Application des réseaux bayésiens à la planification de la réponse à une attaque de pirates contre un champ pétrolier

Amal Bouejla, Xavier Chaze, Franck Guarnieri, Aldo Napoli

Application des réseaux bayésiens à la planification de la réponse à une attaque de pirates contre un champ pétrolier

Amal BOUEJLA* — Xavier CHAZE* — Franck GUARNIERI* — Aldo NAPOLI*

** Mines ParisTech - CRC*
Centre de recherche sur les Risques et les Crises
1 Rue Claude Daunesse, BP 207, F-06904 Sophia Antipolis cedex
{amal.bouejla, xavier.chaze, franck.guarnieri, aldo.napoli}@mines-paristech.fr

RÉSUMÉ. *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 faire face à ce problème, le système SARGOS se présente comme une solution innovante prenant en compte toute la chaîne de traitement depuis la détection d'une menace potentielle jusqu'à la mise en œuvre de la réaction. Pour réagir contre une attaque, il faut considérer de nombreux paramètres relatifs à la menace, la cible potentielle, les dispositifs de protection mis en place, les contraintes liées à l'environnement, etc. Pour gérer ces paramètres, les potentialités des réseaux bayésiens sont exploitées afin de définir les contre-mesures possibles ainsi que leur mode de gestion.*

ABSTRACT. *In recent years, pirates attacks against ships or oil platforms have continued to multiply and get worse. To address this problem, the SARGOS system is as an innovative solution taking account the whole processing chain from detection of a potential threat to the implementation of the reaction. To react against an attack, we should consider many parameters of the threat, the potential target, the existing protection tools, the environment constraints, etc. To manage these parameters, the potentials of Bayesian Networks are used to identify feasible counterattacks and their management.*

MOTS-CLÉS : *plates-formes pétrolières, menace, piraterie, cible potentielle, réseaux bayésiens, SARGOS.*

KEYWORDS: *oil platforms, threat, pirates, potential target, Bayesians networks, SARGOS.*

Bouejla A., Chaze X., Guarnieri F. et Napoli A., 2012 :
« Application des réseaux bayésiens à la planification de la réponse à une attaque de pirates contre un champ pétrolier »,
INFORSID 2012, Montpellier, France, 29-31 mai 2012

1. Introduction

La piraterie maritime moderne représente à l'heure actuelle le risque majeur pour la sécurisation des sites de production énergétique et du transport maritime pétrolier. Sur ces sites les moyens de surveillance présentent des faiblesses majeures au niveau de la détection d'une menace et surtout la procédure à appliquer se révèle souvent inefficace et inadaptée.

Il s'avère donc primordial de disposer d'un nouveau système qui réponde à ce besoin de protection en proposant un système global de lutte contre les actes de piraterie envers les infrastructures pétrolières.

Cet article est organisé en trois parties. La problématique liée aux actes de piraterie contre les champs pétroliers est d'abord présentée. Puis la méthode utilisée pour la planification des contre-mesures préconisées par le système est ensuite décrite précisément, avec notamment, la construction d'un réseau bayésien selon deux principes : l'utilisation de la base de données « piraterie et vol à mains armées » de l'Organisation Maritime Internationale (OMI) et le recueil et la formalisation de connaissances d'experts du domaine. Enfin, les résultats testés sur des scénarios complets et réalistes d'attaques de pirates sont exposés.

