

Réseaux bayésiens pour la lutte contre la piraterie à l'encontre des plateformes pétrolières en mer

Amal Bouejla, Xavier Chaze, Franck Guarnieri, Aldo Napoli

▶ **To cite this version:**

Amal Bouejla, Xavier Chaze, Franck Guarnieri, Aldo Napoli. Réseaux bayésiens pour la lutte contre la piraterie à l'encontre des plateformes pétrolières en mer. [Rapport de recherche] CRC_WP_2012_4, MINES ParisTech. 2012, 19 p. hal-00772529

HAL Id: hal-00772529

https://minesparis-psl.hal.science/hal-00772529

Submitted on 10 Jan 2013

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.

PAPIERS DE RECHERCHE CRC WORKING PAPERS SERIES

CRC_WP_2012_4

(juin 2012)

RESEAUX BAYESIENS POUR LA LUTTE CONTRE LA PIRATERIE A L'ENCONTRE DES PLATEFORMES PETROLIERES EN MER

Amal Bouejla, Xavier Chaze, Franck Guarnieri, Aldo Napoli

CENTRE DE RECHERCHE SUR LES RISQUES ET LES CRISES
MINES ParisTech
Rue Claude Daunesse CS10207
06904 Sophia Antipolis Cedex
www.crc.mines-paristech.fr

PAPIERS DE RECHERCHE DU CRC

Cette collection a pour but de rendre aisément disponible un ensemble de documents de travail et autres matériaux de discussion issus des recherches menées au CRC (CENTRE DE RECHERCHE SUR LES RISQUES ET LES CRISES).

Tous les droits afférant aux textes diffusés dans cette collection appartiennent aux auteurs.

Des versions ultérieures des papiers diffusés dans cette collection sont susceptibles de faire l'objet d'une publication. Veuillez consulter la base bibliographique des travaux du CRC pour obtenir la référence exacte d'une éventuelle version publiée.

http://hal-ensmp.archives-ouvertes.fr

CRC WORKING PAPERS SERIES

The aim of this collection is to make easily available a set of working papers and other materials for discussion produced at the CRC (CENTRE DE RECHERCHE SUR LES RISQUES ET LES CRISES).

The copyright of the work made available within this series remains with the authors.

Further versions of these working papers may have been submitted for publication. Please check the bibliographic database of the CRC to obtain exact references of possible published versions.

http://hal-ensmp.archives-ouvertes.fr

CENTRE DE RECHERCHE SUR LES RISQUES ET LES CRISES
MINES ParisTech
Rue Claude Daunesse CS 10207
06904 SOPHIA ANTIPOLIS Cedex
www.crc.mines-paristech.fr

Introduction

Plus de sept mille plateformes pétrolières sont actuellement réparties à travers le monde, impliquant chacune 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 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 (en 2011, 552 attaques ont été enregistrées auprès du Bureau Maritime International[1] contre 487 attaques en 2010). Il s'avère donc primordial de disposer d'un système qui assure la sécurité des champs pétroliers et propose une protection adaptée ainsi qu'une gestion efficace en cas de crise.

Le système SARGOS[2], financé par l'ANR[3] et labellisé par le pôle de compétitivité mer PACA[4], répond 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 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 et discutés.

---

1 http://www.icc-ccs.org/home/imb

2 Système d'Alerte et de Réponse Graduée OffShore.

3 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.).

4 http://www.polemerpaca.com/

Piraterie contre les installations pétrolières : une menace avérée et des moyens de défense limités

Les infrastructures pétrolières offshore sont soumises à des risques de piraterie en constante augmentation. Ces actes ont de nombreuses répercussions tant au niveau local, de l'exploitation, que global, de la distribution. L'objet de cette section est de préciser les enjeux économiques mais aussi politiques liés à ces attaques et introduire un contexte en insécurité croissante où les acteurs de l'offshore pétrolier se trouvent démunis, les dispositifs actuels ne permettant pas de protéger efficacement ces infrastructures. Enfin, la présentation du système SARGOS illustre les nouveaux apports attendus pour faire face à cette problématique et ainsi légitimer leurs pertinences.

