Apports des Réseaux Bayésiens "Dynamiques" à la lutte contre la piraterie maritime

Franck Guarnieri, Amal Bouejla, Aldo Napoli

Apports des Réseaux Bayésiens « Dynamiques » à la lutte contre la piraterie maritime

Contribution of Dynamic Bayesian networks against maritime piracy

Franck Guarnieri, Amal Bouejla et Aldo Napoli
MINES ParisTech, CRC
Centre de recherche sur les Risques et les Crises
1 Rue Claude Daunesse 06900 Sophia Antipolis
04.93.67.89.14
04.93.95.75.81
franck.guarnieri@mines-paristech.fr
amal.bouejla@mines-paristech.fr
aldo.napoli@mines-paristech.fr

Résumé

L'article développe et discute le projet de conception d'un outil d'aide à la décision fondé sur les modèles de l'analyse probabiliste. Le concept de réseaux bayésiens « dynamiques » a été retenu afin de créer un modèle graphique d'aide à la décision dans un univers incertain. La construction de ce type de réseaux bayésiens 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 décrire la démarche méthodologique qui a permis de concevoir un prototype visant 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. Une étude comparative entre les réseaux bayésiens dits « statiques » et les réseaux bayésiens dits « dynamiques » est conduite dans le double but d'en montrer les différences et les usages complémentaires.

Summary

The paper develops and discusses the project of designing a tool for decision support based on probabilistic analysis. The concept of "dynamic" Bayesian networks was chosen to create a graphical decision support in an uncertain world. The construction of this type of Bayesian networks can incorporate within knowledge bases probabilities distributions useful for predicting the future taking into account the past. The aim of the article is to describe the methodological approach that has helped design a prototype for planning of countermeasures applied against attacks of piracy against an oil platform at sea. The prototype supports the decision taking into account the influence of the decision at time T-1 on the decision to take at time T. A comparative study of Bayesian networks called "static" and Bayesian networks called "dynamic" is driving the dual purpose of showing the differences and complementary uses.

Introduction

En 2006 des pirates abordent une plateforme pétrolière, enlèvent neuf travailleurs offshore et endommagent les matériels de la plateforme. En 2007, un membre d'équipage d'une plateforme pétrolière est kidnappé lors d'une attaque. Ces derniers montent à bord par le navire de soutien, naturellement amarré à la plateforme lors d'une classique opération de logistique. L'otage est libéré après le versement d'une rançon. Plus récemment, le 23 novembre 2013, trois pirates armés de couteaux pénètrent dans un navire de cargaison ancré. Ils font irruption dans la salle des machines. Le chef de la salle est séquestré, tandis que deux pirates dérobent des pièces de rechange des moteurs. Au fil des ans, ces attaques augmentent et deviennent de plus en plus violentes. Elles mettent en danger la vie des collaborateurs des entreprises exploitantes, endommagent des biens d'une grande valeur et menacent l'économie d'une filière industrielle.

Cet article traite de la problématique des risques liés à la maritimisation de l'énergie. Face à ces menaces avérées, le recours aux réseaux bayésiens se révèle comme une solution efficace pour l'aide à la prise de décision dans un univers incertain et contraint par le temps. Parmi les différentes formes de réseaux bayésiens, ceux dits « dynamiques » ont été retenus. Ils complètent en effet avantageusement les réseaux dits « classiques » et offrent de nombreux bénéfices. Un modèle a été conçu et développé au sein d'un prototype. Les résultats sont testés et discutés sur des scénarios complets et réalistes d'attaques de pirates.

Les risques de maritimisation de l'énergie

« *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 Economique 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).

1 Le pétrole et le gaz, des ressources particulièrement menacées

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 que nous consommons actuellement au rythme de 70 millions de barils par jour et certaines estimations prévoient que cela doublera 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 1000 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 Gb.

La construction, le transport, le fonctionnement d'une plateforme pétrolière génèrent divers risques. D'éventuels incidents ou accidents technologiques peuvent aggraver des impacts sur l'environnement, les marins ou les biens. Le risque sismique, le risque des rejets et de toxicité, le risque d'incendie ou d'explosion complètent le panorama des menaces. Le risque d'explosion est le plus redouté. Le risque de pollution perturbe gravement 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 sur l'environnement. Compte tenus des enjeux économiques liés à la cherté des hydrocarbures, les champs de production offshore deviennent de plus en plus une cible de choix pour la piraterie maritime voire la menace terroriste. 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 donc des cibles de choix, isolées et de fait très exposées.

2 Les attaques de piraterie à l'encontre des plateformes pétrolières

La production pétrolière mondiale est répartie sur plus de 10 000 champs offshore, impliquant chacun d'une part un ensemble d'infrastructures 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.

La piraterie à l'encontre des installations pétrolière en mer a depuis 1988 pris une ampleur considérable. (Kashubsky., 2008) a ainsi conduit une étude très détaillée sur le Nigeria. Nous avons retenu quelques évènements significatifs à des fins d'illustrations (Tableau 1).