2. Définition du problème et objet de la recherche

L'exploitation en mer des ressources pétrolières représente actuellement environ le tiers de la production mondiale de pétrole. Cette ressource énergétique, malgré sa raréfaction, présente de nombreuses zones en voie d'exploration, localisées notamment dans des eaux territoriales à risque, comme dans le Golfe de Guinée et plus particulièrement au large du Nigéria. Depuis 2005 les actes de piraterie contre des champs pétroliers et surtout des navires ne cessent de se multiplier. Bien que les attaques envers les plates-formes pétrolières soient moins fréquentes et surtout moins médiatisées, elles sont extrêmement inquiétantes de par la gravité des conséquences sur l'équipage et l'infrastructure (personnels pris en otage, blessés voire tués, installations dégradées ou détruites) mais aussi sur l'économie (flambées des prix) et l'environnement (marées noires). Ces attaques sont les parfaites illustrations de la faiblesse des dispositifs anti-piraterie actuels. La sécurité des installations pétrolières est à ce jour assurée par des dispositifs dits classiques (identification radio, radar, Système d'Identification Automatique, etc.). Ces derniers, malgré leurs points forts pour l'aide à la détection, ne s'adaptent pas aux différents types de menaces (bateau de pêche, jet ski, tanker, etc.) et leurs efficacités dépendent de nombreux paramètres liés à l'environnement ainsi qu'aux contraintes techniques et opérationnelles.

Bouejla A., Chaze X., Guarnieri F. et Napoli A., 2012 :
« Application des réseaux bayésiens à la planification de la réponse à une attaque de pirates contre un champ pétrolier »,
INFORSID 2012, Montpellier, France, 29-31 mai 2012

Afin de répondre à ce nouveau besoin de protection d'infrastructures civiles vulnérables aux actes de piraterie ou de terrorisme menés à partir de la mer, l'ANR[1] a décidé de financer le projet SARGOS[2]. Ce projet a pour objectif la conception d'un système permettant d'augmenter le degré de protection des infrastructures. Pour cela il doit être capable, en cas d'intrusion confirmée, de générer une alarme et d'enclencher des réactions internes et externes adaptées au niveau de dangerosité de la situation. Les travaux présentés dans cet article concernent la problématique de la planification des réactions et la gestion des moyens internes et externes disponibles sur le champ pétrolier tels que les projecteurs aveuglants ou les alarmes sonores.

Dans cette problématique, on observe un véritable déficit en matière de construction de diagnostic pour la planification de la riposte. Pour lever cette insuffisance, on propose une démarche nouvelle d'élaboration automatique de plans de réaction adaptés à la nature de l'intrusion détectée. Il sera en particulier étudié l'apport de l'inférence bayésienne appliquée d'une part à une base de données existante sur les actes de piraterie et d'autre part aux connaissances d'experts des domaines pétrolier offshore et sûreté maritime.

Ces informations et connaissances sont ensuite modélisées par des réseaux bayésiens, outils fondés sur le théorème de Thomas Bayes (1). Ce théorème est utilisé dans l'inférence statistique pour mettre à jour les estimations d'une probabilité à partir des observations et des lois de probabilité de ces observations.

$$\left(\frac{P(B/A) * P(A)}{P(B)}\right) = P(A/B) \qquad (1)$$

Un réseau bayésien est un système représentant la connaissance et permettant de calculer des probabilités conditionnelles. Très utilisés pour le diagnostic (médical ou industriel) (Lee et Lee, 2006), les réseaux bayésiens permettent de capitaliser et exploiter des connaissances et sont particulièrement adaptés à la prise en compte de l'incertitude (Hudson et al., 2002), (Martín et al., 2009). Pour construire le réseau bayésien, le logiciel BayesiaLab[3] a été utilisé. Cet outil de modélisation des réseaux bayésiens présente de multiples fonctionnalités et une interface graphique intuitive.

[1] L'Agence Nationale de la Recherche finance le projet SARGOS qui regroupe de nombreuses entreprises (DCNS, SOFRESUD, etc.) et centres de recherche (ARMINES / Mines ParisTech-CRC, TESA, etc.).

[2] Système d'Alerte et de Réponse Graduée OffShore.

[3] Le logiciel BayesiaLab est développé par la société française Bayesia (http://www.bayesia.com/).

3. Les étapes de la construction du réseau bayésien pour la planification de la réponse contre une menace

Deux étapes, décrites ci-après, ont été nécessaires à l'élaboration du réseau bayésien du système SARGOS : la construction d'un premier réseau à partir d'une base de données métier existante et la construction du réseau final à partir de connaissances d'experts du domaine.

