef B. (2012). The contribution of bayesian networks to manage risks of maritime piracy against oil offshore fields. Information technologies for the maritime sectors, Busan, Corée de sud, 15 avril 2012.

Chaze X., Bouejla A., Napoli A. and Guarnieri F. (2012). Integration of a bayesian network for response planning in a maritime piracy risk management system. System of systems engineering, Genoa, juillet 2012.

Chaze X., Bouejla A., Guarnieri F. and Napoli A. (2013). Causal Probabilistic Modeling with Bayesian Networks to Combat the Risk of Piracy against Offshore Oil Platforms. The Radio science Bulletin, Volume 345, Disaster Management special issue, pp. 21-34, June 2013.

Cowell R.G., Dawid P., Lauritzen S.L. and Spiegelhalter D.J. (1999). Probabilistic Networks and Expert Systems, Series Information Science and Statistics, XII, ISBN 978-0-387-98767-5, 323 p.

Dabrowski J.J. and Pieter de Villiers J.(2013). Maritime piracy situation modelling with dynamic Bayesian networks. Information fusion.

Dagum P. And Martin Chavez R. (1993). Approximating probabilistic inference in bayesian belief networks. IEEE transactions on pattern analysis and machine intelligence, volume 15, No 3, pp. 246-256.

D'ambrosio B., Shachter R.D. and Del Favero B.A. (1990). Symbolic probabilistic inference in belief networks. In : AAAI-90, pp. 126-131.

Darwiche A. (2000). A differential approach to inference in Bayesian networks. Proceedings of Uncertainty in Artificial Intelligence, pp. 123–132.

Darwiche A. (2001). Constant-space reasoning in dynamic bayesian networks. International journal of approximate reasoning, volume 26, pp. 161-178.

Darwiche A. (2009). Modeling and Reasoning with Bayesian Networks, ISBN 9780521884389, April 2009.

Dean T. and Knazawa K. (1989). A model for reasoning about persistence and causation. Computational Intelligence, pp. 142–150.

Dempster A., Laird N. And Rubin D. (1977). Maximum likelihood from incomplete data via the EM algorithm. Journal of the royal statistical society, volume 39, pp. 1-38.

Dillon D.R. (2000). Piracy in Asia: A Growing Barrier to Maritime Trade. Heritage Foundation Backgrounder, volume 1379, www.heritage.org.

Eleye-Datubo A.G., Wall A. and Wang J. (2008). Marine and offshore Safety Assessment by Incorporative Risk Modelling in a Fuzzy-Bayesian Network of an Induced Mass Assignment Paradigm. Society for Risk Analysis, pp. 95-112.

Efron B. (2005). Bayesians, Frequentists, and Scientists. Journal of the American Statistical Association, volume 100, Issue 469, pp. 1-5, 2005.

Efron, B. (2010). Large scale inference: Empirical Bayes methods for estimation, testing, and prediction. Cambridge University Press.

Flin R., Mearns K., Fleming M. and Gordon R. (1996). Risk perception and safety in the offshore oil and gas industry. Health and safety executive-offshore technology report.

François O. (2006). De l'identification de structure de réseaux bayésiens à la reconnaissance des formes à partir d'informations complètes ou incomplètes. Institut national des sciences appliquées de Rouen, 28 November 2006.

Friedman N. (1998). The bayesian structural EM algorithm. In G.F. cooper and S, Moral editors, proceedings of the 14th conference on uncertainty in artificial intelligence, morgan Kaufmann, san Francisco, pp. 129-138.

Friedman N. and Goldszmidt M. (1998). Learning Bayesian Networks with Local Structure. Learning in graphical models, NATO ASI Series, Volume 89, pp. 421-459.

Friedman N., Nachman I. and Peer D. (1999). Learning of bayesian network structure from massive datasets : the sparse candidate algorithm. In proceedings of the 15th conference on uncertainty in artificial intelligence, pp. 206-215, San mateo.

Giraud M.A, Van Gaver A., Napoli A., Scapel C., Chaumartin D., Morel M., Itcia E. and Bonacci D. (2010). SARGOS : Système d'Alerte et de Réponse Graduée OffShore. Workshop Interdisciplinaire sur la Sécurité Globale, Université de technologies de Troyes, janvier 2010.

Giraud M.A., Alhadef B., Guarnieri F., Napoli A., Bottala-Gambetta M., Chaumarin D., Philips M., Morel M., Imbert C., Itcia E., Bonacci D. and Michel P. (2011). SARGOS : Système d'Alerte et Réponse Graduée OffShore. WISG 2011, Troyes, France.