Date	Description de l'attaque	Conséquences
12 juin 2005	un groupe armé aborde le FPSO Jameston (floating production, storage and offloading)	prises en otage de 45 personnes qui seront libérées moyennant rançon trois jours plus tard
11 janvier 2006	une plateforme de Shell est attaquée	4 personnes sont prises en otages depuis le navire de maintenance ancré à la plateforme
15 janvier 2006	une attaque très violente d'une installation de Shell se transforme en un incendie	d'importants dégâts et la mort de 17 personnes
18 février 2006	un speedboat attaque une installation	on dénombre 9 blessés parmi les personnels
2 octobre 2006	des barges de Shell sont attaquées	trois militaires protégeant le dispositif sont tués
1 avril 2007	une installation subie une seconde attaque	le navire de maintenance a été détourné par les pirates, l'accostage a donc été possible
19 avril 2007	un navire de sécurité est attaqué	il est même dépouillé de son propre armement
03 mai 2007	le FPSO Mystras est attaqué, les pirates ont utilisé la chaîne de l'ancre pour monter à bord	huit employés sont kidnappés
21 octobre 2007	un important groupe armé attaque simultanément deux navires de maintenance.	
19 juin 2008	le FPSO Bonga est attaqué et endommagé	la production est arrêtée, une perte est estimée à plus de 200 000 barils par jour
14 septembre 2008	deux plateformes de Shell et Chevron sont attaquées simultanément	
16 septembre 2008	8 bateaux rapides chargés de dynamite et de grenades à main attaquent la station de pompage de Shell (Orubiri)	les pirates ont causés d'importants dégâts
22 septembre 2010	le remorqueur Bourbon Alexandre se trouvant sur le champ pétrolier d'Addax au large du Nigeria, a été attaqué par quatre embarcations rapides	prises en otage de trois marins français. Il s'agissait de la quatrième attaque contre Bourbon depuis 2009
17 novembre 2010	des pirates embarqués sur une vedette rapide ont attaqué un bateau de la société française Perenco qui transportait des forces de sécurité camerounaises près d'une plate-forme pétrolière dans le golfe de Guinée	cette attaque a fait six morts

Tableau 1. Illustrations des attaques de piraterie à l'encontre des installations pétrolières

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 même 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 plupart des attaques de pirates se concentrent en Indonésie et dans le détroit de Malacca. En 2007, le Nigeria s'est soudainement révélé comme une zone dangereuse en particulier pour les navires énergétiques, on y a dénombré 29% des attaques. L'Indonésie reste en tête du peloton avec plus de 35% des attaques. Cependant, en 2008, les pirates somaliens ont accru leur capacité d'intervention en allant au-delà des 200 miles nautiques. C'est ainsi qu'en 2008, on dénombra plus d'attaques au Nigeria et en Somalie qu'en Indonésie et dans le détroit de Malacca. A la fin de 2008, l'OMI (Organisation Maritime Internationale) rapporte plus de 60 attaques.

Le retour d'expérience de ces évènements 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.

Le recours aux réseaux bayésiens dynamiques pour réduire le risque de piraterie

Les actes de piraterie révèlent l'insuffisance des systèmes actuellement disponibles et mis en œuvre sur les infrastructures offshore pour les protéger contre des intrusions hostiles de type piraterie.

La sûreté des installations offshore est à ce jour assurée par deux types des moyens « classiques » (vigie, identification radio, système d'identification automatique communément nommé AIS (*automatic identification system*), radar pour la surveillance de trafic et recours à des bateaux de surveillance généralement opérés par des sociétés sous-traitantes) (Bouejla et al., 2012).

Les radars de surveillance du trafic sont destinés à détecter en priorité des mobiles coopératifs de taille importante ou moyenne. Ils ont des performances jugées insuffisantes face à de petites cibles marines de faible signature radar ou optronique, bien entendu non coopératives (absence de réflecteur radar ou d'AIS), évoluant dans une mer formée (fouillis de mer) et sont pénalisés par une zone aveugle à faible distance du porteur. Les systèmes de type service de trafic maritime VTS (*vessel traffic service*) permettent de sécuriser grandement la navigation commerciale en fournissant une image en temps réel des mouvements des navires dans une zone de surveillance donnée. S'ils sont largement opérationnels, d'une part leurs modes de détection usuels sont plus particulièrement adaptés à des bateaux « coopératifs » et d'autre part leur finalité de gestion du trafic maritime est très différente du concept de protection contre l'intrusion hostile par petite embarcation.

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 sécurité est prévenu, son intervention reste incertaine d'autant plus qu'il se trouvera éloigné du lieu de l'attaque.

L'ambition des travaux conduits vise améliorer la phase de détection, d'alerte et de mise en sécurité de l'installation 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, leurs niveaux 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 entre eux. 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.

