HAL
open science

Conception d'un réseau bayésien pour la prévention du risque de piraterie contre les champs pétroliers

Amal Bouejla, Xavier Chaze, Franck Guarnieri, Aldo Napoli

To cite this version:

Amal Bouejla, Xavier Chaze, Franck Guarnieri, Aldo Napoli. Conception d'un réseau bayésien pour la prévention du risque de piraterie contre les champs pétroliers. 6èmes Journées Francophones sur les Réseaux Bayésiens - JFRB 2012 - IEEE, May 2012, Îles Kerkennah, Tunisie. 6 p. hal-00734358

HAL Id: hal-00734358

https://minesparis-psl.hal.science/hal-00734358

Submitted on 21 Sep 2012

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.

Conception d'un réseau bayésien pour la prévention du risque de piraterie contre les champs pétroliers

Amal BOUEJLA, Xavier CHAZE, Franck GUARNIERI, Aldo NAPOLI
Mines ParisTech
CRC - Centre de recherche sur les Risques et les Crises
Sophia Antipolis, France
{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 et 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.**

Mots-clés - pirates; plates-formes pétrolières; menace; réseaux bayésiens

I. 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 [1]. 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, 439 attaques ont été enregistrées auprès du Bureau Maritime International[1]). 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 de la 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 [2].

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.

II. DEFINITION DU PROBLEME ET OBJET DE LA RECHERCHE

Les infrastructures pétrolières offshore sont soumises à des risques de piraterie en constante augmentation. Ces actes ont de nombreuses répercussions. Pour exemple, l'attaque contre la plate-forme pétrolière Exxon Mobil en 2010 au large du Nigeria s'est soldée par l'enlèvement de dix neuf membres d'équipage et la réduction de 45.000 barils de sa production pétrolière quotidienne ce qui a engendré une montée des prix à l'échelle internationale. 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, 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.

A. Des enjeux économiques et sécuritaires

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 les infrastructures offshore engendrent des coûts supplémentaires élevés pour le versement des rançons, le paiement des primes d'assurances, l'installation d'équipements de sûreté, etc. Ces surcoûts influencent directement le prix du pétrole à l'échelle internationale [3].

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 [4], se pose alors le problème de la responsabilité de la protection de la zone. L'importance des installations

---

[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/

Bouejla A., Chaze X., Guarnieri F. et Napoli A., 2012 :
« Conception d'un réseau bayésien pour la prévention du risque de piraterie contre les champs pétroliers »,
Conférence internationale IEEE JFRB 2012 (6èmes journées francophones sur les Réseaux Bayésiens), Iles Kerkennah, Tunisie, 11-13 mai 2012

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.

B. Des besoins opérationnels émergents

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 due à la faiblesse des dispositifs anti-piraterie actuels. 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[5] peuvent repérer des mobiles 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[6] 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).

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 une zone 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 l'unité offshore attaquée.

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

C. Les apports du système SARGOS

SARGOS répond au besoin de protection des champs pétroliers naturellement 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. Afin de développer ce système de protection global, des compétences pluridisciplinaires sont combinées : 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. Dès que le radar d'alerte FMCW[7] détecte une cible, 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 sera utilisé dans l'étape de la planification où des moyens externes et internes pour lutter contre cette attaque seront utilisés.

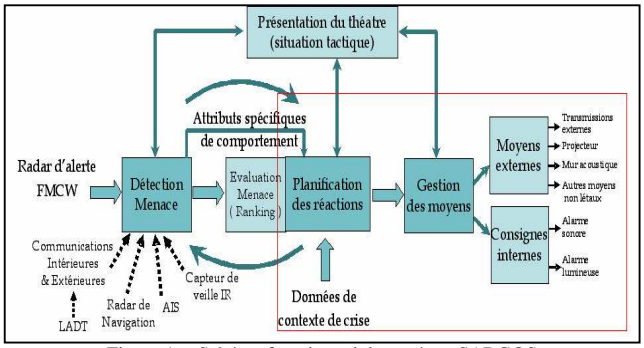

Figure 1. Schéma fonctionnel du système SARGOS

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.