Giraud M. A, Alhadef B, Guarnieri F, Napoli A, Bottala Gambetta M, Chaumartin D, Philips M, Morel M, Imbert C, Itcia E, Bonacci D,and Michel P. (2011). SARGOS: Securing Offshore Infrastructures Through a Global Alert and Graded Response, System Workshop MAST Europe, pp. 27–29, 27 June 2011.

Giraud M.A., Alhadef B., Guarnieri F., Napoli A., Bottala-Gambetta M., Chaumarin D., Philips M., Morel M., Imbert C., Itcia E., Bonacci D. and Michel P. (2012). SARGOS : Système d'Alerte et Réponse Graduée OffShore. Workshop interdisciplinaire sur la sécurité globale, Université de technologies de Troyes, janvier 2012.

Giraud M.A., Alhadef B., Chaze X., Napoli A., Naudibn A.C., Bottala-Gambetta M., Grimaldi G., Chaumarin D., Morel M., Imbert, C., Wasselin J.P., Bonacci D. and Michel P. (2013). SARGOS : Système d'Alerte et Réponse Graduée OffShore. Workshop interdisciplinaire sur la sécurité globale, Université de technologies de Troyes, 22 et 23 janvier 2013.

Gordon R.P.E., Flin R.H., Mearns K. and Fleming M.T. (1996). Assessing the human factors causes of accidents in the offshore oil industry. International conference on health, safety and environment in oil and gas exploration and production, No 3, New Orleans, United States, pp. 635–644.

Hansen S.J. (2009). Piracy in the greater Gulf of Aden, Myths, Misconception and Remedies, Norwegian Institute for Urban and Regional Research.

Harris B. (2011). Graph theory and its applications: proccedings. Academic Press, University of Michigan.

Heckerman D., Meek C. and Cooper G. (1997). A Bayesian Approach to Causal Discovery. technical report, MSR-TR-97-05, February 1997.

Heckerman D. (1999). A tutorial on learning with Bayesian network, M.I Jordan, learning in graphical models, Kluwer Academic Publishers, Boston, pp. 301–351.

Hudson L.D., Bryan S.W., Mahoney S. and Blackmond K. (2002). An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners.

International Maritime Organization. (2008). Reports on Acts of Piracy and Armed Robbery Against Ships. www.imo.org.

Jenkins B.M. (1988). Potential threats of offshore platforms. Rand Corporation.
Jensen F. (1996). Introduction to Bayesian Networks. Springer Verlag.

Jordan M.I. (1998). Learning in Graphical Models. The Netherlands: Kluwer Academic Publishers.

Jordan M.I. (1998). Learning in Graphical Models, MIT Press.

Jordan M.I. (1999). An Introduction to Variational Methods for Graphical Models. Machine Learning, 37, pp. 183–233.

Jordan M. (2004). Graphical Models. Statistical Science, Special issue on Bayesian Statistics, Volume 19, 140-155.

Kaasen K. (1984). Safety Regulation of Offshore Petroleum Activities: a Study of the Legal Framework on the Norwegian Continental Shelf. Oslo University.

Kalev K. and Dechter R. (1999). Stochastic local search for Bayesian networks. 7th International Workshop on Artificial Intelligence and Statistics.

Kashubsky M. (2008). Offshore energy force majeure: Nigeria's local problem with global consequences. Maritime studies.

Khakzad N., Khan F. and Amyotte P. (2013). Quantitative risk analysis of offshore drilling operations: A Bayesian approach. Safety Science, 57, pp. 108-117.

Kim J.H. and Pearl J. (1983). A computational model for causal and diagnostic reasoning in inference engines. Proc. 8th Int. Joint Conf. on Artificial Intelligence, pp.190–193.

Kim J. et Pearl J. (1987). Convice : a conversational inference consolidation engine. IEEE Trans. On Systems, Man and Cybernetics, volume 17, 120-132.

Koskinen J.H. and Snijders T.A.B. (2007). Bayesian inference for dynamic social network data. Journal of statistical planning and inference , olume 137, pp. 3930-3938.

Langseth H. and Bangso O. (2001). Parameter learning in object-oriented Bayesian networks, Annals of Mathematics and Artificial Intelligence, 32, pp. 221–243.