Des enjeux économiques et politiques

L'activité pétrolière offshore est en forte croissance. L'exploitation en mer des ressources pétrolières représente actuellement environ le tiers de la production mondiale de pétrole. Cette ressource énergétique, malgré sa raréfaction recouvre de nombreuses zones en voie d'exploration certaines étant localisées dans des eaux territoriales à risque. Au large de pays politiquement instables, les attaques menées contre ces infrastructures engendrent des coûts supplémentaires élevés pour le versement des rançons, le paiement des primes d'assurances, l'installation d'équipements de sûreté, etc. Le coût de la piraterie est estimé entre 7 et 12 milliards de dollars par an[5] (BMI, 2011). Ces surcoûts influencent directement le prix du pétrole à l'échelle internationale.

De plus, les champs pétroliers constituent l'interface entre le monde maritime et le monde de l'industrie pétrolière. C'est en fait plus l'hétérogénéité des règles applicables que l'absence de droit qui font du statut juridique des plates-formes pétrolières un puzzle juridique. Cette complexité peut conduire à des conflits politiques entre les états : la société exploitant la plate-forme appartenant à un état différent de celui de son emplacement, se pose alors le problème de la responsabilité de la protection de la zone (ISEMAR, 2010).

L'importance des installations pétrolières sur l'économie et l'industrie mondiale et les conséquences qui peuvent découler de la piraterie obligent donc à augmenter le degré de protection de ces biens.

Des attaques violentes

Bien que les attaques contre les champs pétroliers sont peu fréquentes et surtout peu médiatisées, elles sont extrêmement inquiétantes de par la gravité des conséquences sur l'équipage et l'infrastructure.

---

[5] BMI, « Study: Piracy Costs World Up to $12 Billion Annually », Bureau Maritime International, 14-juill-2011.

Citons à ce titre, les trois exemples d'attaques suivants (Giraud, 2011), :

- Le 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 qui ont pris en otage trois marins français. Il s'agissait de la quatrième attaque contre Bourbon depuis 2009.
- L'attaque de la plate-forme Exxon Mobil, au large des côtes du Nigeria, a engendré l'enlèvement de dix neuf de ses employés et des dégâts importants sur l'installation pétrolière causés par les engins explosifs utilisés par les pirates.
- Enfin le 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.

Les responsables des infrastructures, les employés et les agents de sûreté ne souhaitent plus voir leurs biens détournés faire l'objet de fortes rançons, ni voir des hommes d'équipages blessés, traumatisés voire tués, ou retenus dans des conditions extrêmes durant des jours, des semaines, voire des mois. Les assureurs, quant à eux, se refusent à assurer indéfiniment des risques d'une valeur trop importante. Enfin les états ne veulent plus voir le cours du pétrole impacté par de tels événements.

Des besoins opérationnels émergents

Ces exemples d'attaques sont les parfaites illustrations de la faiblesse des dispositifs anti-piraterie actuellement mis en place. En effet à ce jour, il n'existe pas de système global qui gère toute la chaîne de traitement d'une menace. Les principaux systèmes exploités opèrent indépendamment la détection et la réponse à une menace. Parmi les dispositifs de détection, les systèmes à base de radar (à impulsions[6]) savent repérer des mobiles coopératifs de taille importante ou moyenne mais ils présentent des performances médiocres face aux petites embarcations (de type barque de pêche, canot à moteur, etc.) dans un fouillis de mer et sont de plus relativement lents pour analyser un domaine étendu. Il existe également des systèmes de surveillance optroniques[7] qui, malgré leurs points forts dans la détection à longue portée d'objectifs de petite taille, restent handicapés par les problèmes de réflexion solaire sur la mer et se révèlent très sensibles aux conditions météorologiques. Quant aux dispositifs utilisés pour contrer une attaque, ils sont souvent inappropriés ou mal employés (jets d'eau par exemple).

---

[6] L'antenne du radar émet en direction de la cible des impulsions micro-ondes. Ces signaux sont alors réfléchis puis interceptés par le récepteur du radar, qui recueille ainsi un signal électrique nommé « écho ».