D. Eléments 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 des difficultés liées à l'exploitation d'un 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 [4]. La seconde contrainte réside donc dans la gestion de ces nombreuses

---

[5] 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 ».

[6] 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.

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

relations de dépendance 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 ou les caméras infrarouges (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.

En prenant en compte ces deux concepts dans le raisonnement, les réseaux bayésiens se présentent donc comme une solution appropriée à l'élaboration automatique de plans de réaction adaptés à la nature de l'intrusion détectée [5] [6] [7].

Un réseau bayésien est un système représentant la connaissance et permettant de calculer des probabilités conditionnelles [8]. Très utilisés pour le diagnostic (médical ou industriel), les réseaux bayésiens, outils fondés sur le théorème de Thomas Bayes (1), résultat de base en théorie des probabilités [9] [10], permettent de capitaliser et exploiter des connaissances et sont particulièrement adaptés à la prise en compte de l'incertitude.

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

Le réseau bayésien est ainsi 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 [11] [12].

Pour construire le réseau bayésien SARGOS, le logiciel BayesiaLab[8] a été utilisé [13]. Cet outil de modélisation des réseaux bayésiens présente de multiples fonctionnalités et une interface graphique intuitive.

III. LES ETAPES DE LA CONSTRUCTION DU RESEAU BAYESIEN POUR LA PLANIFICATION DE LA REPONSE CONTRE UNE MENACE

Pour combler le manque de connaissances a priori et de retour d'expérience dans le domaine de la piraterie offshore, deux étapes, décrites ci-après, ont été nécessaires : la construction d'un premier réseau à partir d'une base de données existante et la construction du réseau final à partir de connaissances d'experts du domaine. L'élaboration du réseau bayésien du système SARGOS est donc le fruit de la complémentarité de ces deux ressources de connaissances [14] [15].

A. *Contruction 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) a été exploitée. C'est la seule base de données existante contenant un historique (depuis 1994) des actes de piraterie en milieu maritime. Au 15 juillet 2011, la base contenait 5 502 enregistrements (dont 3 seulement concernent des plates-formes pétrolières) et proposait pour chaque attaque recensée un rapport détaillée contenant : 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.

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 ; plus de 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 : 60,49% des attaques sont organisées par des équipes de pirates composées de plus de 5 personnes, etc.

Le logiciel BayesiaLab a été utilisé afin de générer automatiquement un réseau bayésien et de proposer les relations de dépendances entre les principaux éléments de la base. Parmi les méthodes d'apprentissage non supervisé disponibles, les experts ont utilisé un algorithme de découverte d'associations car il proposait la modélisation la plus pertinente.

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 renseignés 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 identifiées par apprentissage automatique.

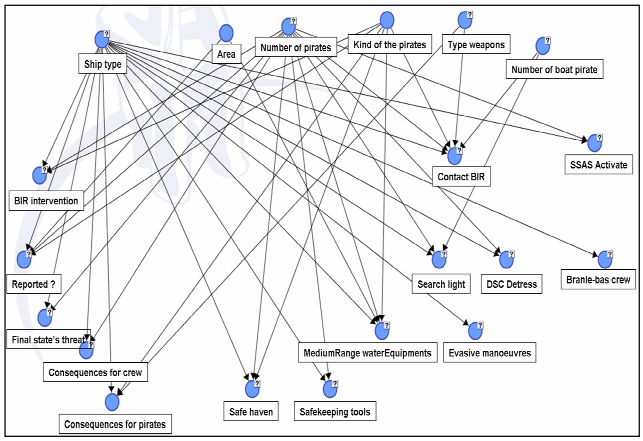

Figure 2. Réseau bayésien fondé sur les données OMI

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

Grâce au réseau construit à partir de la base de données, il a été ainsi possible de disposer d'une vision très claire de la tactique des pirates, la nature de l'armement et surtout du 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.

Cette analyse de la base de données « Piraterie et vol à mains armées » a ainsi permis de définir précisément les principales contre-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.

B. Complémentarité des connaissances extraites du réseau bayésien OMI et des connaissances expertes dans la construction du réseau bayésien SARGOS

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. 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 (ex : les manœuvres évasives ne sont pas proposées pour une plate-forme). La conception de ce nouveau réseau bayésien s'est faite lors de nombreux brainstormings au cours desquels les différents experts ont pu partager leurs expériences et discuter des modalités et probabilités du réseau.

Les différents scénarios d'attaques envisagés et l'étude des réactions préconisées par le réseau permettent ensuite d'affiner les probabilités des modalités des noeuds.

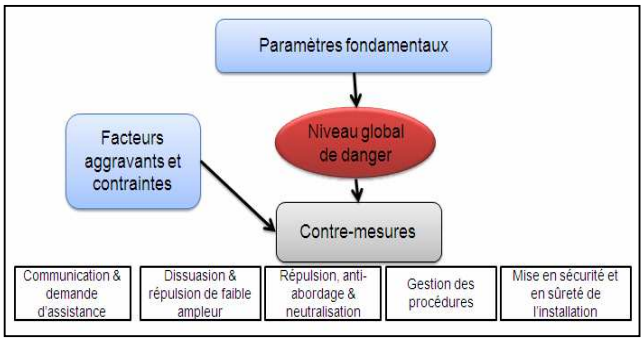

Figure 3. Structure du réseau bayésien SARGOS

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 3).

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.

C. Description du réseau bayésien SARGOS

Le réseau bayésien SARGOS se compose d'une quarantaine de nœuds et d'une centaine de liaisons. 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 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.

1) Les paramètres fondamentaux

Ce sont des données 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 (suspecte ou hostile), la distance entre la menace et la cible, la criticité de la cible, etc. Dans ce nœud sont définies quatre modalités : critique, majeur, important ou autre.

2) Le niveau global de danger de la situation

Il est élaboré à partir des paramètres fondamentaux pour définir la gradation de dangerosité globale de la situation. 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.

3) 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 et la période de la journée.

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 ou son possible contrôle à distance.

4) 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. Les contre-mesures sélectionnées s'adaptent au niveau de danger, aux variables environnementales et aux disponibilités techniques et opérationnelles. 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) 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, mettre en œuvre le Système d'Alerte de Sûreté Silencieux, 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. Par exemple, 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%.

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 la 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 le 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.

IV. L'USAGE DE SCENARIOS POUR DEMONTRER LES APPORTS DU RESEAU BAYESIEN

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.

A. Etude de scénarios d'attaques

Prenons l'exemple 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. Le réseau bayésien évalue le niveau de dangerosité de la situation à "2" avec un pourcentage de réalisation de 64,68% et préconise les contre-mesures suivantes : 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.

B. Intégration du réseau bayésien dans le système SARGOS

Afin d'intégrer le réseau bayésien dans le système SARGOS, un module 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 des contre-mesures dont la réponse est la plus pertinente à un instant donné. Il a été décidé que seules les contre-mesures dont une des modalités obtient une probabilité strictement supérieure à

70% seront préconisées dans le rapport de planification. 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 les contre-mesures 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 à son efficacité, les éventuelles fonctions additionnelles d'une contre-mesure. 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 des contre-mesures par ordre chronologique d'activation (cf. figure 4). La probabilité d'activation de chaque contre-mesure est représentée graphiquement par une barre d'état de couleurs (exemple ci-dessous avec la contre-mesure « Security vessels »).

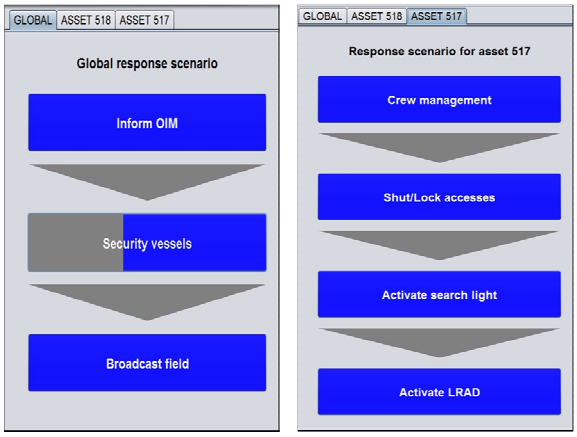

Figure 4. Affichage dans l'interface homme-machine du système SARGOS des contre-mesures globales (successivement : informer le maître de l'équipage, demander l'intervention du navire de sûreté et informer l'ensemble du champ) et spécifiques (regrouper l'équipage, fermer les accès à l'infrastructure, activer les projecteurs et activer le canon sonore) à appliquer.

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.

V. 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. De plus il s'adapte en temps réel à l'évolution du niveau de danger de la situation tout en tenant compte de l'incertitude liée aux données en entrée du système. La planification de la réponse proposée par SARGOS se traduit 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.

REFERENCES

[1] N. Boudong, « La piraterie maritime moderne », Faculté de droit de science politique d'Aix-marseille, Mémoire de master 2 professionnel droit maritime et des transports, 2009.

[2] M. A. Giraud, B. Alhadef, F. Guarnieri, A. Napoli, M. Bottala Gambetta, D. Chaumartin, M. Philips, M. Morel, C. Imbert, E. Itcia, D. Bonacci, et P. Michel, « SARGOS : Système d'Alerte et Réponse Graduée Off Shore », presented at the WISG2011, Troyes, 2011.

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

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

[5] L. D. Hudson, B. S. Ware, S. M. Mahoney, et K. Blackmond Laskey, « An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners », p. 8, août 2002.

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

[7] K. Palaniappan R., « Bayesian networks: Application in safety instrumentation and risk reduction », *ISA Transactions*, vol. 46, n°. 2, p. 255–259, avr. 2007.

[8] Y. Y. Bayraktarli et M. H. Faber, « Bayesian probabilistic network approach for managing earthquake risks of cities », *Georisk: Assessment and Management of Risk for Engineered Systems and Geohazards*, vol. 5, n°. 1, p. 2–24, 2010.

[9] P. Naïm, P.-H. Wuillemin, P. Leray, O. Pourret, et A. Becker, *Réseaux bayésiens*, 3e éd. Eyrolles, 2007.

[10] P. Leray, « Réseaux bayésiens : apprentissage et modélisation de systèmes complexes », Habilitation à dériger les recherches, INSA, Rouen, 2006.

[11] C.-J. Lee et K. J. Lee, « Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal », *Reliability Engineering & System Safety*, vol. 91, n°. 5, p. 515–532, mai 2006.

[12] S. L. Scott, « A Bayesian paradigm for designing intrusion detection systems », *Computational Statistics & Data Analysis*, vol. 45, n°. 1, p. 69–83, 2004.

[13] S. Ammar et P. Leray, « Etude comparative des outils manipulant les réseaux bayésiens », Université de Nantes, Nantes, 7, 2006.

[14] A. Bouejla, X. Chaze, F. Guarnieri et A. Napoli, « Bayesian networks in the management of oil field piracy risk », Risk Analysis'12, Croatie, 19 - 21 septembre 2012.

[15] X. Chaze, A. Bouejla, F. Guarnieri et A. Napoli, « The contribution of Bayesian networks to manage risks of maritime piracy against oil offshore fields », ITEMS'12, Corée de sud, 15 avril 2012.