3.1. *Construction d'un réseau bayésien à l'aide d'une base de données*

La base de données « Piraterie et vol à mains armées » de l'Organisation Maritime Internationale (OMI) est la seule base de données existante contenant un historique (depuis 1994) des attaques de piraterie en milieu maritime. Au 15 juillet 2011, la base contenait 5 502 enregistrements et proposait pour chaque attaque recensée : le nom du bien attaqué, le nombre de pirates, le type d'armement utilisé, les mesures prises par l'équipage afin de se protéger, les conséquences, etc.

Le logiciel BayesiaLab permet alors de générer automatiquement un réseau bayésien et de proposer les relations de dépendances entre les principaux éléments de la base (SûretéGlobale.org, 2008). La figure 1 présente le réseau bayésien construit à partir de la base de données. Le réseau contient une vingtaine de nœuds relatifs notamment au type du navire attaqué, 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.

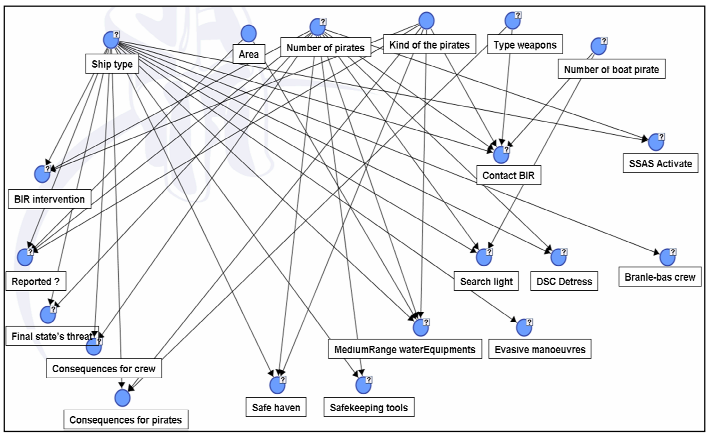

Figure 1. *Réseau bayésien fondé sur les données OMI*

Cette analyse de la base de données a ainsi permis de définir les principales mesures prises par la plupart des entités attaquées : enclencher des manœuvres évasives, activer le Système d'Alerte et de Sûreté Silencieux (SSAS), etc.

Grâce au réseau construit à partir de la base de données « Piraterie et vol à mains armées », il a été ainsi possible de disposer d'une vision très claire sur la tactique des pirates, la nature de l'armement et surtout le nombre de personnes impliquées, de déterminer les principaux outils et mesures utilisés par l'équipage des entités attaquées pour se protéger, d'évaluer l'efficacité de ces outils et de définir les probabilités de certaines occurrences d'attaques.

3.2. *Construction d'un réseau bayésien à l'aide d'une base de connaissances expertes*

Le réseau bayésien OMI ainsi créé avec ses modalités et probabilités conditionnelles, se présente donc comme un cadre formel dans lequel les experts vont venir apporter leurs connaissances pour construire le réseau bayésien SARGOS.

En effet, la seconde étape de la démarche méthodologique a consisté à faire analyser les informations extraites du réseau bayésien OMI par des experts des domaines maritime et pétrolier. La base de données OMI contenant essentiellement des informations relatives aux attaques de navire, les experts ont apporté leurs connaissances pour transposer les résultats du réseau bayésien à un champ pétrolier : des nœuds et des arcs ont ainsi été ajoutés afin de le rendre le plus polyvalent possible.

L'architecture fondamentale du réseau de planification de la réaction SARGOS a été conçue lors de nombreux brainstormings au cours desquels les différents experts maritime et sûreté ont pu partager leurs expériences et discuter des modalités et probabilités du réseau. Cette architecture est constituée de quatre modules et cinq sous-modules (figure 2).