Une contrainte supplémentaire à prendre en compte est 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[1] (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.

3 De l'usage des Réseaux Bayésiens pour la prévention des risques maritimes

Les contraintes définis précédemment 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 d'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 réactions adaptés à la nature de l'intrusion détectée fondés sur les réseaux bayésiens sont donc proposés.

3.1 Définition

Les modèles graphiques et plus précisément les réseaux bayésiens ont été initiés par Judea Pearl dans les années 1980 [Pearl, 1988]. Ils facilitent la conception de systèmes de prédiction et d'abduction en intelligence artificielle. Les réseaux

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

bayésiens recouvrent un ensemble de modèles probabilistes pour de larges collections de variables. Ils ont pour objectif d'acquérir, représenter et utiliser la connaissance.
Les réseaux bayésiens (Naïm et al., 2007) sont des modèles graphiques qui représentent les relations probabilisées entre un ensemble des variables. Depuis quelques années, les Réseaux Bayésiens sont devenus très populaires pour représenter et manipuler des connaissances expertes dans un système à base de connaissances. Ils sont souvent utilisés car ils conjuguent les avantages de diverses approches :

- La compréhensibilité des modèles symboliques,
- Les fondements probabilistes rigoureux des méthodes statistiques,
- Et la structure en réseau de composants simples des approches connexionnistes.

Un réseau bayésien est donc un graphe causal auquel on a associé une représentation probabiliste sous-jacente. Cette représentation permet de rendre quantitatifs les raisonnements sur les causalités que l'on peut faire à l'intérieur du graphe. L'utilisation essentielle des réseaux bayésiens est de calculer des probabilités conditionnelles d'événements reliés les uns aux autres par des relations de cause à effet. Cette utilisation s'appelle inférence.

3.2 Brève revue de littérature de l'utilisation des réseaux bayésiens dans le domaine de prévention des risques maritimes

Le recours aux réseaux bayésiens s'est largement développé dans le domaine de la prévention des risques et des menaces en mer de tout ordre.

(Ren et al., 2007) ont traité l'apport des réseaux bayésiens pour la prise en compte du facteur humain afin de modéliser les relations de cause à effet sur l'évaluation de la sécurité en mer. Une méthodologie a été conçue et développée. Elle s'appuie sur le modèle du « fromage suisse » élaboré par James Reason (1990). Le modèle de Reason offre un cadre générique d'évaluation des risques liés au facteur humain. Cinq niveaux permettent de caractériser les défaillances latentes au sein de la chaîne causale des événements : les causes profondes, les événements déclencheurs, les incidents, les accidents et les conséquences. La caractérisation fine de chacun des niveaux a permis de construire le réseau bayésien. Une série d'événements a été spécifiée, et les probabilités a priori et conditionnelles concernant le modèle ont été attribuées sur la base des caractéristiques intrinsèques de chaque événement.

(Trucco & al, 2008) présentent une approche pour intégrer les facteurs humains et organisationnels dans l'analyse des risques. Cette approche a été développée et appliquée à une étude de cas dans l'industrie maritime, mais elle peut également être utilisé dans d'autres secteurs. Un réseau bayésien a été développé pour modéliser les risques inhérents aux systèmes de transport maritime, en tenant compte de ses différents acteurs comme l'armateur, le port et le chantier naval et leurs influences réciproques.

(Vinnem & al., 2012) ont traité la question des fuites d'hydrocarbure en mer libérées en phase d'exploitation ou de maintenance d'une plateforme. Un modèle générique fondé sur le risque de facteurs humains d'influence a été développé et adapté à l'utilisation pour les scénarios de défaillance spécifiques. Le modèle complet du réseau bayésien est décrit, et deux implémentations sont discutées. Les probabilités d'erreur humaine, la mesure de l'importance des conséquences, ainsi que la modélisation de la cause et les interactions communes sont analysées. Les auteurs démontrent que le modèle est apte à considérer les facteurs humain et organisationnel et la culture de sécurité.

Enfin (Khakzad & al., 2013) se sont intéressés à prévenir le risque de fuites incontrôlées de pétrole brut « blowouts » durant les opérations de forage. Les auteurs proposent deux méthodes pour démontrer l'intérêt de l'usage conjoint de « bow-tie » (nœud papillon) et de réseaux bayésiens. La première méthode consiste à utiliser un arbre de défaillance et un arbre d'événements développés pour des scénarios d'accidents potentiels. Dans la seconde méthode, des réseaux bayésiens sont créés pour des scénarios d'accidents puis, un réseau bayésien « orienté objet » est construit afin de les relier les uns aux autres. Le réseau bayésien offre ainsi une meilleure approche que le modèle « bow-tie », car il permet d'envisager des défaillances de cause commune et des dépendances conditionnelles avec l'exécution probabiliste mise à jour et l'apprentissage séquentiel en utilisant des précurseurs d'accidents.

