Mesure de la confiance dans les systèmes d'information : application aux données de navires

Benjamin Costé*, Cyril Ray**
Gouenou Coatrieux***

*Chaire de Cyber Défense des Systèmes Navals
École Navale - CC 600
29240 Brest Cedex 9, FRANCE
benjamin.coste@ecole-navale.fr
**Institut de Recherche de l'École Navale
École Navale - CC 600
29240 Brest Cedex 9, FRANCE
cyril.ray@ecole-navale.fr
***Institut Mines-Télécom - Télécom-Bretagne
Technopole Brest-Iroise, CS 83818
29238 Brest Cedex 3, FRANCE
gouenou.coatrieux@telecom-bretagne.eu

Résumé. Ces dernières années, la prolifération rapide des capteurs et des objets communicants de tous types a significativement enrichi le contenu des systèmes d'information. Cependant, cela suscite de nouvelles questions quant à la confiance que l'on peut accorder aux informations et aux sources d'informations. En effet, ces sources peuvent être leurrées ou sous l'emprise d'un tiers qui falsifie ou altère les informations. Cet article propose donc d'aborder la sécurité des systèmes d'informations sous l'angle de la confiance dans les sources d'informations.

En premier lieu, la définition puis l'évaluation de la confiance dans un réseau hétérogène sont introduits. Une modélisation des sources est ensuite proposée. La confiance dans ces sources d'informations est abordée au travers de deux caractéristiques : la compétence et la sincérité. L'extraction de la confiance est réalisée via un ensemble de mesures de ces deux caractéristiques. Une expérience basée sur plusieurs sources simulées à partir d'un jeu de données réelles montrent la pertinence de l'approche; approche qui peut être transposée à d'autres systèmes d'information. Cette étude est appliquée à l'analyse des données de navigation et de positionnement d'un navire.

1 Introduction

Les systèmes d'information (SI) produisent puis stockent, analysent, traitent et diffusent de nombreuses informations. Lorsqu'il s'agit de SI à bord des navires, ces informations renseignent le système sur son environnement (informations géographiques, météorologiques, etc.) aussi bien que sur son état interne (par ex. alimentation, température, orientation). Ces renseignements sont produits par diverses sources qui peuvent être des capteurs (par ex. GPS, gyroscope), des équipement industriels (automates, actionneurs ...), des outils informatiques classiques (routeurs, switchs, ordinateurs personnels, serveurs etc.), des logiciels (IHM, microcodes, noyau ...) ou même des humains (administrateur, opérateur ...). Les multiples informations produites par les sources assurent la sécurité du navire. Ces informations sont susceptibles d'être altérées à chaque étape des traitements dont elles font l'objet, depuis l'observation d'un phénomène physique à la réception par le système. Divers moyens existent pour garantir l'intégrité de l'information : codes correcteurs d'erreurs, fonctions de hachage, codes d'authentification de message, tatouage de données, etc. . Toutefois, ces solutions sont limitées quand une source est leurrée ou sous l'emprise d'un tiers malveillant. Se pose alors la question de savoir quelle confiance accorder tant aux sources qu'aux informations elles-mêmes.

Cet article aborde la sécurité des systèmes d'information sur la base de la confiance qu'ils peuvent avoir de leur environnement. La confiance est une notion complexe qui permet de raisonner en présence d'incertitudes (Abdul-Rahman et Hailes, 2000). Dans un contexte de sécurité d'un SI, pouvoir mesurer la confiance en son sein nous semble donc adapté pour gérer l'absence de preuve formelle de compromission du SI et ainsi d'être capable de faire face à des attaques inconnues a priori. Nous proposons donc une définition de la confiance et une mesure de celle-ci réalisée à partir de l'analyse des multiples informations reçues, collectées et manipulées par le système. Cette mesure est dépendante des caractéristiques intrinsèques d'une source mais également de l'évolution des informations qu'elle transmet, au regard des données transmises par les autres sources du système d'information.

Le reste de cet article est organisé comme suit. La Section 2 présente plusieurs définitions et mesures de confiance existantes. Les Sections 3 et 4 développent une modélisation des sources d'informations puis un ensemble de mesures de la confiance fondées sur ce modèle. Avant de conclure, la Section 5 expose des résultats expérimentaux appliqués aux navires.

2 Modèles de confiance

Divers modèles de confiance existent. Tandis que certains cherchent à définir cette notion complexe (Demolombe, 2004) d'autres tentent de la mesurer (Capra et Musolesi, 2006).