[7] Ces systèmes associant optique et électronique sont composés généralement d'un capteur optique, d'un système de traitement d'images et d'un système d'affichage ou de mémorisation des données.

Concernant la réponse face à une menace, les cibles mises en danger peuvent actuellement envoyer des messages d'alerte aux unités qui se trouvent dans la même zone mais cette diffusion est géographiquement très restreinte. De plus, même si le navire de sûreté et sécurité est prévenu lors d'une menace, son intervention reste incertaine surtout lorsque le navire est très éloigné de la position de l'attaque.

La solution consiste donc à développer et proposer un nouveau système, appelé SARGOS, apte à traiter la menace selon un cycle d'étapes allant de la détection et jusqu'à la planification des contre-mesures non létales (utilisation de canons sonores, condamnation des accès à l'infrastructure, etc.) à appliquer pour éliminer ce danger.

Les apports du système SARGOS

SARGOS répond au besoin de protection d'infrastructures civiles vulnérables aux actes de piraterie ou de terrorisme menés à partir de la mer. Il s'agit d'un système global prenant en compte toute la chaîne de traitement depuis la détection d'une menace potentielle jusqu'à la mise en œuvre de la réaction, en s'intégrant dans les modes de fonctionnement de l'infrastructure pétrolière et en prenant en compte les contraintes réglementaires et juridiques tant nationales qu'internationales.

Le système fait appel à des compétences pluridisciplinaires (développement d'un système de protection global : détection et identification automatiques de menaces, estimation des risques potentiels et gestion d'une réponse adaptée).

Le schéma fonctionnel du système SARGOS (figure 1) décrit le cycle de traitement de la menace. Le principe de fonctionnement du système SARGOS est le suivant : dès que les instruments du module de détection (radar d'alerte FMCW[8], caméra infra-rouge, etc.) repèrent une embarcation dans une zone proche du champ pétrolier, le système évalue la menace et sa potentielle dangerosité en générant un rapport d'alerte qui contient l'ensemble des informations liées à celle-ci. Parmi ces informations, citons par exemple la visibilité, la période de la journée, la vitesse, la longitude et la latitude de l'embarcation détectée et de la cible potentielle, etc. A partir de ces données, la distance entre ces deux entités ainsi que le temps théorique d'intervention du navire de sûreté sont calculés. Lorsque la menace est identifiée comme suspecte ou hostile, le système SARGOS génère un rapport d'alerte toutes les secondes. Ce rapport est utilisé dans l'étape de la planification où des moyens externes et internes pour lutter contre cette attaque sont mobilisés.

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.

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

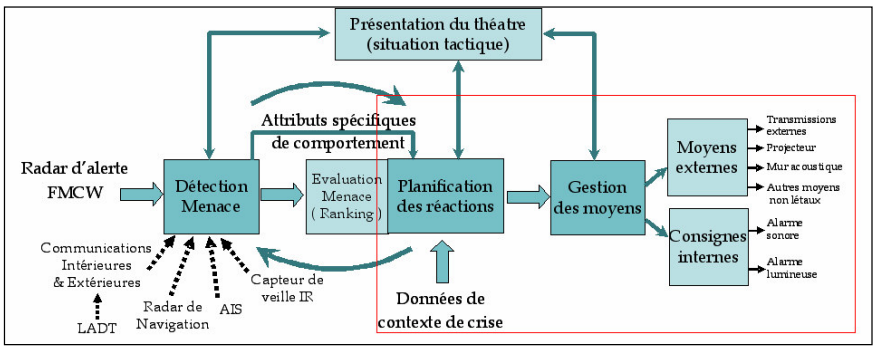


Figure 1. *Schéma fonctionnel du système SARGOS*

Éléments et principes de l'analyse de la menace et de la proposition de gestion des moyens

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 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 le bien attaqué, 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.

Ces deux premières contraintes incitent donc à 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.

Une contrainte supplémentaire à prendre en compte est l'incertitude des informations relatives à une menace. Le système SARGOS génère 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 (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 du bien attaqué, etc.). 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.