Ces références soulignent la richesse des travaux conduits tant sur la prise en compte des risques techniques que des facteurs humains et organisationnels afin de prévenir les menaces qui pèsent sur les plateformes pétrolières en mer et plus globalement sur la filière (Bouejla et al., 2014).

4 Réseaux bayésiens statiques versus réseaux bayésiens dynamiques

Les réseaux bayésiens ne modélisent classiquement pas des relations temporelles entre les variables et la prise en compte d'une dimension temporelle peut engendrer des complications techniques dans la modélisation et l'édition du réseau qui devient vite fastidieuse et source d'erreurs. Ces réseaux dits « statiques » représentent seulement des liens probabilistes au sein d'un ensemble de variables à un instant de temps donné (Neapolitan, 2004). Pourtant dans plusieurs domaines, la modélisation des relations temporelles se révèle indispensable. La piraterie maritime n'échappe pas à cette exigence puisque les données concernant la planification de réaction contre une attaque sont forcement à générer selon l'évolution d'une situation tant dans l'espace que dans le temps. Le recours à un réseau bayésien dit « dynamique » est dés lors pertinent.

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, une notation graphique est utilisée afin de représenter des nœuds indexés par des pas de temps génériques. Deux types de liens, les liens classiques des réseaux bayésiens et des liens dits temporels permettent de définir les tables de probabilités conditionnelles des nœuds en fonction de leurs parents situés à des indices de temps inférieurs (Bouissou et al., 2012).

La figure 1 illustre un réseau bayésien dynamique générique illustrant cinq pas de temps. Les variables sont divisées en variables d'état dont les valeurs sont non déterminées, et en variables d'observation dont les valeurs sont déterminées. Les variables d'état évoluent dans le temps selon un modèle ayant préalablement calculé leurs tables de probabilités

conditionnelles. Les variables d'état sont en relation avec les variables d'observation par les tables de probabilités conditionnelles de l'observation (Zweig, 1998).

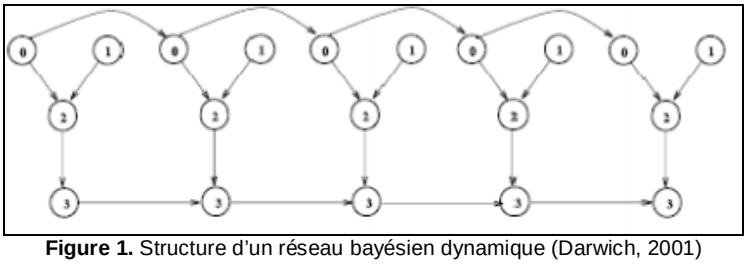

Figure 1. Structure d'un réseau bayésien dynamique (Darwich, 2001)

5 Démarche de modélisation

Dans cette section, nous présentons d'abord un prototype de système de planification d'une réponse face à une probable attaque de pirates basé sur les réseaux bayésiens statiques. Puis, nous décrivons les limites de ce modèle. Enfin, nous présentons le premier prototype d'un système d'élaboration d'une procédure de réponses à une menace, tenant compte de l'évolution temporelle, fondé sur l'usage des réseaux bayésiens dynamiques.

5.1 Présentation du système de planification des réactions basé sur les réseaux bayésiens statiques

Dans (Chaze et al., 2013), nous avons proposé un système d'aide à la décision dans le cas d'une attaque de piraterie contre un champ pétrolier. L'approche élaborée est de développer un réseau bayésien statique exploitant les données de la base OMI sur les actes de piraterie pour déduire les réactions les plus utilisées, leurs efficiences et les distributions d'utilisation de ces réactions. Ces résultats sont intégrés dans un autre réseau bayésien statique (Figure 2) élaboré à partir de la connaissance d'experts du domaine maritime. La planification des réactions possibles est déterminée selon le niveau de connaissance acquis en temps réel sur les différentes menaces détectées (critères de comportement, classes d'identité, et par comparaison de la situation connue en temps réel aux situations antérieurement rencontrées et mémorisées par le système) en tenant compte des éventuelles restrictions induites par la situation territoriale du champ pétrolier ou par le statut juridique de ce champ. Le réseau bayésien gère toutes les interactions possibles entre les caractéristiques de la menace, de la cible, de l'environnement afin de déterminer le meilleur enchaînement de réponse pour faire face à la menace détectée. Ainsi le plan d'actions s'adapte à chaque instant à l'évolution du niveau de dangerosité de la situation.

Ce plan est présenté en support d'aide à la décision à l'opérateur qui en valide les différentes étapes, l'éventail des procédures proposées pouvant aller d'une simple activation d'alarme jusqu'à la mise en œuvre de moyens à capacité non létale.

La définition de la structure de ce réseau bayésien présenté dans la figure 2 a été définie dans (Bouejla et al., 2012). Cette classification regroupe les paramètres fondamentaux, le niveau global de danger de la situation, les facteurs aggravants et les contraintes, les nœuds relatifs à la communication et la demande d'assistance et les contre-mesures, détaillés ci-après.