Les définitions de la confiance proposées jusqu'à aujourd'hui concernent de multiples domaines (Blomqvist, 1997; McKnight et Chervany, 2000). Bien qu'originellement étudiée pour appréhender les rapports entre individus (Lewis et Weigert, 1985), la confiance est de plus en plus considérée dans le cadre des nouveaux moyens de communication qui mélangent humains et services (Grandison et Sloman, 2000). De manière assez générale, la confiance dans une source peut être exprimée à partir de multiples critères intrinsèques à cette dernière ou non (par ex. risques ou menaces auxquels cette source est soumise). Pour une source d'information, la confiance que le système lui accorde peut être définie comme étant fonction de sa *compétence* et de sa *sincérité* (Paglieri et al., 2014; Liu et Williams, 2002). Grandison et Slo-

man (2000) définissent la compétence comme "la capacité d'une source à assurer les fonctions qui lui sont attribuées". Ainsi, une source n'est pas compétente si elle commet des erreurs car celles-ci témoignent de son incapacité à informer le système d'information sur son environnement. De même, une source est sincère "si elle croit vraie les informations qu'elle transmet" (Demolombe, 2001). Une source malveillante est donc non sincère puisqu'elle envoie de fausses informations tout en ayant connaissance de l'information vraie. Afin de participer au renforcement de la sécurité d'un système d'information, la confiance doit prendre en compte l'éventuelle malveillance de la source qui se traduit par une falsification volontaire de l'information. Cependant, une source peut également commettre des erreurs comme donner accidentellement une information erronée. Ainsi, pour modéliser séparément les erreurs accidentelles d'une source, de ses falsifications intentionnelles, un modèle pertinent de confiance devrait s'appuyer a minima sur les notions de compétence et de sincérité (Costé et al., 2016).

Plusieurs travaux ont cherché à mesurer la confiance. La plupart de ces contributions sont basées sur un modèle de réseau dans lequel les divers nœuds interagissent. Les interactions sont alors sources de recommandations faites par les divers membres du réseau pour calculer leurs indices de confiance (Yan et al., 2003; Teacy et al., 2006; Das et Islam, 2012; Josang et al., 2015). La recommandation est le processus par lequel un nœud i va communiquer sa confiance $C_{i,j}$ dans le nœud j. Très utilisée, cette mesure suppose cependant que les nœuds ont conscience les uns des autres. Si chaque nœud est isolé des autres et n'a pas conscience du réseau alors la recommandation est impossible. Bien que cette hypothèse soit vérifiée dans les réseaux sociaux ou sur le web, elle ne l'est cependant pas en général. Par exemple, la recommandation est difficile dans les réseaux dits centralisé où un serveur communique avec plusieurs clients qui ne se connaissent pas entre eux.

Lorsqu'il n'est pas possible d'obtenir les diverses appréciations des sources entre elles, il est encore possible de mesurer la confiance à partir de l'analyse des informations transmises par la source (Matt et al., 2010). Nombre de ces mesures sont construites sur la base de la théorie de l'argumentation (Dung, 1993) qui modélise un ensemble de propositions appelées *arguments* et un ensemble d'*attaques* entre ces arguments. Les arguments sont assimilés aux nœuds d'un réseau et les attaques à des arêtes unidirectionnelles. La théorie de l'argumentation cherche à établir quels arguments sont rationnellement acceptables. Plus clairement, et comme illustré en figure 1, l'argument d est acceptable puisqu'il n'est attaqué par aucun autre. Il en est de même pour l'argument f. En revanche, l'argument e est contesté à la fois par b et f.

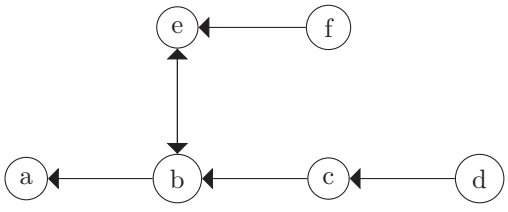

FIG. 1 – *Exemple d'un modèle utilisant 6 arguments et 6 attaques entre ces arguments.*

Sur la base de cette théorie, divers modèles de confiance utilisant des sources d'information ont été suggérés (Stranders et al., 2008; Parsons et al., 2011; Villata et al., 2013; Paglieri et al., 2014). Ces modèles reposent sur deux hypothèses : l'ensemble des arguments utilisables

ainsi que leurs liens (c.-à-d. les attaques) sont connus et sont en nombre fini. Pour juger de l'acceptabilité d'un argument (sur laquelle repose la confiance), il est donc nécessaire de pouvoir comparer l'ensemble de ceux à disposition et donc de pouvoir clairement identifier les attaques. Ce n'est pas toujours possible, notamment en présence d'incertitude. En effet, les arguments peuvent ne pas s'opposer formellement. Par exemple, les deux assertions "il fait chaud" et "il fait froid" ne s'opposent pas nécessairement : elles peuvent indiquer une température modérée, intermédiaire. La théorie de l'argumentation n'est donc pas adaptée lorsqu'un conflit entre informations n'est pas clairement identifié et est donc incertain.

Néanmoins, plusieurs travaux ont cherché à pallier cette faiblesse. Parmi ceux-là, l'article de Da Costa Pereira et al. (2011) propose un modèle dans lequel l'acceptabilité des arguments (i.e. le degré de croyance qu'ils sont vrais) est évaluée selon la confiance attribuée à la source. Contrairement aux modélisations de Dung (1993) et Villata et al. (2013) où un argument est soit accepté soit rejeté, l'acceptabilité d'un argument est ici continue. Cependant, la confiance est considérée comme un concept unidimensionnel alors qu'elle est multidimensionnelle pour Villata et al. (2013) qui la modélisent à partir de la compétence et de la sincérité de la source.

D'autres théories plus adaptées à la gestion de l'incertitude ont été utilisées (Josang, 2001; Yu et Singh, 2002; Sun et al., 2006; Wang et Singh, 2007). En particulier, Sun et al. (2006) arguent que la confiance est une mesure de l'incertitude et définissent ainsi leur mesure de confiance sur la probabilité qu'une entité effectue une certaine action. De même, Wang et Singh (2007) considèrent l'importance de la prise en compte de la certitude comme critère pour mesurer la confiance. Malgré une gestion efficiente des grandeurs réelles, ces travaux se basent cependant exclusivement sur une confiance unidimensionnelle.

Nous souhaitons donc étendre ces modèles en proposant une mesure de la confiance qui soit multidimensionnelle, fondée sur la compétence et la sincérité. Cette mesure ne repose pas, voire peu, sur une connaissance a priori et ne nécessite pas d'interactions entre les sources. Elle doit, de plus, être adaptée à des informations continues telles que des valeurs réelles.

3 Modélisation des producteurs et des sources d'information

Un système d'information est composé de multiples blocs fonctionnels interconnectés qui mesurent, analysent, traitent voire prennent des décisions et émettent de l'information. Ces blocs, quelle que soit leur fonction, peuvent être vus comme des *producteurs d'informations* (capteurs, automates, humains, etc.) pouvant être perçus comme mono ou multisources.

Au contraire d'un producteur, une source est à l'origine d'une information d'une nature ou d'un type particulier. Il peut s'agir d'une entité physique comme un capteur. Cette section présente notre modélisation des sources et des producteurs d'information ; laquelle différencie les constituants d'un système d'information comme cibles ou objets de la confiance.

3.1 Modélisation des producteurs d'informations

Les producteurs d'informations sont de différentes natures. Ils produisent de nombreuses informations (position, vitesse ...) sous différentes formes (nombre, texte, image, son, vidéo, etc.). On pourra distinguer différents types de producteurs : mono-source mono-information, multi-sources mono-information (cas d'un système constitué de plusieurs capteurs de même type) ou multi-sources multi-informations.

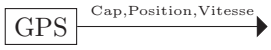

FIG. 2 – *Modélisation du GPS sous la forme d'un producteur multi-informations*

La figure 2 illustre la modélisation du producteur "GPS", et la figure 3, les sources qui le constituent. Cette modélisation permet de simplifier l'ajout ou la suppression d'un producteur au niveau du système (par ex. nouveau capteur installé, capteur en panne). La notion de producteur permet également de prendre en compte le fait que des sources et leurs informations sont liées à un même composant du système. Cette représentation pourra être utile notamment en cas d'attaque par leurre du producteur de données. Un producteur est cependant plus complexe à manipuler du fait du nombre d'informations transmises à un instant t qui n'est pas forcément fixe. Les informations ne sont pas émises à la même période, certaines pouvant être envoyées occasionnellement (par ex. les alertes SAR [1] du système AIS [2]). D'où l'intérêt de pouvoir modéliser un producteur comme constitué de sources d'informations. Ce dernier modèle allie simplicité (une source est spécialisée, c'est-à-dire qu'elle n'envoie qu'un seul type d'information et sert une unique fonctionnalité) et souplesse (il est facile d'ajouter ou d'enlever des sources d'un producteur, en cas de défaillance par exemple).

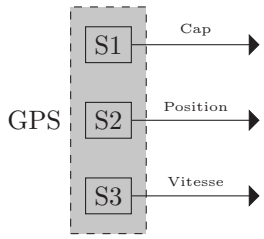

FIG. 3 – *Modélisation multi-sources mono-information du GPS.*

Si l'on revient à l'exemple de la figure 3, le producteur GPS est constitué de trois sources distinctes émettant respectivement les informations de cap, position et vitesse. Si le GPS est éteint alors trois sources distinctes n'émettront plus d'informations. Ce modèle prend en compte les liens qui existent entre les différentes sources, en particulier le fait qu'elles font partie d'un même producteur. Enfin, pour aller plus loin, il est possible de rassembler plusieurs producteurs en un sous-système, comme illustré en figure 4, où un sous-système regroupe un ensemble de producteurs qui n'interagissent qu'entre eux. Avec cette modélisation, nous pourrons évaluer la confiance au niveau des sources, des producteurs et des sous-systèmes.

1. Search and Rescue, alerte pour le sauvetage en mer.
2. Automatic Identification System, système standardisé par l'Organisation Maritime Internationale pour la diffusion en temps réel d'informations de navigation par VHF

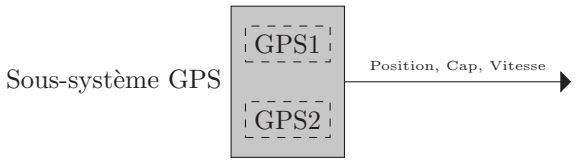

FIG. 4 – *Modélisation d'un sous-système GPS regroupant l'ensemble des producteurs GPS du navire.*

3.2 Modélisation des sources

Une source d'information est une entité qui observe un phénomène et le restitue au système. Par exemple, lorsque la source est un capteur, elle mesure une grandeur physique (vitesse, température etc.). Cette mesure est imparfaite et entachée d'erreur. En effet, la mesure est dépendante des caractéristiques du capteur (sensibilité, usure ...). Deux sources mesurant le même phénomène et ayant les mêmes caractéristiques ne rendront pas forcément compte de la réalité de la même manière du fait d'un bruit dans la mesure. Cependant, ces mesures ne seront pas très éloignées et en tous cas seront proches de la réalité à moins de la défaillance du capteur ou d'une attaque. Suivant la complexité des capteurs, des phénomènes physiques observés et des composants électroniques utilisés, il est plus ou moins difficile de quantifier cette erreur dans la mesure. Néanmoins, une solution simple consiste à résumer l'ensemble des bruits de la chaîne d'acquisition à un bruit additif, de nature gaussienne le plus souvent.

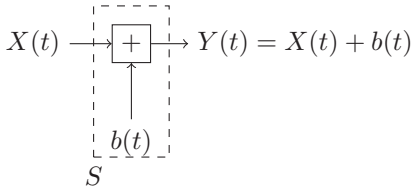

FIG. 5 – *Modélisation d'une source par un canal gaussien*

Comme illustré en figure 5, nous considérons qu'une source S observe le phénomène réel $X(t)$, une fonction dépendante du temps (température, vitesse, position), transmet sa mesure $Y(t) = X(t) + b$ où b est une variable aléatoire de loi normale $\mathcal{N}(\mu, \sigma)$ de moyenne μ et d'écart-type σ. Sans perte de généralité, nous supposerons que b est centrée (c.-à-d. $\mu = 0$). Par la suite, une source sera dite *idéale* ou *parfaite* si celle-ci renvoie telle quelle l'information observée, c'est-à-dire $X(t) = Y(t)$ pour tout t (c.-à-d. $\mu = 0$, $\sigma = 0$).

4 Mesurer la confiance

Comme décrit en Section 2, nous définissons la confiance accordée à une source comme une fonction de la compétence et de la sincérité de cette dernière. Nous précisons ci-après les concepts et comment les mesurer.

4.1 Mesure de compétence

Nous rappelons que la compétence d'une source est "sa capacité à remplir les fonctions qui lui sont attribuées" (Grandison et Sloman, 2000). Cette capacité de la source est dépendante de ses caractéristiques intrinsèques. D'après cette définition et le modèle de source proposé, la compétence $Comp$ d'une source est donc dépendante de l'imprécision de sa mesure. Ainsi, une source *idéale* est jugée compétente car elle remplit sa fonction en fournissant exactement la mesure réelle. Nous avons

$$Comp = f(b) \overset{b \text{ est centrée}}{=} f(\sigma)$$

où f est une fonction de la mesure de la compétence à définir (telle que $Comp = f(\sigma) \in [0; 1]$). Considérant que si la source est parfaite alors la compétence est maximale, c.-à-d. $f(\sigma = 0) = 1$ et qu'a contrario, si la source est très imprécise (c.-à-d. $\sigma \to +\infty$) alors elle est incompétente, c.-à-d. sa compétence tend vers 0 ($\lim_{\sigma \to +\infty} f(\sigma) = 0$), nous proposons de définir la fonction f telle que

$$Comp = \frac{1}{1+\sigma}.$$

Malgré sa simplicité, nous verrons que cette fonction répond au besoin. Par exemple, dans le cas d'un GPS qui mesure une latitude avec une précision de l'ordre de 10^{-5}, la compétence de la source associée à cette mesure est de l'ordre de 0.99999.

4.2 Mesure de sincérité

La sincérité d'une source est par nature difficile à évaluer. Liu et Williams (2002) proposent de la mesurer à partir de la croyance que les sources ont dans l'information qu'elles envoient. Ils l'identifient à la différence entre ce que la source, un humain dans le contexte, "dit" et ce qu'elle "pense", ou "sait". Dans notre cas, sur la base de notre modèle de source, ce concept de "pensée" d'une source n'est pas valide. Nous proposons donc de comparer les informations des différentes sources entre elles à l'instar de (Paglieri et al., 2014). Plus clairement, la sincérité d'une source est évaluée à partir des informations émises par les autres sources.

Il est également important de souligner qu'il existe un phénomène de dépendance entre la compétence et la sincérité. En effet, lorsqu'une source est incompétente, elle émet une information très imprécise qui complexifie sa comparaison avec des informations fournies par des sources compétentes. Plus une information est imprécise et plus celle-ci sera éloignée de la réalité et, par voie de conséquence, des autres informations plus précises et de même nature. Dès lors, dans le cas où la compétence de la source est faible, sa sincérité doit l'être également. Par contraposition, lorsque la compétence de la source est élevée (c.-à-d. proche de 1), aucune conclusion ne peut être induite sur sa sincérité. Nous proposons alors de borner la mesure de sincérité d'une source par sa compétence :

$$\forall i \geq 1 \; Sinc_i(t) = min(p_i(t), Comp_i(t))$$

où $p_i \in [0; 1]$ représente le degré d'accord de la source i avec les autres à l'instant t. Le degré d'accord d'une source avec les autres se mesure en comparant les informations que celle-ci fournit avec celles émises par les autres sources. Il sera élevé si l'information émise par la source est en accord avec celle des autres. Ainsi, considérant un ensemble de sources

compétentes, une source émettant une information similaire à la majorité sera jugée plus sincère qu'une source contestée (c.-à-d. en accord avec une minorité). Tel que défini, le degré d'accord est une mesure de consensus, c'est-à-dire à quel point la source est confortée par les autres sources. Elle peut être vu comme le ratio entre le nombre de sources en accord avec la source i à l'instant t, et le nombre total de sources. Pour mesurer l'accord entre deux sources, une solution possible est de passer par un consensus binaire, comme proposé dans (Paglieri et al. (2014)) : deux sources sont complètement d'accord ou en complet désaccord. Dans notre contexte, et avec notre modèle de source, cette approche n'est pas la plus judicieuse, car l'information correspond à des nombres réels. Nous proposons plutôt d'utiliser une fonction de similarité, notée Sim, continue pour mesurer le consensus prenant en compte les informations émises aux instants précédents, c'est-à-dire :

$$p_i(t) = \begin{cases} 1 & n = 1 \\ \dfrac{1}{n-1} \sum\limits_{\substack{j=1 \\ j \neq i}}^{n} Sim(\{Y_i(t)\}_{t>0}, \{Y_j(t)\}_{t>0}) & n \geq 2 \end{cases}$$

où n est le nombre de sources et $\{Y_i(t)\}_{t>0}$ l'ensemble des informations émises par la source i jusqu'à l'instant t. De manière à garantir $p_i = 1$ lorsque toutes les sources sont en accord et inversement si $p_i = 0$ lorsque la source i s'oppose à toutes les autres, la fonction de similarité utilisée ci-après correspond à une mesure de corrélation entre les informations des différentes sources. Un autre intérêt de cette mesure est que la valeur de p_i est relativement stable lorsque le nombre n de sources est "suffisamment" grand.

Au contraire, dans le cas particulier d'une unique source, le consensus ne peut être mesuré à cause du manque d'informations supplémentaires. Par convention, nous proposons alors de poser $p_1(t) = 1$ ce qui symbolise l'accord de la source avec elle-même. Il en résulte alors une égalité directe entre la sincérité d'une source unique et sa compétence (i.e. $Sinc_1(t) = Comp_1(t)$ pour tout t).

4.3 De la compétence et de la sincérité à la confiance

Pour obtenir une mesure de confiance $Conf(S_i)$ à partir des mesures de compétence et de sincérité (c.-à-d. $Conf(S_i) = Conf(Comp(S_i), Sinc(S_i))$), plusieurs solutions ont été définies dans (Liu et Williams (2002)). Ces mesures respectent toutes les contraintes suivantes :

- $Conf(1, 1) = 1$
- $Conf(0, 0) = 0$
- $Conf(Comp, 1) = Comp,\ Comp \in [0; 1]$
- $Conf(1, Sinc) = Sinc,\ Sinc \in [0; 1]$

Les auteurs proposent ainsi plusieurs mesures en adéquation avec ces contraintes :

$$Conf_1(Comp, Sinc) = Comp * Sinc \quad (1)$$
$$Conf_2(Comp, Sinc) = min(Comp, Sinc) \quad (2)$$
$$Conf_3(Comp, Sinc) = 1 - (1 - Comp)(1 - Sinc) \quad (3)$$

Comme nous le verrons, la mesure $Conf_3$ ne traduit pas nécessairement l'absence de confiance en une source incompétente ou non sincère. En particulier, $Conf_3$ est non nulle

lorsque la compétence ou la sincérité de la source est nulle, propriété cependant souhaitée dans notre contexte. Cela revient à augmenter le jeu de contraintes précédent des règles suivantes :

- $Conf(0, Sinc) = 0,\ Sinc \in [0; 1]$
- $Conf(Comp, 0) = 0,\ Comp \in [0; 1]$

Dans la section suivante, nous expérimentons ces différentes mesures sur des données réelles.

5 Expériences

Les mesures de confiance, compétence et sincérité définies précédemment ont été testées sur des données provenant de l'*Automatic Identification System* d'un bateau, à proximité de Brest. L'AIS fournit différentes informations : position, vitesse, identifiant du bateau, etc. À partir de ces données, nous avons simulé 3 producteurs d'information (cf Section 3.2) : deux GPS et un Loch Doppler. Ces producteurs peuvent se retrouver embarqués sur des navires tels que des navires de croisière par exemple. Dans notre contexte expérimental, les deux GPS sont respectivement situés à l'avant et à l'arrière du navire et le Loch Doppler en son milieu. Si un GPS est constitué de trois sources donnant trois types d'informations distinctes : la position, la vitesse et le cap, un Loch Doppler ne comporte qu'une seule source : la vitesse. En effet, un Loch Doppler mesure la vitesse du navire par rapport au fond en utilisant un signal ultrasonore.

La figure 6 montre le comportement des différentes mesures de compétence, de sincérité et de confiance en simulant les trois sources de vitesse des producteurs à partir des données de vitesse produites par l'AIS. Un bruit gaussien centré a été ajouté pour simuler les 3 sources suivant le modèle de source décrit en Section 5. Les trois bruits gaussien sont de variance identique. Pour simuler une attaque de "leurrage", le Loch Doppler émet de fausses informations à partir de l'instant $t = 500$; instant à partir duquel la vitesse transmise est de 1 nœud supérieure à la vitesse réelle. En effet, un attaquant peut vouloir falsifier les informations de vitesse pour ralentir le navire (e.g. pour faciliter son interception par des pirates) ou bien le faire accélérer (e.g. surconsommation, usure prématurée du moteur ou de la ligne d'arbre). Cette attaque, bien que peu subtile (un regard à l'historique suffit à la détecter), peut se révéler gênante voire dangereuse sur le long terme.

La première ligne de courbes en figure 6 montre la vitesse telle que perçue par chaque source avec une précision d'environ 0.1 nœuds (spécifications constructeur). Les deux lignes intermédiaires montrent l'évolution de la compétence et de la sincérité de chacune des sources au fil du temps. On peut voir que la compétence de chaque source est identique, du fait qu'un bruit de même variance a été ajouté aux données réelles. On peut voir l'impact de l'attaque du Loch Doppler au niveau de la mesure de sincérité des trois sources. Dès que ce dernier indique une vitesse différente de celle mesurée par les GPS, la mesure de sa sincérité tend à la baisse et de manière plus forte que les mesures de sincérité des deux GPS.

La dernière ligne de courbes montre l'évolution de la confiance respective des trois capteurs en utilisant les trois mesures tirées de (Liu et Williams, 2002). La confiance dans la deuxième source (c.-à-d. celle attaquée) diminue comme sa sincérité dès l'instant où elle envoie de fausses informations, et cela de manière plus importante que les deux autres sources, comme attendu. Comme supposé en section 4.3, la mesure $Conf_3$ est très peu sensible aux variations de sincérité (et de compétence, par symétrie). Parmi les trois mesures testées, c'est la seule à ne pas respecter les contraintes additionnelles (voir la Section 4.3). Dans un contexte de détection de falsifications d'informations, cette mesure n'est donc pas adaptée.

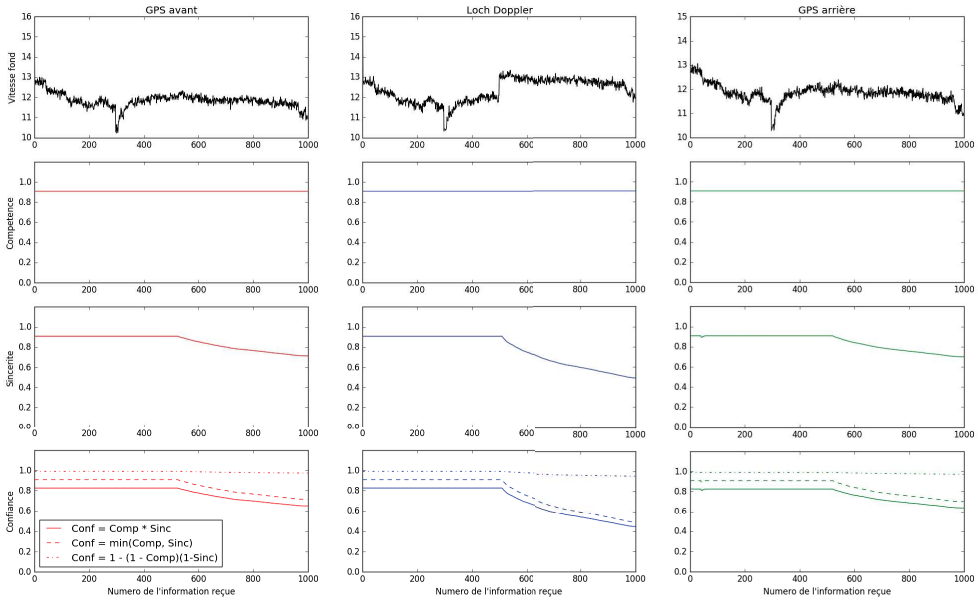

FIG. 6 – *Comparaison des trois mesures de confiance en présence de trois sources de vitesse sur un navire.*

Cette expérimentation basée sur plusieurs sources simulées à partir d'un jeu de données réelles montrent la pertinence de l'approche ; approche qui peut être transposée à d'autres systèmes d'information. Cependant, bien que fondées sur les spécifications techniques des capteurs, les sources modélisées sont de compétences identiques. De plus, comme l'ont montré Bhatti et Humphreys (2015), un attaquant peut utiliser des falsifications incrémentales pour dissimuler ses agissements. La confrontation de nos modèles à des scenarii plus complexes fera l'objet de travaux ultérieurs.

6 Conclusion

Sur un navire, un système d'information (SI) est composé de multiples sources d'informations qui peuvent être leurrée ou malveillantes, mettant en danger sa sécurité. Cet article propose d'extraire la confiance que peut avoir le SI envers les sources qui le constituent par l'analyse des informations qu'elles émettent. Sur la base d'un modèle de sources et de producteurs d'informations constituant le SI, une mesure de confiance a été élaborée à partir de mesures de compétence et de sincérité des sources. Ces mesures ont été testées et comparées dans une situation de falsification d'informations. Les résultats obtenus valident l'approche. Toutefois, les sources sont jugées indépendamment les unes des autres. La prise en compte des relations qui les unissent, notamment de dépendance, pourrait permettre de limiter la portée des collusions éventuelles.

Références

Abdul-Rahman, A. et S. Hailes (2000). Supporting trust in virtual communities. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, pp. 9–19. IEEE.

Bhatti, J. et T. Humphreys (2015). Hostile control of ships via false gps signals : Demonstration and detection. *submitted to Navigation, in review*.

Blomqvist, K. (1997). The many faces of trust. *Scandinavian journal of management 13*(3), 271–286.

Capra, L. et M. Musolesi (2006). Autonomic trust prediction for pervasive systems. In *20th International Conference on Advanced Information Networking and Applications*, Volume 2, pp. 48–59. IEEE.

Costé, B., C. Ray, et G. Coatrieux (2016). Évaluation de la confiance dans un environnement multisources. In *Informatique des Organisations et Systèmes d'Information et de Décision (INFORSID), Atelier Sécurité des systèmes d'information : technologies et personnes*.

Da Costa Pereira, C., A. B. TeTettamanzi, et S. Villata (2011). Changing one's mind : Erase or rewind ? possibilistic belief revision with fuzzy argumentation based on trust. In *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence*, Volume 1, pp. 164–171.

Das, A. et M. M. Islam (2012). Securedtrust : a dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing 9*(2), 261–274.

Demolombe, R. (2001). To trust information sources : a proposal for a modal logical framework. In *Trust and deception in virtual societies*, pp. 111–124. Springer.

Demolombe, R. (2004). Reasoning about trust : A formal logical framework. In *Trust Management*, pp. 291–303. Springer.

Dung, P. M. (1993). On the acceptability of arguments and its fundamental role in nonmonotonic reasoning and logic programming. In *International Joint Conferences on Artificial Intelligence*, pp. 852–857.

Grandison, T. et M. Sloman (2000). A survey of trust in internet applications. *Communications Surveys & Tutorials, IEEE 3*(4), 2–16.

Josang, A. (2001). A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems 9*(3), 279–311.

Josang, A., M. Ivanovska, et T. Muller (2015). Trust revision for conflicting sources. In *Proceedings of the 18th International Conference on Information Fusion (FUSION 2015)*, pp. 550–557.

Lewis, J. D. et A. Weigert (1985). Trust as a social reality. *Social Forces 63*(4), 967–985.

Liu, W. et M.-A. Williams (2002). Trustworthiness of information sources and information pedigree. In *Intelligent Agents VIII*, pp. 290–306. Springer.

Matt, P.-A., M. Morge, et F. Toni (2010). Combining statistics and arguments to compute trust. In *Proceedings of 9th International Conference on Autonomous Agents and Multiagent Systems*, pp. 209–216.

McKnight, D. H. et N. L. Chervany (2000). What is trust ? a conceptual analysis and an interdisciplinary model. *Americas Conference on Information Systems*, 827–833.

Paglieri, F., C. Castelfranchi, C. da Costa Pereira, R. Falcone, A. Tettamanzi, et S. Villata (2014). Trusting the messenger because of the message : feedback dynamics from information quality to source evaluation. *Computational and Mathematical Organization Theory 20*(2), 176–194.

Parsons, S., Y. Tang, E. Sklar, P. McBurney, et K. Cai (2011). Argumentation-based reasoning in agents with varying degrees of trust. In *Proceedings of the International Conference on Autonomous Agents and Multiagent Systems*.

Stranders, R., M. de Weerdt, et C. Witteveen (2008). Fuzzy argumentation for trust. In *Computational Logic in Multi-Agent Systems*, pp. 214–230. Springer.

Sun, Y. L., Z. Han, W. Yu, et K. R. Liu (2006). A trust evaluation framework in distributed networks : Vulnerability analysis and defense against attacks. In *INFOCOM*, pp. 1–13.

Teacy, W. T. L., J. Patel, N. R. Jennings, et M. Luck (2006). TRAVOS : Trust and reputation in the context of inaccurate information sources. *Autonomous Agents and Multi-Agent Systems 12*(2), 183–198.

Villata, S., G. Boella, D. M. Gabbay, et L. van der Torre (2013). A socio-cognitive model of trust using argumentation theory. *International Journal of Approximate Reasoning 54*(4), 541–559.

Wang, Y. et M. P. Singh (2007). Formal trust model for multiagent systems. In *International Joint Conference on Artificial Intelligence*, pp. 1551–1556.

Yan, Z., P. Zhang, et T. Virtanen (2003). Trust evaluation based security solution in ad hoc networks. In *Proceedings of the Seventh Nordic Workshop on Secure IT Systems*, Volume 14.

Yu, B. et M. P. Singh (2002). An evidential model of distributed reputation management. In *Proceedings of the first international joint conference on Autonomous agents and multiagent systems : part 1*, pp. 294–301. ACM.

Summary

Rapid evolution of numerous types of sensors and communicating objects has significantly enhanced the content of information systems, especially mobile ones. However, it raises new questions about trust one can have in information and sources. Indeed, sources can be duped or under external control falsifying source's information. This paper proposes to study security of information systems through the notion of trust. First, definition then evaluation of trust in heterogeneous networks are introduced. Afterwards, we propose modelling of sources. Trust in sources is studied and measured through two characteristics: competence and sincerity. Experiments based on several simulated sources from a real dataset show the relevance of our approach. This work is applied to the analysis of position and navigation data.