Cette contrainte d'incertitude inhérente met l'accent sur la nécessité d'utiliser un système s'appuyant sur la théorie des probabilités et les calculs probabilistes.

En prenant en compte ces deux principes dans le raisonnement, une démarche d'élaboration automatique de plans de réaction adaptés à la nature de l'intrusion détectée fondée sur les réseaux bayésiens est ainsi proposée.

Le réseau bayésien est utilisé dans le processus de planification de la réponse qui a pour but de mettre au point une « riposte » adaptée, graduée et évolutive face à une menace. Les informations contenues dans une base de données et les raisonnements d'experts des domaines maritime et pétrolier sont mis en commun pour combler les manques de connaissances a priori de l'objet considéré et de retour d'expérience dans le domaine applicatif.

Ces informations et connaissances sont ensuite modélisées par des réseaux bayésiens, outils fondés sur le théorème de Thomas Bayes (1), résultat de base en théorie des probabilités.

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

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, 2006), les réseaux bayésiens permettent de capitaliser et exploiter des connaissances et sont particulièrement adaptés à la prise en compte de l'incertitude (Hudson, 2002), (Martín, 2009). Pour construire le réseau bayésien, le logiciel BayesiaLab[9] a été utilisé. Cet outil de modélisation des réseaux bayésiens présente de multiples fonctionnalités et une interface graphique intuitive.

Couplage des connaissances quantitatives et qualitatives pour la construction d'un réseau bayésien d'aide à la planification de la réponse

L'idée principale adoptée pour la construction du réseau bayésien de planification des réponses contre une menace de piraterie, est de se baser sur le couplage entre les connaissances quantitatives issues de la base de données "piraterie et vol à main armées" de l'Organisation Maritime Internationale[10] (OMI) et les connaissances qualitatives acquises auprès des experts du domaine maritime.

La première étape est de construire un réseau bayésien à partir des enregistrements liés aux attaques contre les navires et les plateformes dans le monde alors que la deuxième étape consiste à exploiter les connaissances expertes afin d'affiner les résultats et d'ajouter des contre-mesures de riposte.

---

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

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

Construction d'un réseau bayésien à l'aide des connaissances quantitatives

La base de données « Piraterie et vol à mains armées » de l'Organisation Maritime Internationale (OMI) a été exploitée. C'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 personnes participant à l'attaque, le type d'armement utilisé, les mesures prises par l'équipage afin de se protéger, les conséquences sur l'équipage et sur les pirates, 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). Parmi les méthodes d'apprentissage non supervisé disponibles algorithmes de segmentation des données ou de caractérisation du nœud cible par exemples), un algorithme de découverte d'associations a été choisi car il proposait la modélisation la plus pertinente.

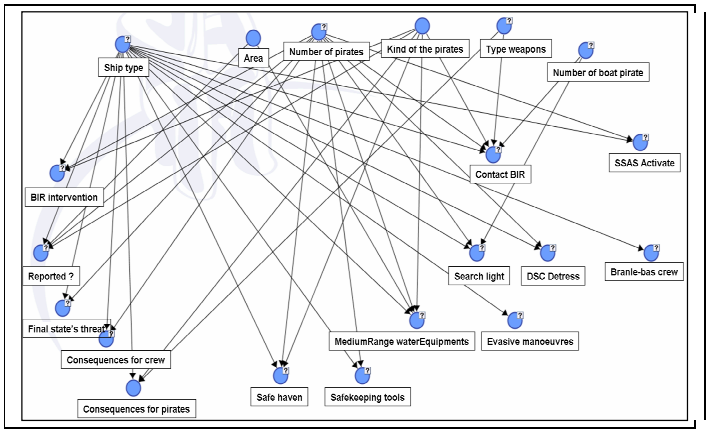


Figure 2. Réseau bayésien fondé sur les données OMI

La figure 2 présente le réseau bayésien construit à partir de la base de données. Certaines informations comme la longitude, la latitude, le nom du bien attaqué, etc. ont été éliminées. Ce choix est dû au fait que ces champs ne sont pas mentionnés pour toutes les attaques. 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, ceci est dû à l'absence de contrôles de sécurité ; les pirates profitent aussi souvent de leurs nombres : 68% des attaques sont organisées par des équipes de pirates composées de plus de 5 personnes.