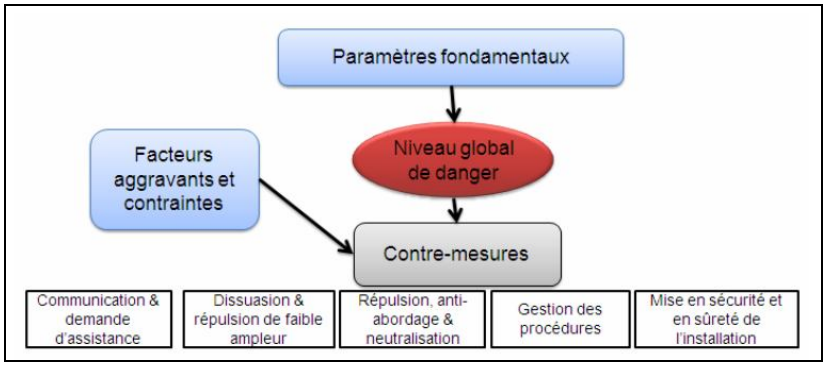

Figure 2. Structure du réseau bayésien statique (Bouejla & al., 2012)

5.1.1 Les 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, citons par exemple 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.

5.1.2 Le niveau global de danger de la situation

Ce niveau est élaboré à partir des paramètres fondamentaux pour définir la dangerosité globale de la situation. Le nœud « *Show Gradation Level* » est la formalisation de ce module dans le réseau bayésien. Le système de gradation s'échelonne de 1 pour le moindre risque à 4 pour le risque maximal.

5.1.3 Les facteurs aggravants et les contraintes

Les facteurs aggravants et les contraintes 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* ».

5.1.4 La communication et la demande d'assistance

La communication et la demande d'assistance sont deux types de réponse indispensables en cas de menace. La communication interne à la cible permet d'avertir tous les personnels concernés (exemple "informer le maître de l'équipage « *Inform OIM* ») alors que la communication externe permet à différentes échelles d'avertir les différents acteurs concernés par la sûreté de la vie en mer (demander l'intervention du navire de sûreté « *Request Security Vessels* », Mettre en œuvre le Système d'Alerte de Sûreté Silencieux « *Raise SSAS* », etc.).

5.1.5 Les 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. Elles sont la concrétisation du plan de réponse et constituent un ensemble des moyens et d'actions pour normaliser au plus vite la situation de la cible attaquée.
Ces contre-mesures sont partagées en cinq sous-modules. Ces sous-modules ainsi définis traduisent la notion même de gradation de la réponse en proposant des contre-mesures d'ampleur croissante selon la nature de la menace détectée. Ces contre-mesures sont détaillées ci-après :

- La dissuasion et la répulsion de faible ampleur : Il s'agit de faire savoir aux attaquants que la cible connait ses intentions, qu'elle est capable de les suivre et qu'ils n'ont aucun intérêt à passer à l'action en utilisant des moyens à effets faibles tels que le projecteur lumineux de recherche, les lances à incendie ou les canons sonores « *Activate LRAD* » (Long-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. Le rôle du « *Set CrowControl Munition* » est de retarder la progression des attaquants pour les fatiguer voire les neutraliser et ainsi laisser un maximum de temps à l'équipage pour mieux gérer les autres actions de sûreté.
- La gestion des procédures : Cette planification est composée des contre-mesures suivantes :
    - Le nœud « *Crew Mangement* » propose pour chaque cas de sonner le branle-bas équipage de l'infrastructure puis de les réunir aux points de rassemblement définis en cas d'alerte de sûreté.
    - Le nœud « *Asset Assault Management* » permet dans chaque cas une gestion de la cible potentielle en termes de mise en sécurité et sûreté.
- La mise en sécurité et en sûreté de l'installation : Comme pour la gestion des procédures, Le réseau propose au sein de la planification des actions qui concernent le contrôle de l'outil de production afin de le stopper en toute sécurité ou l'interdiction d'accéder aux locaux sensibles.

Les contre-mesures gérées par le système s'articulent en un ensemble de contre-mesures d'ampleur croissante permettant de graduer la réponse pour s'adapter à la nature et l'évolution de la menace et un réseau de communication interne et externe permettant la diffusion de l'alerte, la coordination de la réponse et la demande d'assistance.

Malgré l'adaptabilité, la graduation et l'évolutivité du modèle statique présenté ci-dessus, plusieurs limites sont à signaler.

5.2 Les limites de l'existant

Le réseau bayésien proposé permet la formulation et le déclenchement d'un ensemble de contre-mesures en situation d'urgence. A chaque alerte, le système 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 protégée, la distance entre la cible et le navire pirate, etc.).