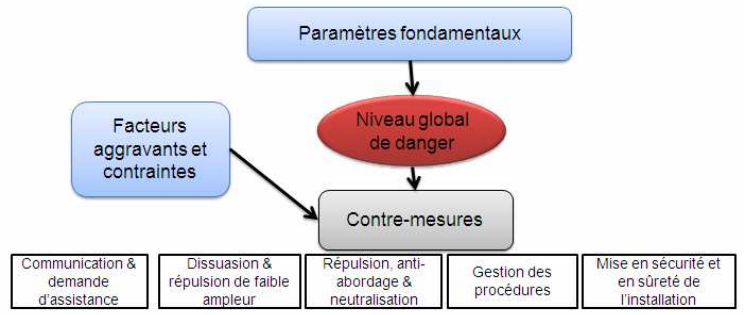

Figure 2. *Structure du Réseau Bayésien SARGOS*

La définition du périmètre de chacun de ces modules est directement liée à la signification des nœuds qui le constituent. 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, sont détaillés ci-après.

Les paramètres fondamentaux sont des données physiques statiques ou dynamiques qui caractérisent la menace et la cible. Elles sont directement issues ou déduites du rapport d'alerte produit par le module de détection du système.

Les facteurs aggravants permettent de prendre en compte le potentiel de détérioration de la situation alors que les contraintes sont des paramètres à considérer obligatoirement pour s'assurer de l'efficacité de la réponse tant sur le plan technique qu'opérationnel.

Le niveau global de danger de la situation est défini à partir des paramètres fondamentaux. L'analyse de la dangerosité globale d'une situation prend en effet en compte le potentiel de nuisance portée par la menace et la vulnérabilité de la cible.

Les contre-mesures sont l'ensemble des moyens de défense mis en œuvre lorsque la cible est attaquée pour revenir au plus vite et dans les meilleures conditions à une situation sûre. Les contre-mesures sont classées en cinq sous-modules selon le niveau de dangerosité de la situation et la disponibilité opérationnelle des appareils embarqués à bord de la cible attaquée. Ces sous-modules sont : la communication et la demande d'assistance ; la dissuasion et la répulsion de faible ampleur ; la répulsion, l'anti-abordage et la neutralisation ; la gestion des procédures ; la mise en sécurité et en sûreté de l'installation.

Dans le réseau bayésien, 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 représente. 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.

4. L'usage de scénarios pour démontrer les apports du Réseau Bayésien

La distribution des probabilités des différentes modalités étant réalisée, le réseau bayésien ainsi élaboré a été testé en jouant différents scénarios d'attaque qui sont traduits au sein du réseau en fixant des observations de manière certaine. L'étude de ces scénarios permet ainsi de finaliser le réseau avant de l'intégrer au système SARGOS.

Afin d'intégrer l'utilisation du réseau bayésien dans le système SARGOS, un prototype intégrant en entrée un rapport d'alerte et générant en sortie un rapport de planification a été développé. Ce plan contient l'ensemble des contre-mesures à appliquer par l'équipage ou automatiquement par le système.

Des calculs intermédiaires sont réalisés pour alimenter le réseau bayésien d'experts via le logiciel BayesiaEngine qui offre une interface d'application (API) et une librairie Java. Via ce module, les paramètres concernant une attaque sont insérés dans le réseau. Les résultats des contre-mesures varient selon les situations, d'où la nécessité de fixer un seuil d'activation pour n'intégrer que les contre-mesures dont la réponse est la plus pertinente à cet instant donné de la situation. Il a été décidé que seules les contre-mesures, intégrées au rapport de planification, dont une des modalités obtient une probabilité strictement supérieure à 70% soient pris en compte dans l'élaboration de la réponse. Ce seuil a été choisi par les experts car il correspond à une réalité dans plus des deux tiers des cas rencontrés. Après de nombreux essais et ajustements, les résultats en sortie du réseau correspondent ainsi à des réponses fiables et réalistes. Une fois que les contre-mesures dont la valeur de la probabilité en sortie du réseau bayésien dépasse le seuil d'activation, sont sélectionnées, elles sont inscrites dans le rapport de planification suivant un ordre d'affichage précis. Les principaux facteurs qui jouent sur cet ordre de priorisation sont : le mode d'action de la contre-mesure, sa facilité de mise en œuvre, l'automatisation poussée ou la nécessité de personnels pour l'activer, le temps nécessaire pour que la contre-mesure soit effectivement efficace, les éventuelles fonctions additionnelles d'une contre-mesure.