Grâce à ce réseau, une vision très claire sur la tactique des pirates, la nature de l'armement et surtout le nombre des personnes impliquées est désormais disponible.

Dans l'exemple ci-dessous, des modalités spécifiques pour les nœuds caractérisant la menace ont été fixées afin d'identifier les contre-mesures utilisées par l'équipage de la cible attaquée. La figure 3 illustre ainsi les hypothèses choisies :

- Le bien attaqué : un tanker
- La position de l'accident : eaux internationales
- Type des attaquants : des voleurs
- Type d'armement : des personnes armées

Le réseau bayésien indique dans ce cas précis, comme dans la majorité des cas, que les assaillants ont tiré des coups de feu sur la cible potentielle et que l'équipage, pour se protéger de ce danger, a essayé d'appliquer des manœuvres évasives et de projeter des jets d'eau sur les attaquants.

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), contacter le navire de sûreté, mettre l'équipage en sécurité, activer les projecteurs, etc.

Grâce au réseau construit à partir de la base de données « Piraterie et vol à mains armées », il a donc été possible 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.

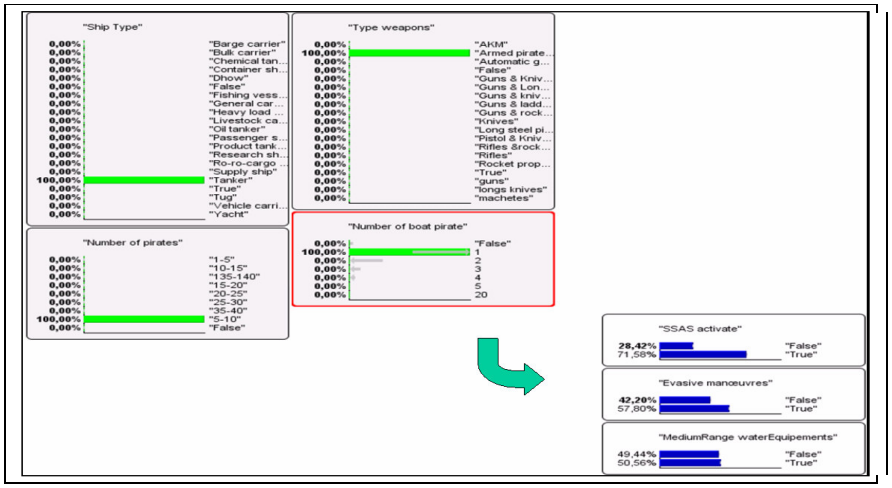


Figure 3. Cas d'une attaque contre un tanker

Couplage du réseau bayésien basé sur les données de l'OMI avec les connaissances qualitatives des experts maritimes

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 (Hudson, 2002).

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. Le réseau bayésien est donc unique pour les deux grandes catégories de cible (navire ou plate-forme), les variables en entrée du réseau sont identiques quelle que soit la nature de cette cible (type du navire de la menace, sa cinématique, etc.). Cependant les contre-mesures préconisées par le réseau bayésien sont adaptées au type de la cible attaquée (par exemple : les manœuvres évasives ne sont pas proposées pour une plate-forme).

La conception de ce nouveau réseau bayésien adapté aux contraintes et conditions liées aux plates-formes pétrolières s'est faite 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 (Chaze, 2012) et (Bouejla, 2012)..

Cette complémentarité entre les informations contenues dans la base de données OMI et les raisonnements d'experts des domaines maritime et sûreté offshore a permis de générer le réseau de planification de la réaction SARGOS, dont l'architecture est constituée de quatre modules et cinq sous-modules (figure 4).

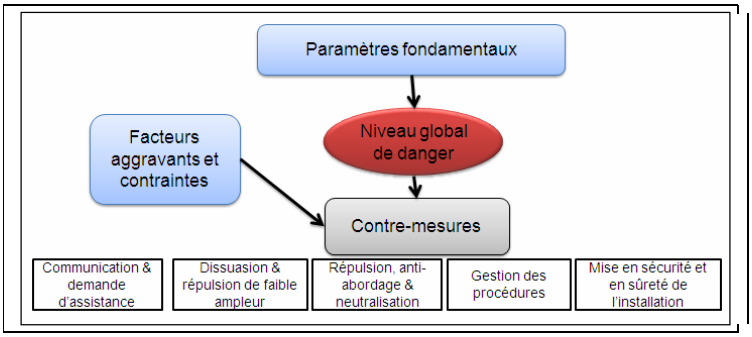


Figure 4. *Structure du Réseau Bayésien SARGOS*

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, détaillés ci-après.

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. Elles constituent une forme de modélisation minimale nécessaire mais suffisamment pertinente pour permettre une pleine appréhension du couple menace / cible dans la problématique de réponse face à l'agression. Parmi ces données, 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. Dans ce nœud sont définies quatre modalités : critique, majeur, important ou autre.

Le niveau global de danger de la situation

Il est calculé 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 fonctionne par niveaux de 1 pour le moindre à 4 pour le pire. Ce niveau et la planification des contre-mesures sont en permanence adaptés à chaque situation.

Les facteurs aggravants et les contraintes

Les facteurs aggravants et les contraintes sont des éléments internes et externes au système.

Les facteurs aggravants permettent de prendre en compte le potentiel de détérioration de la situation et donc d'anticiper sur l'éventuelle orientation à donner à la planification. Ils représentent l'environnement : la visibilité « Visibility » et la période de la journée « PeriodOfDay ».

Les contraintes sont représentées par des paramètres qui traduisent l'efficacité de la réponse tant sur le plan technique qu'opérationnel. Les contraintes techniques sont directement liées à la facilité d'utilisation des contre-mesures comme la disponibilité immédiate d'un effecteur « ImmediateReadiness » ou son possible contrôle à distance « RemoteControlled ».

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 de moyens et d'actions pour normaliser au plus vite la situation de la cible attaquée.

Ces contre-mesures sont partagées en cinq sous-modules qui traduisent la notion même de gradation de la réponse en proposant une hiérarchisation d'ampleur croissante selon la nature de la menace détectée : 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, détaillés ci-après.

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 d'avertir à différentes échelles d'intervention les 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.). Cette communication permettra aux installations et navires du champ pétrolier d'anticiper sur leur plan de réponse et de demander si possible une intervention extérieure.

La dissuasion et la répulsion de faible ampleur ont pour but de faire savoir aux attaquants que la cible connait leurs intentions, qu'elle est capable de les suivre et qu'ils n'ont aucun intérêt à passer à l'action. La répulsion de faible ampleur est la capacité de la cible à pouvoir repousser l'attaque 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).

La répulsion, l'anti-abordage et la neutralisation constituent des contre-mesures actives avec impact fort et dont la fonction principale est au moins l'atténuation si ce n'est la neutralisation des attaquants. Dans le nœud des dispositifs répulsifs « Engage Repellent Equipement », sont regroupés les matériels de plus en plus nombreux sur le marché de l'anti-piraterie maritime qui assurent la répulsion à distance d'un assaut tout en restant dans le cadre de la légitime défense non létale. De même que pour les équipements de répulsion, les équipements anti-invasions ont pour fonction principale d'empêcher les attaquants de monter à bord lorsqu'ils se trouvent à proximité de l'installation ou du navire. Le rôle du « Set Crowd Control 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 est composée de deux contre-mesures. D'une part, 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. D'autre part, le nœud « Asset Assault Management » permet dans chaque cas une gestion de la cible potentielle en termes de mise en sécurité et sûreté. Les modalités de ce nœud sont : activer le mode citadelle, effectuer des manœuvres évasives pour les cas des unités mobiles et navires, et déclarer le poste de sûreté qui est un ensemble de procédures individuelles que devra appliquer chaque membre de l'équipage le cas échéant.

Comme pour la gestion des procédures, SARGOS propose une mise en sécurité et en sûreté de l'installation au sein de la planification à travers 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.

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.

Les probabilités des nœuds fondamentaux sont ici normalisées puisque aucun élément caractérisant une attaque précise n'a été inséré. La distribution de probabilité initiale d'activation du canon sonore ("Activate LRAD") est alors ainsi répartie : inactif ("stand-by") : 99,51%, haut-parleurs ("LRAD Loudspeaker") : 0,27% et canon sonore ("LRAD Sonic Weapon") : 0,22%.

Démonstration de l'apport du réseau bayésien et discussion des résultats

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.

Etude de scénarios d'attaques

L'exemple ci-dessous (figure 5) présente les résultats liés à l'insertion des paramètres d'une attaque d'une unité flottante de production, de stockage et de déchargement (Floating Production, Storage and Offloading [unit], FPSO) par un navire inconnu.

Cet exemple montre que le niveau de dangerosité de la situation est "2" avec un pourcentage de réalisation de 64,68%. Dans ce cas les contre-mesures à appliquer sont : informer le maître de l'équipage, demander l'intervention du navire de sûreté, émettre un message fort et clair à longue portée via le haut parleur, activer le projecteur lumineux, engager le poste de sûreté et activer les équipements de répulsion.

La planification est adaptée au niveau de dangerosité de la situation et change suivant l'évolution des paramètres de la menace et de la cible.

La génération de différents exemples d'attaques, permet d'affiner les probabilités et de tester la réaction du réseau bayésien en changeant les paramètres relatifs à la menace, la cible, l'environnement, etc.

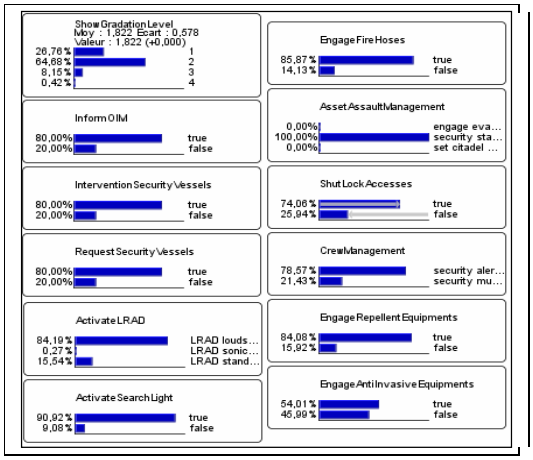


Figure 5. *Résultat de la planification des réactions suite à l'insertion d'une attaque élaborée par une piste inconnue*

Intégration du réseau bayésien dans le système SARGOS

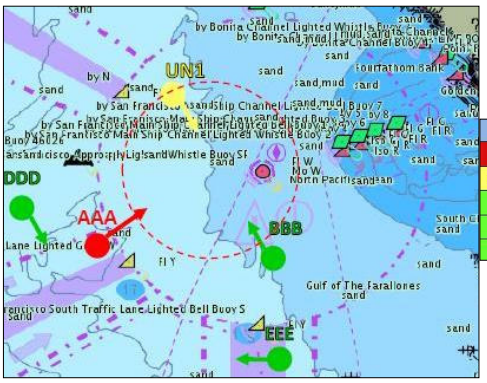
Afin d'intégrer l'utilisation du réseau bayésien dans le système SARGOS, un prototype intégrant en entrée un rapport d'alerte et générant en sortie un rapport de planification a été développé. Ce plan contient l'ensemble des contre-mesures à appliquer par l'équipage ou automatiquement par le système.

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. La figure 6 présente l'interface homme-machine du système SARGOS et la multiplicité des menaces traitées simultanément.



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 6. *Hiérarchisation des menaces dans l'interface homme-machine du système SARGOS*

Dans cet exemple, le système détecte l'ensemble des cibles qui se dirige vers le champ pétrolier et les classe selon un type "Enemy","Unknown" ou "Friend". L'alerte est générée dans les cas de classification en "Enemy" et "Unknown" seulement. 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 (cf. figure 7).

La séparation verticale visible uniquement dans cet exemple pour la demande d'intervention du navire de sûreté représente la valeur de la probabilité résultante.

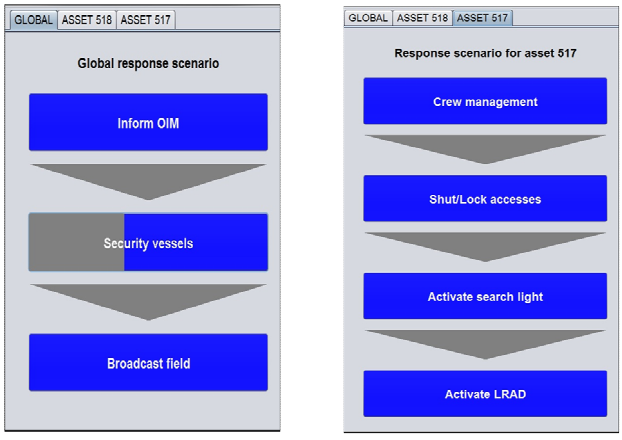


Figure 7. *Affichage dans l'interface homme-machine du système SARGOS des contre-mesures globales (successivement : informer le maître de l'équipage, demander l'intervention du navire de sûreté et informer l'ensemble du champ) et spécifiques (regrouper l'équipage, fermer les accès à l'infrastructure, activer les projecteurs et activer le canon sonore) à appliquer.*

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 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.

L'évolutivité du réseau est également 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.

Enfin, dans le but d'améliorer la modélisation des connaissances intégrées au réseau bayésien SARGOS, il serait intéressant de pouvoir s'appuyer sur une ontologie adaptée (Vandecasteele, 2012). En effet, l'exploitation d'une ontologie permettrait de formaliser les connaissances en amont du réseau bayésien afin de consolider les étapes de détection et d'identification d'une menace.

Références

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.

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

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

Lee, Chang-Ju, & 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, May 2006, p 515-532.

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

Patrick N, Wuillemin P.H, Leray P, Pourret O, & Becker A. 2007. *Réseaux bayésiens,* 3e éd. Eyrolles.

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

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

Chaze X., Bouejla A., Guarnieri F. & Napoli A. *The contribution of Bayesian networks to risk management in oil field piracy,* ITEMS2012, 15 April 2012 , Busan, South Korea.

Bouejla A., Chaze X., Guarnieri F. & Napoli A. *Bayesian networks in the management of oil field piracy risk,* ITEMS2012, 15 April 2012, Busan, South Korea.

Vandecasteele A. & Napoli A. *Spatial ontologies for detecting abnormal maritime behaviour,* OCEANS2012, 2012, Yeosu, South Korea.

Torti L. & Wuillemin P.H.. *Modélisation de réseaux bayésiens de très grandes tailles,* MajecSTIC , 16-18 November 2009 , Avignon, France.

Dantu R. & 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, April 2007 , p 255-259.

RESEAUX BAYESIENS POUR LA LUTTE CONTRE LA PIRATERIE A L'ENCONTRE DES PLATEFORMES PETROLIERES EN MER

Mots clefs : réseaux bayésiens, piraterie, plates-formes pétrolières en mer

Résumé

Depuis quelques années, les attaques de pirates à l'encontre des plateformes pétrolières en mer se multiplient. Afin de réduire la vulnérabilité de ces infrastructures critiques, les opérateurs convoquent les nouvelles technologies de l'information et de la communication. C'est dans ce cadre que les chercheurs du CRC de Mines ParisTech ont conçu et développé un prototype de réseau bayésien pour détecter les menaces.

Amal Bouejla
MINES ParisTech
Amal.bouejal@mines-paristech.fr

Xavier Chaze
MINES ParisTech
xavier.chazel@mines-paristech.fr

Franck Guarnieri
MINES ParisTech
franck.guarnieri@mines-paristech.fr

Aldo Napoli
MINES ParisTech
aldo.napoli@mines-paristech.fr

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