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, pour un navire qui se dirige vers une plateforme ou un navire pétrolier, les paramètres fondamentaux 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 adaptés à l'évolution des informations détectées et il conserve les contre-mesures déclenchées lors du premier traitement. Comme dans l'exemple cité dans la figure 3, 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[2] et un « *ranking*[3] » supérieur à 900 secondes. Le prototype qualifie les pirates comme « *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 envoi 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[4] 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

[2] 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.

[3] 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.

[4] 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.

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 excessive des contre-mesures pendant toutes les étapes du traitement d'une attaque et créé de fait de la confusion dans le choix des mesures à activer par les membres de l'équipage.

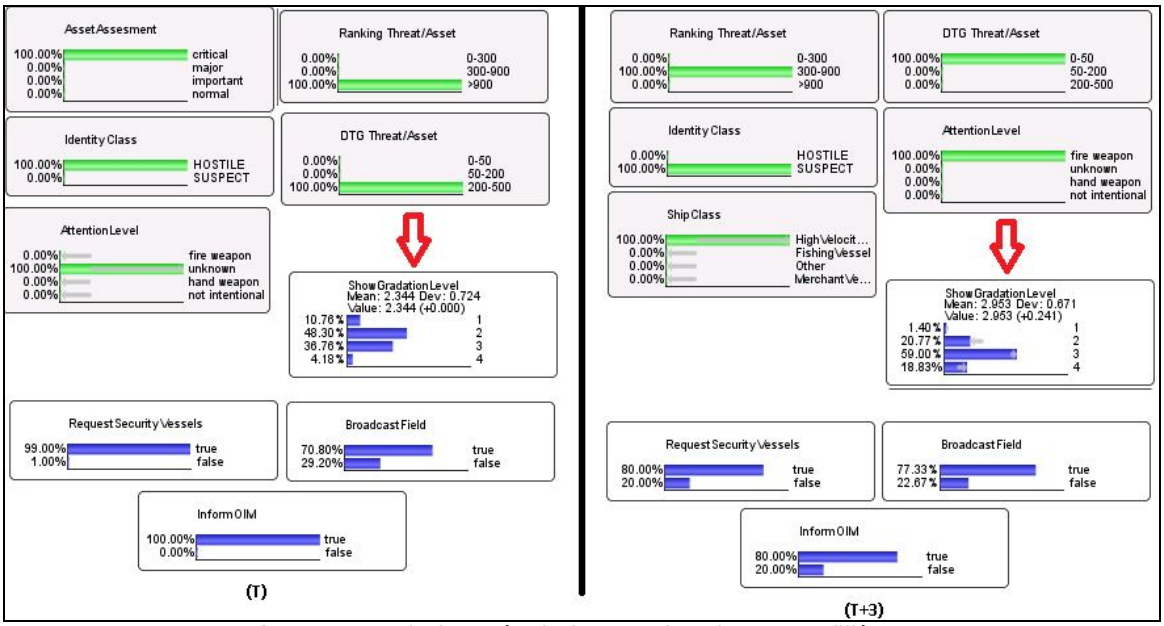

Figure 3. Exemple d'un scénario d'attaque dans deux temps différents

Les contre-mesures ne se déploient pas toutes automatiquement. Elles demandent parfois l'intervention d'un opérateur pour les déclencher. 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.

5.3 Présentation du système de planification des réactions basé sur les réseaux bayésiens dynamiques

Afin de lever les limites citées plus haut, 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.

L'architecture du réseau bayésien dynamique présentée dans la figure 4 est caractérisée par une partie (B_1, $B_{->}$), où B_1 définie 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 sont de gauche à droite et reflètent l'avancement du temps.

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.

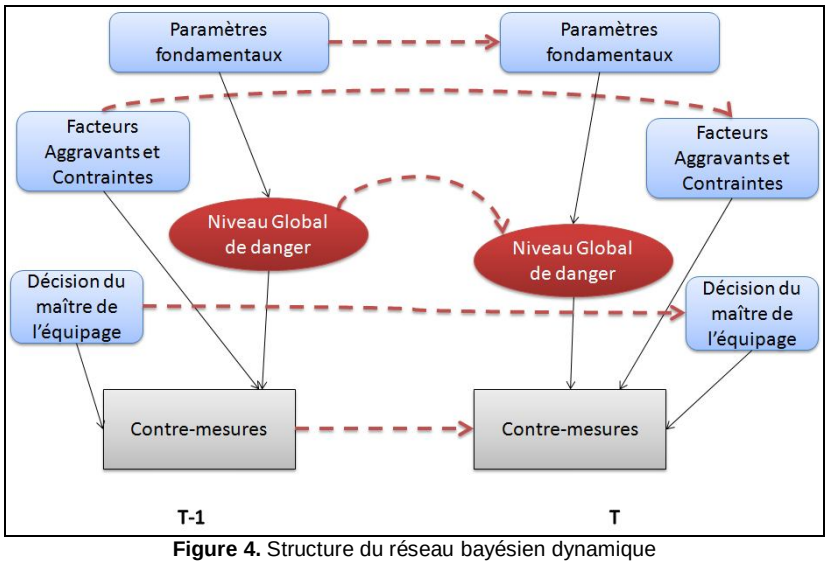

Figure 4. Structure du réseau bayésien dynamique

5.3.1 Le module Décision du maître d'équipage

Des nœuds permettent 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 reliés directement aux contre-mesures, comme le montre l'exemple dans la figure 5, par des arcs intra-tranches en utilisant l'apprentissage des paramètres statiques. Chaque nœud de décision est constitué de deux modalités : vrai ou faux.