Lauritzen S.L. and Spiegelhalter D.J. (1988). Local Computations with Probabilities on Graphical Structures and Their Application to Expert Systems, Journal of the Royal Statistical Society. Series B (Methodological), Volume 50, No 2, pp. 157–224.

Lee C. and Lee K.J. (2006). Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal. Reliability Engineering & System Safety, volume 91, n°5, pp. 515–532.

Leray P. (2006). Réseaux bayésiens : apprentissage et modélisation de systems complexes. Habilitation à diriger les recherché, université de rouen, UFR des sciences.

Leray P., Meganck S., Maes S., and Manderick B. (2008). Causal graphical models with latent variables : learning and inference. In Holmes D. E. and Jain L., editors, Innovations in Bayesian Networks: Theory and Applications, Studies in Computational Intelligence, vol.156, pp. 219-249. Germany, Springer.

Little R.J. (2006). Calibrated Bayes : A bayes/ Frequentist roadmap. The American Statistician, volume 60, issue 3, pp. 213-223.

Martín J.E., Rivas T., Matías J.M., Taboada J. and Argüelles A. (2009). A Bayesian network analysis of workplace accidents caused by falls from a height. Safety Science, volume 47, n°2, pp. 206–214.

Meganck S., Laray P. and Manderick B. (2006). Learning causal Bayesian Networks from observations and experiments: A decision theoretic approach. Modeling decisions for artificial intelligence, lecture notes in computer science, volume 3885, pp. 58-69.

Morel M., Gleizes M.P., Napoli A., Littaye A., Bazin V., Alhadef B., Scapel C., Leroy B., Lebrevelec J. and Dejardin D. (2007). ScanMaris: an Adaptive and Integrative Approach for Wide Maritime Zone Surveillance, Cognitive Systems with Interactive Sensors.

Morel M., Napoli A., Littaye A., Gleizes M.P., Bazin V., Alhadef B., Scapel C., Leroy B., Lebrevelec J. and Dejardin D. (2007). Sureveillance et contrôle des activités des navires en mer. La sécurité globale. Menaces et réponses, No 10, Novembre 2007.

Morel M., Napoli A., George J P., Jangal F., Giraud M A. and Botalla M. (2010). Surveillance et contrôle des activités des navires en mer. Workshop interdisciplinaire sur la sécurité globale, Université de technologies de Troyes, 26 et 27 janvier 2010.

Morel M., Napoli A., Littaye A., Georgé J P. and Jangal F. (2008). Surveillance et contrôle des activités des navires en mer. Workshop interdisciplinaire sur la sécurité globale, Université de Technologie de Troyes, 29 et 30 janvier 2008.

Morel M. and Broussolle J. (2011). I2C, Interoperable sensors and Information sources for Common Detection of abnormal vessel behaviours and Collaborative suspect events analysis. MAST 2011, Marseille, France.

Mukundan P. (2003). Piracy and Armed robbery against ship today. WMU journal Of Maritime Affairs, Volume 3, Issue 2, pp. 167–180, October 2003.

Murphy K.P., Weiss Y. And Jordan M. (1999). Loopy belief propagation for approximate inference : An empirical study. In : proceeding of the fifteenth annual conference on uncertainty in artificial intelligence, san Francisco, pp. 467-475.

Murphy K.P. and Weiss Y. (2001). The factored frontier algorithm for approximate inference in dynamic bayesian networks., UAI.

Murphy K.P. (2002). Dynamic Bayesian networks: Presentation, Inference and Learning. Cambridge University.

Naïm P., Wuillemin H., Leray P., Pourret O. and Becker A. (1999). Réseaux bayésiens. Eyrolles, 3ème édition, ISBN : 978-2-212-11972-5.

Naïm P., Wuillemin P.H., Leray P., Pourret O. and Becker A. (2004). Réseaux Bayésiens, Eyrolles, ISBN, 2-212-11137-1.

Naïm P., Wuillemin P.H., Leray P., Pourret O., and Becker A. (2007). Réseaux bayésiens. Eyrolles, Paris, 3ème edition.

Napoli A. (2014). Sécurité et sûreté de la maritimisation de l'énergie. Revue des Ingénieurs des Mines, Dossier La Mer, volume 472, pp. 23-25, mars/avril 2014.

Neapolitan E. (2003). Learning Bayesian Networks, Prentice-Hall, Inc. Upper Saddle River, NJ, USA, ISBN : 0130125342.