Le système SARGOS peut traiter plusieurs menaces au sein d'un seul rapport d'alerte. La première menace à traiter est donc toujours celle qui engendre le temps de réaction le plus faible pour la cible potentielle la plus exposée.

Après l'étape de traitement de la menace, le rapport de planification est partagé en deux parties : d'une part la communication et la demande d'assistance qui concernent l'ensemble du champ pétrolier et d'autre part les cibles spécifiquement mises en danger avec l'affichage, par ordre chronologique d'application, des contre-mesures à activer.

5. Conclusion et perspectives

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 pour 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 du système SARGOS puisque le réseau gère les

Bouejla A., Chaze X., Guarnieri F. et Napoli A., 2012 :
« Application des réseaux bayésiens à la planification de la réponse à une attaque de pirates contre un champ pétrolier »,
INFORSID 2012, Montpellier, France, 29-31 mai 2012

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. La planification de la réponse proposée par SARGOS se traduit en effet par l'émission d'un rapport de planification issu du traitement intelligent des rapports d'alerte successifs traduisant l'évolution de la situation.

Enfin l'évolutivité du réseau est possible par l'intégration des retours d'expériences relatifs aux traitements des attaques qu'il est amené à gérer. Le module de planification est ainsi adapté et amélioré de manière itérative.

6. Bibliographie

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

Giraud M.A., Alhadef B., Guarnieri F., Napoli A., Bottala-Gambetta M., Chaumartin D., Philips M., Morel M., Imbert C.,Itcia E., Bonacci D. et Michel P., 2011 : *« SARGOS : Système d'Alerte et Réponse Graduée Off Shore »*. Conférence WISG, 25-26 janvier 2011 , Troyes, France.

Hudson, Linwood D, Bryan S Ware, Suzanne M Mahoney, et Kathryn Blackmond Laskey. 2002. *« An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners »*. Août 2002. 8p.

ISEMAR. 2010. *« Piraterie: perturbation de l'économie maritime? »*. Mer et marine, octobre 2010.

Lee, Chang-Ju, et Kun Jai Lee. 2006. *« Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal »*. Reliability Engineering & System Safety, volume 91, n°5, mai 2006, p 515-532.

Martín, J.E., T. Rivas, J.M. Matías, J. Taboada, et A. Argüelles. 2009. *« A Bayesian network analysis of workplace accidents caused by falls from a height »*. Safety Science, volumr 47, n°2, février 2009, p 206-214.

Naïm, Patrick, Pierre-Henri Wuillemin, Philippe Leray, Olivier Pourret, et Anna Becker. 2007. *« Réseaux bayésiens »*. 3e éd. Eyrolles.

SûretéGlobale.org. 2008. *« Apport des réseaux bayésiens dans la prévention de la délinquance »*.

Torti L. et Wuillemin P.H.. *« Modélsation de réseaux bayésiens de très grandes tailles »*. Conférence MajecSTIC , 16-18 novembre 2009 , Avignon, France.

Dantu R. et Kolan P. *« Risk management using behavior based bayesian networks »*. Intelligence and Security Informatics , volume 3495, 2005 , p 115-126.

Kannan P.R. *« Bayesian networks: Application in safety instrumentation and risk reduction »*. ISA Transactions , volume 46, n°2, avril 2007 , p 255-259.

Cordonnier I. *« La piraterie en Asie du Sud-Est »*. Revue internationale et stratégique, volume 43, n°3, 2001, 48p.