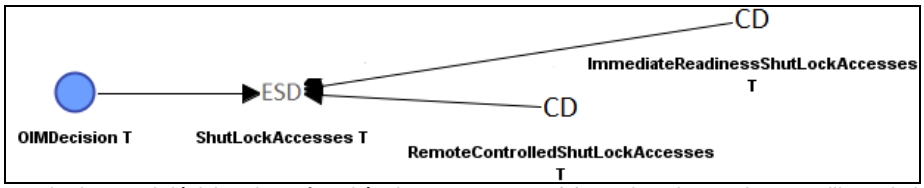

Figure 5. Exemple du nœud décision du maître d'équipage « *OIM Decision* » dans le cas de verrouillage de la production « *ShutLockAccesses* »

5.3.2 Construction des arcs inter-tranches

L'apprentissage de la structure du réseau bayésien dynamique est composé de deux types d'arcs :

- Des connexions entre les arcs d'intra-tranches, ce sont les arcs que contiennent une seule tranche, ces connexions sont déterminées dans le réseau bayésien statique existant.
- L'apprentissage des connexions des arcs d'inter-tranches, ce sont les arcs qui relient 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 connaitre 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 bayésiens 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.

Discussion des résultats

Il est 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 au regard du réseau bayésien statique.

6 Etude de scénarios d'attaques

L'exemple ci-dessous 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.

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.

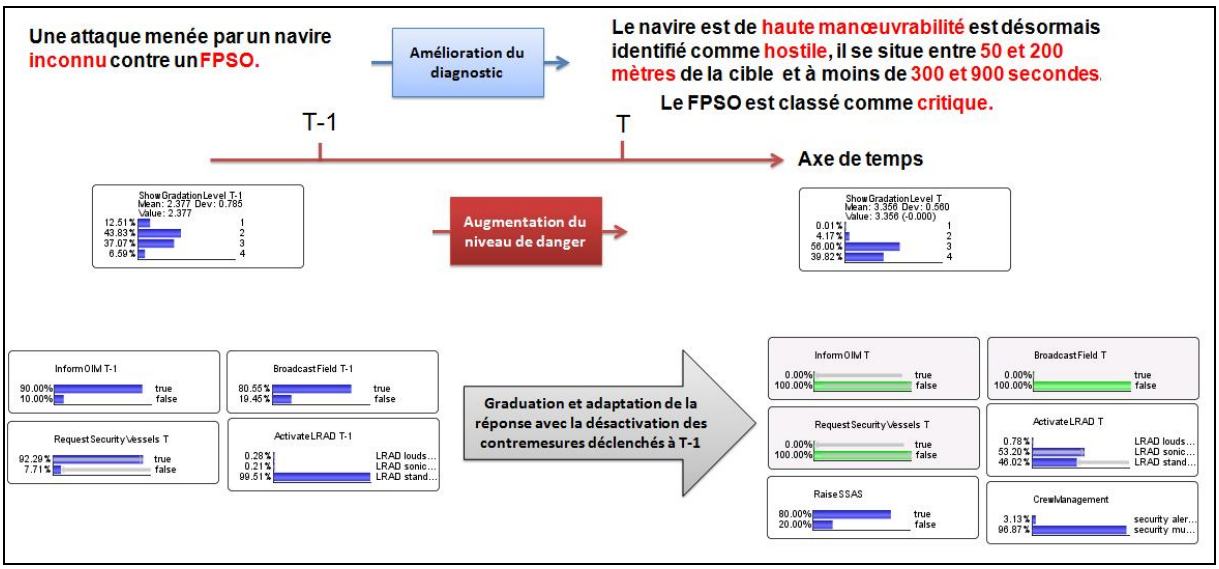

Figure 6. Résultats de la planification dans deux tranches de temps (T-1 et T) lors d'une attaque contre un FPSO

Le réseau bayésien dynamique conçu considère aussi les interventions des opérateurs. L'exemple illustré dans la figure 7 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.

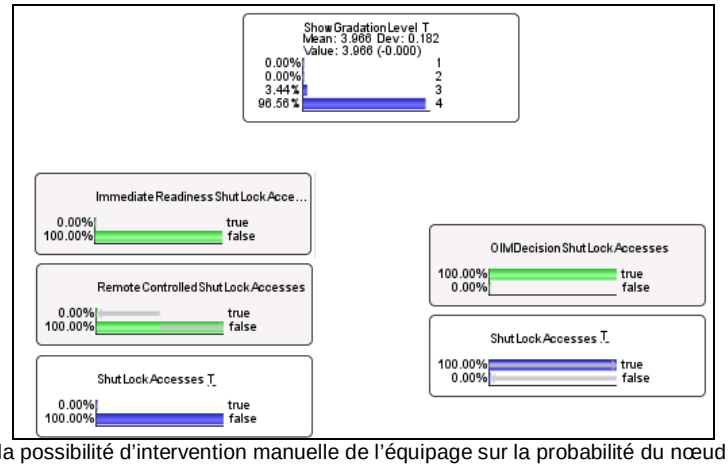

Figure 7. Résultats de la possibilité d'intervention manuelle de l'équipage sur la probabilité du nœud « *ShutLockAccesses* »

L'exemple ci-dessus 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, 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 d'autre part permet 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.

Conclusion et perspectives

Les réseaux bayésiens statiques et les réseaux bayésiens dynamiques sont 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.

Dans cet article, 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 basés 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 incrémentale des données collectées. Ainsi, nous avons pu concevoir un prototype de système permettant à l'exploitant d'un champ pétrolier d'accroitre 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.

Malgré ces atouts au niveau des résultats, la structure du réseau bayésien dynamique n'est pas facile à manipuler en augmentant le nombre des nœuds et arcs d'indépendances. En plus l'augmentation du nombre des parents d'un nœud engendre des grandes matrices de probabilités. Dans le cas où le réseau est construit seulement à partir d'une base de données, ce problème sera facile à manipuler avec l'apprentissage automatique. Alors que dans le cas des connaissances expertes, la détermination des probabilités demandent plusieurs sessions de travail et une phase importante de test et validation à partir des différents exemples et scénarios d'attaque.

Notre modèle peut être amélioré, car il nécessite des probabilités dont la détermination requière typiquement de grandes quantités de données ou plusieurs connaissances a priori, donc la quantité de données est très importante pour 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 adapter et améliorer de manière itérative.

7 Références

Bouejla, A., Chaze, X., Guarnieri, F., Napoli, A. : Apports des réseaux bayésiens pour la sûreté et la mise en sécurité des infrastructures pétrolières offshore, 18ème Congrès de Maîtrise des Risques et Sûreté de Fonctionnement, 16-18 octobre 2012.

Bouejla, A., Chaze, X., Guarnieri, F., Napoli., A. : The contribution of Bayesian networks to manage risks of maritime piracy against oil offshore fields, Information Technologies for the Maritime Sector ITEMS, Busan, Corée, 2012.

Bouejla, A., Guarnieri, F., Napoli, A. : A Bayesian Network to Manage Risks of Maritime Piracy against Offshore Oil Fields, Safety Science, accepté, 2014.

Bouissou M., Bourreau B.: Revue des applications des réseaux bayésiens dynamiques en analyse des risques, 18ème Congrès de Maîtrise des Risques et Sûreté de Fonctionnement, 16-18 octobre 2012.

Chaze, X., Bouejla, A., Guarnieri, F., Napoli, A. : Causal Probabilistic Modelling with Bayesian Networks to combat the Risk of Piracy against Offshore Oil Platforms, The Radio Science Bulletin, vol 345, N° The Radio Science Bulletin, 2013.

Darwich, A.: Constant-space reasoning in dynamic bayesian networks, International journal of approximate reasoning, vol 26, page 161-178, 2001.

Jenkins B.M.: Potential threats of offshore platforms. Rand Corporation, 1988.

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

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

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

Napoli, Aldo : Sécurité et sûreté de la maritimisation de l'énergie, Revue des Ingénieurs des Mines, Dossier Mer, N°472, mars/avril 2014.

Neapolitan R.: Learning Bayesian Networks, Pearson Education, upper saddle River, 2004.

Nincic, D. J.: 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), 2009.

Reason J.: *Human Error,* Cambridge University Press, 320p, 1990.

Ren J, Jenkinson I, Wang J, Xu DL, Yang JB. : A methodology to model causal relationships on offshore safety assessment focusing on human and organizational factors, Journal of Safety Research 39, page 87-100, 2008.

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

Vinnem JE , Bye R, Gran BA, Kongsvik T, Nyheim OM, Okstad EH, Seljelid J, Vatn J.: Risk modeling of maintenance work on major process equipment on offshore petroleum installations. Journal of Loss Prevention in the Process Industries 25 , page 274-292, 2012.

Zweig, G.: Speech Recognition with dynamic Bayesian networks, Ph.D, Thesis, University of California, Berkeley, 1998.

8 Remerciements

Les auteurs remercient la société Preventeo qui soutient ce projet de recherche.