Neapolitan R.E. (2012). Probabilistic Reasoning In Expert Systems: Theory and Algorithms. ISBN 1477452540 9781477452547.

Nielsen T.D. and Verner J.F. (2007). Bayesian Networks and Decisions Graphs. Series Information Science and Statistics, 2nd edition, XVI, ISBN 978-0-387-68282-2, 447 p.

Nielsen T.D. and Finn V.J. (2009). Bayesian networks and decision graphs. Springer, 463 p.

Nikoski D. (1998). Learning stationary temporal probabilistic networks. In : conference on automated learning and discovery.

Nincic D. J. (2009). Maritime Security as Energy Security: Current Threats and Challenges. In Luft, G., and Konin, A., eds. Energy Security: Challenges for the 21st Century. Washington DC: Greenwood Publishing in collaboration with the Institute for the Analysis of Global Security (IAGS).

Onuoha F. (2010). Sea piracy and maritime security in the Horn of Africa : The Somali coast and Gulf Of Aden in perspective, African Security Review, Volume 18, Issue 3, pp. 31–44, 22 July 2010.

Pearl J. (1988). Probabilistic Reasoning in Intelligent Systems : Networks of Plausible Inference. Morgan Kaufmann Publishers, Inc. San Mateo, CA.

Pearl J. (2000). Causality: Models, Reasoning and Inference. Cambridge, England: Cambridge University Press, ISBN, 0-521-77362-8.

Pichard J.F. (1998). Approche épistémologique et diverses conceptions de la probabilité. Reperes-IREM, No 32, Université de Rouen, juillet 1998.

Rabiner L.R. (1989). Atutorial on hidden markov models and selected applications in speech recognition. Proceedings of the IEEE, volume 77, No 2.

Reason J. (1990). Human Error. Cambridge University Press, 320 p.

Ren J., Jenkinson I., Wang J., Xu D.L. and Yang J.B. (2008). A methodology to model causal relationships on offshore safety assessment focusing on human and organizational factors. Journal of Safety Research 39, pp. 87-100.

Riveiro M., Falkman G., Ziemke T. and Warston H. (2009). VISAD : an interactive and visual analytical tool for the detection of behavioral anomalies in maritime traffic data. Proceedings of SPIE, mai 2009.

Ryan M.(2006). Captain counts the cost of piracy. BBC News, news.bbc.co.uk.

Saab groupe. (2005). Sea Giraffe AMB multi-rôle naval surveillance radar. http://www.saabgroup.com/Global/Documents%20and%20Images/Naval/Situational%20Awareness/Sea%20GIRAFFE%20AMB/SEA%20GIRAFFE%20AMB%20ENG%20print.pdf

Sagem. (2012). SAGEM l'excellence en optronique, avionique, électronique et logiciels critique. http://www.sagem.com/IMG/pdf/SAGEM_PLAQUETTE-FR.pdf

Schroeder D.M., and Love M.S. (2004). Ecological and political issues surrounding decommissioning of offshore oil facilities in the Southern California Bight. Ocean and Coastel Management, volume 47, 2004, pp. 21-48.

Spirtes P., Glymour C. And Scheines R. (1993). Causation, prediction, and search. Springer-verlag, ISBN : 0387979794.

Stephenson A. (2000). An introduction to bayesian network theory and usage. IDIAP Research report, pp. 00-03.

Trucco P., Cagno E., Ruggeri F. and Grande O. (2008). A Bayesian Belief Network modelling of organisational factors in risk analysis : A case study in maritime transportation, Reliability Engineering and System Safety, pp. 823-834.

United Nations. United Nations Convention on the Law of the Sea. www.un.org.

Vandecasteele A. and Napoli A. (2012). Spatial ontologies for detecting abnormal maritime behaviour. OCEANS2012, Yeosu, South Korea.

Vandecasteele A., Devillers R. and Napoli A. (2014). From movement data to objects behavior using semantic trajectory and semantic events. Marine Geodesy, volume 37, No 2, pp. 126-144, 03 april 2014.

Verma T. And pearl J. (1991). Equivalence and synthesis of causal models. In M. Henrion, R. Schachter, L. Kanal, and J. Lemmer, editors, proceedings of the sixth conference on uncertainty in artificial intelligence, San Francisco, pp. 220-227.

Vinnem J.E., Bye R., Gran B.A., Kongsvik T., Nyheim O.M., Okstad E.H., Seljelid J. and Vatn J. (2012). Risk modeling of maintenance work on major process equipment on offshore petroleum installations. Journal of Loss Prevention in the Process Industries 25, pp. 274-292.

Wainwright J. and Jordan M. (2008). Graphical Models, Exponential Families and Variational Inference. Foundations and Tends in Machine Learning, Volume 1, No 1-2, pp. 1-305.

White H.K., Hsing P.Y., Cho W., Shank T.M., Cordes E.E., Quattrini A.M., Nelson R.K., Camilli R., Demopoulos A.W.J., German C.R., Brooks J.M., Roberts H.H., Shedd W., Reddy C.M. and Fisher C.R. (2011). Impact of the Deepwater Horizon oil spill on a deep-water coral community in the Gulf of Mexico, Cross Mark, Volume 109 No 50, November 2011.

Wright C. (1994). A fallible safety system: institutionalised irrationality in the offshore oil and gas industry. The sociological review, Volume 42 Issue 1, pp. 79–103.

Yergin, D. (2006). Ensuring Energy Security, Foreign Affairs. Volume 85, No. 2.

Yuan C. And Druzdzel M.J. (2006). Importance sampling algorithms for bayesian networks : principles and performance. Mathematical and computer modelling, volume 43, pp. 1189-1207.

Zhang L. (1994). A simple approach to Bayesian network computations. In : Proc. Of the Trenth Canadian Conference on Artificial Intelligence, pp. 171-178.

Apports des réseaux bayésiens à la prévention du risque de piraterie à l'encontre des plateformes pétrolières

RESUME : Ces dernières années, les attaques de pirates contre des navires ou des champs pétroliers n'ont cessé de se multiplier et de s'aggraver. Pour exemple, l'attaque contre la plateforme Exxon Mobil en 2010 au large du Nigeria s'est soldée par l'enlèvement de dix-neuf membres d'équipage et la réduction de 45.000 barils de sa production pétrolière quotidienne ce qui a engendré une montée des prix à l'échelle internationale. Cet exemple est une parfaite illustration de l'ampleur des dommages sur la sécurité des infrastructures pétrolières offshore.

Dans le cadre de notre recherche, nous proposons une démarche de pilotage et de management du risque de piraterie en se basant sur le concept des réseaux bayésiens qui permettent la représentation des connaissances et le calcul des probabilités conditionnelles. Une dimension temporelle a été ajoutée par le recours aux réseaux bayésiens qualifiés de « dynamiques ». Ces réseaux, fondés sur les chaines de Markov cachées ou filtres de Kalman, se révèlent très performants dans le domaine de l'analyse des risques.

L'application de ces réseaux au domaine de la piraterie a été envisagée, les apports et les limites seront évalués dans le cadre de cette thèse.

Mots clés : Management du Risque, Piraterie Maritime, Champs Pétroliers Offshore, Réseaux Bayésiens, Réseaux Bayésiens Dynamiques, Système d'aide à la décision.

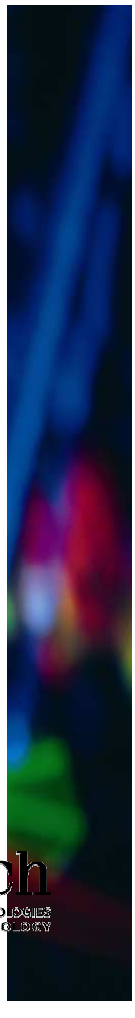
Contribution of Bayesian networks to the prevention of the risk of piracy against Oil Offshore Fields

ABSTRACT : In recent years, pirate attacks against ships or oil fields have continued to multiply and worsen. For example, the attack against the Exxon Mobil platform in 2010 in the coast of Nigeria has resulted in the removal of nineteen crew members and the reduction of 45,000 barrels of daily oil production which resulted in a rise prices internationally. This example is a perfect illustration of the extent of damage on the safety of offshore oil infrastructure.

As part of our research, we propose an approach to control and management of the risk of piracy based on the concept of Bayesian networks that enable knowledge representation and calculation of conditional probabilities. A temporal dimension was added by the use of Bayesian networks called "dynamic". These networks, based on Markov chains or Kalman filters, are proving very effective in the field of risk analysis.

The application of these networks on piracy was considered, the contributions and limitations will be evaluated as part of this thesis.

Keywords : Risk management, Maritime piracy, offshore oil fields, Bayesian Networks, dynamic Bayesian Network, decision support system.



MINES ParisTech

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY