Une ontologie pour la description des intrusions dans les RCSFs.

Hubert Ngankam Kenfack, Thoma Djotio Ndié, Emmanuel Nataf, Olivier Festor

Une ontologie pour la description des intrusions dans les RCSFs

Hubert N. Kenfack[*] — Thomas Djotio Ndié[*] — Emmanuel Nataf[**] — Olivier Festor[**]

[*] *Equipe-Projet MASECNESS, LIRIMA / Université de Yaoundé 1*
BP: 8390 Yaoundé/Cameroun
{einshubert, tdjotio}@gmail.com
[**] *Equipe-Projet MADYNES, INRIA*
Centre de Recherche INRIA Nancy – Grand Est
615, rue du Jardin Botanique
54601 Villers-lès-Nancy, France
{Emmanuel.Nataf, Olivier.Festor}@inria.fr

RÉSUMÉ. *Nous proposons une définition formelle d'une intrusion par la mise sur pied d'une ontologie de différentes intrusions dans les Réseaux de Capteurs Sans Fil (RCSF) ; l'objectif étant d'offrir une classification complète qui prend en compte l'intrusion aussi bien du point de vue de son impact sur le service offert, du point de vue des fonctionnalités implantées dans les protocoles de sécurité, et celui des dysfonctionnements aléatoires dus à un phénomène naturel ou inattendu.*

ABSTRACT. *We propose a formal definition of an intrusion through the establishment of an ontology of different intrusions in Wireless Sensor Networks (WSNs), the aim being to offer a more comprehensive classification that takes into account the intrusion as well from an offered service point of view, an established functionality in the security protocols point of view, as that of random dysfunction due to a natural or unexpected phenomenon.*

MOTS-CLÉS : *intrusion, réseaux de capteurs, détection, système de détection d'intrusion, ontologie, sticky values.*

KEY WORDS: *intrusion, sensor networks, detection, intrusion detection system, ontology, sticky values.*

1. Introduction

Les réseaux de capteurs ont des applications dans de nombreux domaines allant de la surveillance de trafic urbain au suivi de marchandises, de l'assistance médicale à l'automatisation dans les habitations. Etant par nature distribués et généralement d'une taille importante (centaines à milliers de nœuds), les réseaux de capteurs ont tout intérêt à bénéficier des connaissances issues du fonctionnement de l'Internet. De plus, ces réseaux sont amenés à être connecté à l'Internet, pour former l'*Internet of Things* [VAS 10], facilitant leur exploitation, mais augmentant les problèmes de sécurité.

Le comportement du capteur ou d'un Réseau de Capteurs sans Fil (RCSF) en général peut être altéré par plusieurs facteurs. Parmi ces facteurs nous pouvons rappeler sans être exhaustif l'environnement, l'utilisation d'un médium ouvert de communication, l'utilisation des stratégies de coopération [KAC 02][SUN 07] qui peuvent provoquer des comportements inconnus. Plusieurs solutions pour résoudre le problème sont proposées ; comme par exemple la cryptographie symétrique, l'authentification et la sécurisation des protocoles de routages [KAC 02][SUN 07] [ROM 05]. La difficulté avec ces solutions est qu'elles sont pour la plupart hautement spécialisées pour une attaque précise. De plus, il est pratiquement impossible vu les contraintes (mémoire, calcul, communication, …) liées aux capteurs d'embarquer toutes ces solutions (cryptographie symétrique, l'authentification…) dans un nœud. Enfin, elles n'offrent pas la possibilité de détecter de nouvelles attaques, ni même celle de défendre le réseau contre des nœuds internes compromis [KET 08]. D'où la nécessité d'utiliser des solutions basées sur la détection des intrusions dans les RCSFs qui semblent offrir de meilleurs résultats [SUM 08][BYU 06][CHE 09][IOA 07].

Pour offrir une vision plus formelle des intrusions certains travaux offrent une classification ou une taxonomie [SOB 06][ULF 97][NEU 95][DAV 95][FRE 97][FAT 07] de différentes attaques et des systèmes de détection d'intrusions (IDS : *Intrusion Detection System*) pour RCSF. L'auteur de [SOB 06] montre plusieurs niveaux de classifications de détection des intrusions. La première est basée sur le comportement du système et une hypothèse initiale prenant en compte les activités du système qui sont observables et des activités normales et intrusives provenant de différentes sources. Par la suite, ils proposent une seconde classification en se basant cette fois-ci sur les types d'intrusions, le comportement et la technique de détection. Comme pour toutes les autres propositions [SOB 06][ULF 97][NEU 95][DAV 95][FRE 97][FAT 07] nous sommes confrontés au même problème : l'intrusion n'est pas prise dans sa globalité, mais uniquement par les aspects liés aux attaques de déni de service.

Dans ce papier nous proposons une ontologie des différentes intrusions dans le domaine des RCSFs. Nous essayons d'apporter des éléments pour identifier et caractériser les différentes intrusions de manière globale dans les RCSFs. Notre solution utilise un haut niveau d'abstraction et considère les intrusions aussi bien d'un point de vue service offert, d'un point de vue fonctionnalité implantée dans les protocoles de sécurité, que celui de dysfonctionnement aléatoire dû à un phénomène naturel ou inattendu. Le reste du document est organisé comme suit : la section 2 présente les différentes intrusions dans les RCSFs. La section 3 présente notre modèle d'ontologie dans les RCSFs, la section 4 présente comment se fera l'exploitation de l'ontologie réalisée. La section 5 conclut ce travail et présente les travaux futurs.

2. Les intrusions dans les RCSFs

Pour offrir l'efficacité et la pertinence attendues en termes de détection d'intrusions dans le contexte des RCSFs, il est important de bien connaître l'impact du climat, du terrain et du module de lecture de données. Lorsque des nœuds ne remplissent pas correctement leurs fonctions initiales, que cela soit par l'envoi de données erronées ou par l'absence d'émission, ils sont considérés comme des intrus. Plusieurs causes sont à l'origine de la transformation de ces nœuds en intrus. Dans sa thèse, Frédéric Majorczyk [MAJ 08] regroupe ces dysfonctionnements suivant trois niveaux : (1) la défaillance qui survient lorsque le service délivré dévie de l'accomplissement de la fonction du système ;(2) les erreurs qui ont entraînées par des défaillances ; (3) et les fautes qui sont les causes adjugées ou supposées des erreurs. Tout en montrant comment ces entraves forment une chaîne causale logique, il affirme par la suite qu'elles sont récursives. Avant d'étudier différentes solutions proposées dans [KAC 02][SUN 07][ROM 05] pour détecter les intrus dans les RCSFs ou alors pour réduire le nombre de fausses alertes [BHA 07], il est opportun de définir et d'identifier l'origine de ces entraves qui débouche sur une intrusion.

2.1. *Intrusion dues aux sticky values*

La capacité [GAN 04] d'un RCSF à effectuer ses tâches ne dépend pas uniquement de sa capacité à communiquer avec les autres nœuds du réseau, mais surtout de sa capacité à capter les grandeurs physiques de son environnement et des procédés de traitement des données collectées. L'agrégation des données provenant de multiples nœuds nécessite que l'on accorde une certaine confiance à ces nœuds, or les fortes contraintes en terme de ressources limitées rendent ceux-ci très peu fiables. Les fautes les plus courantes dans les RCSFs surviennent lors du déploiement. Ils sont ainsi classés dans la catégorie de *sticky values* [GAN 04]. Ce sont des valeurs qui peuvent provenir soit des erreurs de mesure par les capteurs, soit des données hors limites, soit des dépassements de plage de lecture soit enfin de la similitude qui existe entre certaines valeurs de calibrage de la radio, de l'antenne, de la *mote* et des équipements de récupération des données. Pour résoudre ces problèmes, [GAN 04] propose une solution appelée RFSN (*Reputation Based Framework for Sensor Networks*) basée sur la confiance, où les nœuds maintiennent une liste de la confiance envers d'autres nœuds du réseau. Il s'agit pour un nœud de construire progressivement sa liste de réputations sur les autres nœuds en surveillant leur comportement et le taux de coopération (comportement attendu du nœud) et de non coopération (comportement non attendu). Le nœud utilise ensuite cette liste pour évaluer la loyauté des autres nœuds et les données qu'ils produisent. Dans cette solution, un nœud peut évaluer les données provenant des autres nœuds avec la réputation correspondante pour identifier en temps réel les nœuds intrus. Dans [BHA 07], l'organisation du réseau en DAG (Directed Acyclic Graph), couplée à une transmission redondante des données sur plusieurs chemins permet de réduire l'impact du bruit et des fausses alarmes qui en résultent. Cette approche offre ainsi un modèle relationnel entre les multiples conditions externes et l'élément de captage.

2.2. *Détection des intrusions comme service offert par le RCSF*

Les RCSFs sont souvent utilisés comme équipements de surveillance. La détection de la cible (personne, véhicule, objet, ennemi dans un champ militaire,…) comme intrus est l'un des objectifs majeurs dans la surveillance. Plusieurs techniques sont mises en œuvre pour la détection des intrus dans un tel système de surveillance. L'utilisation d'un seuil fixe de valeur offre une détection efficace mais avec un fort taux de fausses alarmes [STR 07]. Le calcul de probabilité pour l'obtention d'un seuil dynamique de valeur est proposé comme alternative pour offrir un meilleur équilibre entre la quantité de fausses alarmes et le taux de détection [BHA 07]. Dans [ERM 06], les auteurs utilisent la procédure de FDR (*False Discovery Rate*) et l'algorithme de propagation de croyance via des méthodes statistiques pour détecter et localiser les équipements émettant un signal avec une faible ou une puissance inconnue. Pour détecter et reporter les anomalies d'accès aux constructions, les auteurs de [MAR 09] surveillent les bureaux avec des RCSFs. L'objectif étant de reporter toute occupation suspecte des bureaux par des intrus via l'utilisation des techniques de réseau de neurones tel que l'ART (*Adaptive Resonance Theory*). [JIN 09] met sur pied une communauté de détection d'intrusions basée sur le WNN (*Wavelet Neural Network).* Lorsqu'un phénomène anormal survient, le système met en marche des caméras et le WNN est utilisé pour reconnaitre l'image issue de différentes caméras. Les auteurs de [MEC 03] ont mis sur pied une nouvelle méthode pour traquer le mouvement des personnes et des véhicules dans des environnements ouverts en utilisant les techniques de *cooperative tracking* via la combinaison des données provenant des nœuds voisins.

2.3. *Détection des intrusions comme politique de sécurité dans le RCSF*

Dans le domaine de la sécurité, est considérée comme intrusion, toute tentative de violation de la politique de sécurité d'un système. Notamment, il s'agit de la violation d'une des propriétés de confidentialité, d'intégrité ou de disponibilité du système. Pour la plupart, elles sont causées par des nœuds corrompus ou par des nœuds externes usurpant des privilèges de sécurité. Le réseau devrait continuer son fonctionnement malgré l'apparition d'un comportement inconnu susceptible de gêner le bon fonctionnement de celui-ci. Pour assurer cela, plusieurs mécanismes de détection des intrusions sont mis en place :

— Des solutions d'IDS hiérarchiques [CHE 09] basées sur les tables d'isolation ITIDS (*Isolation Table IDS*) ou encore celle [SUM 08] utilisant une couverture hiérarchique telle que celle basée sur les réseaux GSM, mettent sur pied des clusters dans lesquels des nœuds régionaux assurent une détection distribuée des intrusions.

— Des organisations à plat [ROM 05] utilisant la technique de chien de garde spontané associé à deux agents par nœud, le premier chargé de surveiller les données destinées au nœud et le second ayant pour rôle de surveiller son voisinage.

— Certaines solutions sont basées sur des techniques centralisées via les SVM (*Support Vector Machine*) [BYU 06], l'objectif étant de produire de bons résultats même pour des apprentissages de comportements complexes.

Des IDS complètement décentralisés sont fondés sur un module de détection à trois phases (acquisition des données, applications des règles et détection proprement dite) s'intégrant parfaitement dans l'architecture du nœud [DAS 05].

Les IDS dans le domaine des RCSFs sont devenus assez matures et offrent de bons résultats tant dans la pertinence que dans la fiabilité. Certains, pour avoir de bons résultats se sont simplement spécialisés dans la détection d'une seule attaque [BYU 06]. Les trois approches d'interprétation d'intrusions que nous venons de présenter (*sticky values*, service et politique de sécurité) vont constituer trois domaines de connaissances sur lesquelles les outils de gestion d'intrusions s'appuient pour détecter ou prévenir les intrusions. Dans la section suivante nous proposons une approche générique de structuration de ces domaines de connaissances en utilisant une ontologie.

3. Ontologie pour la description des intrusions

Quelque soit l'approche utilisée, le problème reste celui de la caractérisation d'une intrusion. Utiliser une ressource sémantique telle qu'une ontologie pourrait être un moyen efficace d'enrichir les données sur les intrusions en vue de répondre plus précisément à des questions complexes sur la définition, la nature, la caractéristique de l'intrusion, et surtout de recueillir de nouvelles informations sur de nouvelles intrusions éventuelles pour permettre une meilleure intégration de celles-ci. Plusieurs classifications et taxonomies ont été étudiées dans la littérature [SOB 06][ULF 97][NEU 95][DAV 95][FRE 97][FAT 07][GUL 05]. Toutes ces classifications et taxonomies n'offrent pas la possibilité de prendre en compte l'intrusion dans sa globalité. Pour certaines classifications, seuls les aspects sécurité sont mis en exergue. Nous allons donc nous servir des classifications proposées dans [SOB 06][GUL 05] pour établir une ontologie plus complète en considérant l'intrusion à un niveau d'abstraction plus élevé.

Une ontologie définit formellement les termes employés pour décrire et représenter un domaine de connaissance. L'objectif est de permettre le partage, la réutilisation et le raisonnement sur les connaissances construites. L'ontologie construite est bâtie autour de trois grandes classifications qui représentent les trois grands domaines de connaissances:

— Une ontologie de haut niveau (*upper level ontology* ou *top-level ontology*) comportant les concepts abstraits et généraux du domaine des intrusions. Cette ontologie subsume les concepts existant dans les différentes intrusions.

— Une ontologie générale du domaine (*core ontology*) où ontologie noyau est celle qui permet de fédérer les concepts et relations centraux du domaine des intrusions.

— Une ontologie de bas niveau (*low level ontology*) traitant des aspects opérationnels des solutions de détections d'intrusions.

3.1. *Ontologie de haut niveau*

Chaque intrusion dans un réseau de capteurs peut être décrite suivant un schéma bien précis. A ce schéma nous pouvons associer trois sources distinctes constituant le plus haut niveau d'abstraction illustré figure 1.

— La première source, celle des *given_services* offre la possibilité d'utiliser le réseau de capteurs comme application à la détection des intrusions. Pour ce faire les capteurs sont déployés

pour surveiller une zone, l'objectif étant d'émettre une alarme dès qu'un intrus pénètre dans la zone surveillée.

— La seconde source *security_policy* représente les aspects liés aux politiques de sécurité mis en œuvre pour surveiller les différents nœuds constituant le réseau de capteurs. Ce volet permet de mettre en évidence toute tentative de corruption d'un nœud interne par un nœud externe désirant accéder au système, ou à une usurpation des différents privilèges des nœuds internes.

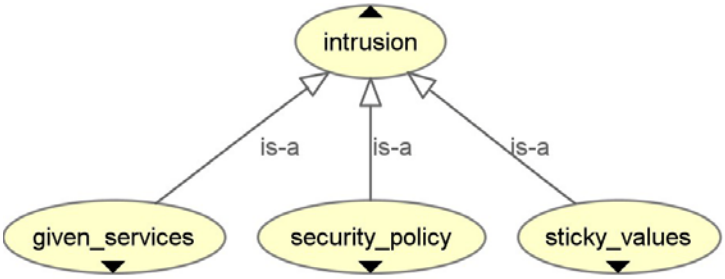

Figure 1. Ontologie de haut niveau

— La dernière source est celle liée aux *sticky values (cf. 2.1)*. Elle permet de mettre en évidence l'impact de l'environnement et des dysfonctionnements aléatoires pouvant survenir durant une transmission ou durant la lecture d'une grandeur physique quelconque.

3.2. *Ontologie générale du domaine*

L'ontologie générale du domaine permet de décrire les différents aspects du domaine considérés. Elle apporte les caractéristiques nécessaires pour définir et identifier les éléments provoquant les intrusions dans chaque domaine.

— Dans le domaine des *given_service*, figure 2, la protection et la surveillance sont les principales sources d'informations pouvant conduire à la détection d'intrusions. Les concepts se rapprochant le plus des intrusions sont particulièrement ceux qui sont regroupés dans la classe *intruding_object* qui présentent les différents éléments surveillés (soldat, champ de bataille, véhicule…) et la classe *site_condition* quant à elle présente les différentes conditions dans lesquelles est déployé le RCSF de surveillance. La classe *approach* regroupe les conditions pouvant influencer le résultat de la détection en agissant sur les différentes techniques utilisées pour y parvenir. La classe *network_topology* quant à elle met en évidence les différentes organisations réseau et matériel utilisées.

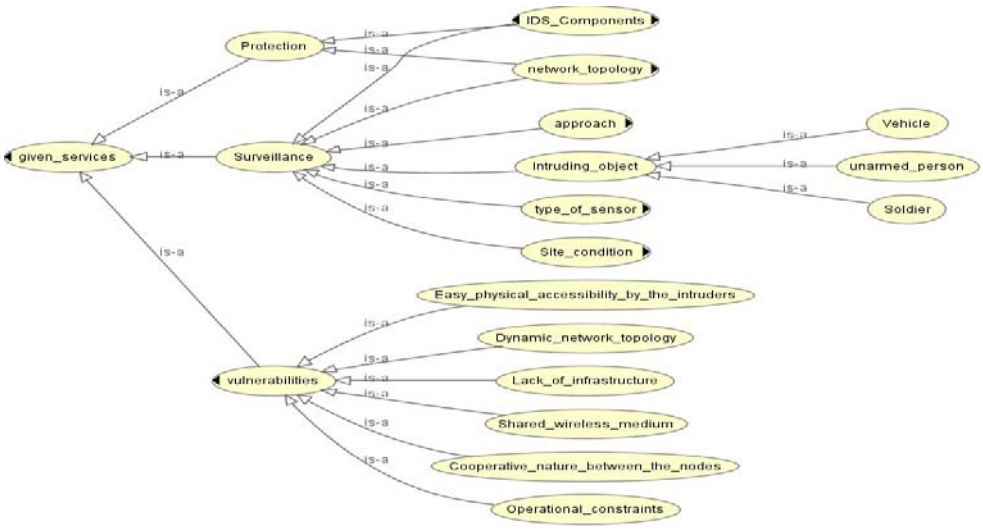

Figure 2. Ontologie du domaine des *given_services*

— La classification dans le domaine des *sticky_values* ; la figure 3 montre les deux principales classes : *WSN_Components* et *vulnerabilities*. La première représente les composants d'un capteur et les différentes relations existantes entre eux. Entre autre nous pouvons citer la classe *battery* qui représente comment le manque d'énergie dans une batterie peut conduire à un dysfonctionnement. La classe *radio*, elle, est constituée des éléments caractérisant l'arrêt de réception de données et les différentes attaques connues sur l'émission sans fil. La classe *Sensor* représente la hiérarchie des différentes erreurs (inconsistance dans les données, erreur de lecture…) pouvant conduire indirectement à une intrusion. La principale seconde classe *Vulnerability* représente les catalyseurs exposants le plus un RCSF aux attaques, on y trouve entre autre la nature coopérative des nœuds, l'absence d'infrastructure physique, le partage du médium de communication et la simplicité d'accès physique aux nœuds constituants le réseau.

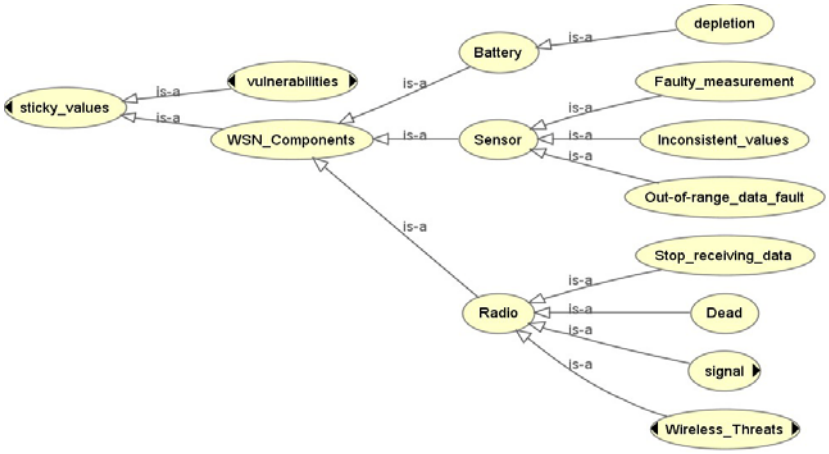

Figure 3. *Ontologie* du domaine des *sticky_values*

— Dans le domaine de la sécurité, la figure 4 regroupe tous les concepts se rapportant à l'intrusion. Plusieurs classes sont décrites et elles montrent une nette séparation entre les attaques contre les IDS (*Intrusion Detection System*) et les attaques contre les RCSFs. La classe *security_threats* qui regroupe par couche (Application, Réseau) les différentes attaques connues dans les RCSFs, et la classe Attacks_against_IDS présentant les attaques contre les IDS (Dénis de service, attaque d'insertion) sont présentées comme origine du dysfonctionnement. Nous y notons aussi les classe IDS et les IPS (*Intrusion Prevention System*) où un IPS est un IDS avec des mesures de prévention, représentant les solutions étudiées dans la littérature pour offrir un haut niveau de sécurité contre toute éventuelle intrusion.

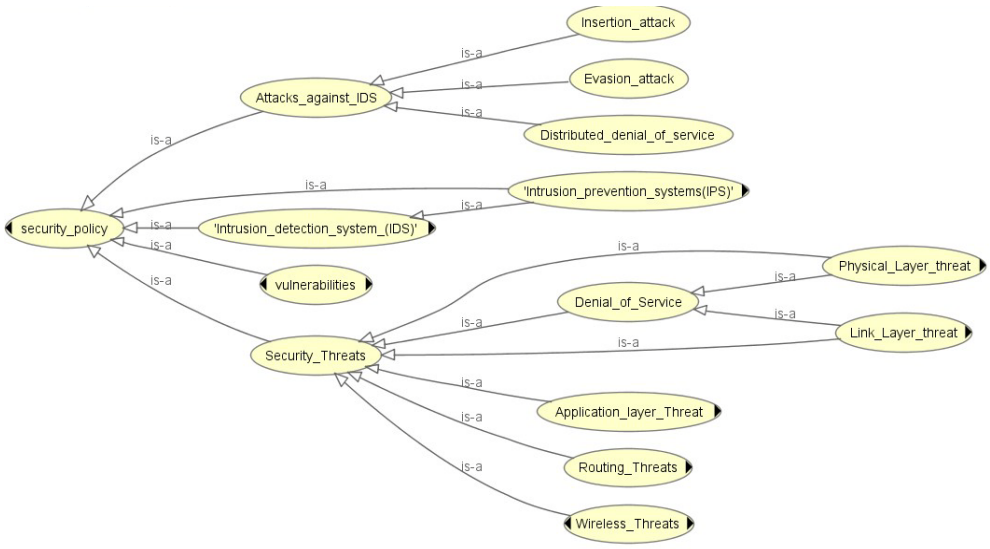

Figure 4. *Ontologie* du domaine des politiques de sécurités

3.3. *Ontologie de bas niveau*

L'ontologie de bas niveau est une ontologie dite opérationnelle car elle met en relation des exemples d'implémentation, des approches algorithmiques aux topologies utilisées pour faire fonctionner différents systèmes de détection. Pour des raisons de simplicité et de clarté nous allons nous intéresser à des visions réduites et partielles de l'ontologie construite.

— La classe *components_of_intrusion_detection* du domaine principal *given_services*, figure 5, décrit les différents éléments nécessaires à la détection d'intrus dans la zone de surveillance. On y retrouve la classe *Knowledge_Base* qui représente une base de connaissance contenant soit un ensemble de signatures et/ou de comportements nécessaire à l'identification d'un intrus. La classe *Responses* contient l'ensemble d'actions à entreprendre au cas où une éventuelle détection a été détectée. La classe *Decision_engine* représente le moteur de règles responsable de l'état d'un événement survenu. La classe *Audit_Data_Processor* est responsable de la lecture, du captage des événements qui surviennent dans l'espace de surveillance. La classe *Alarm_generation*

responsable de l'émission d'alertes en tout genre (sonore, textuelle, vidéo...) nécessaire à la notification d'éventuelle intrusion.

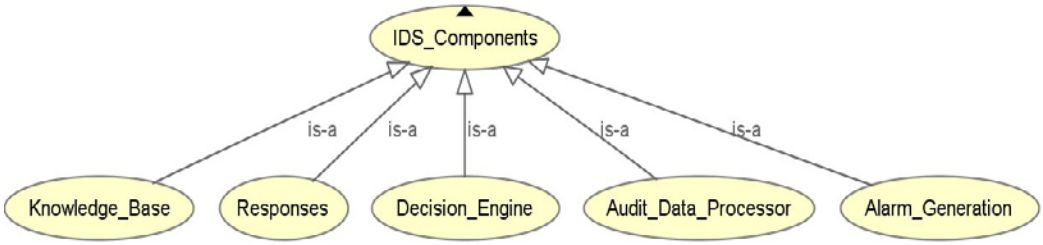

Figure 5. Ontologie opérationnelle des services offerts

— Au niveau opérationnel pour les *sticky values* nous détaillons pour l'exemple la classe *Radio* dans la figure 6. Cette classe permet de mieux faire une séparation entre les différents concepts pouvant générer une intrusion liée au composant radio du nœud capteur, nous y trouvons entre autre les attaques sur l'altération des données et l'attaque passive de la classe *Eavesdropping* permettant de violer la confidentialité du système via l'écoute des informations échangés. Elles sont des cas particuliers de la classe *Wireless_Threats* où figurent les attaques classiques connues sur les transmissions sans fil. Un autre exemple est celui de l'attaque *jamming* où l'objectif de l'attaquant est d'essayer de transmettre un signal à une antenne réceptrice à la même fréquence ou sous fréquence que le récepteur causant ainsi une interférence. Cette attaque est un cas particulier d'attaque liée au signal.

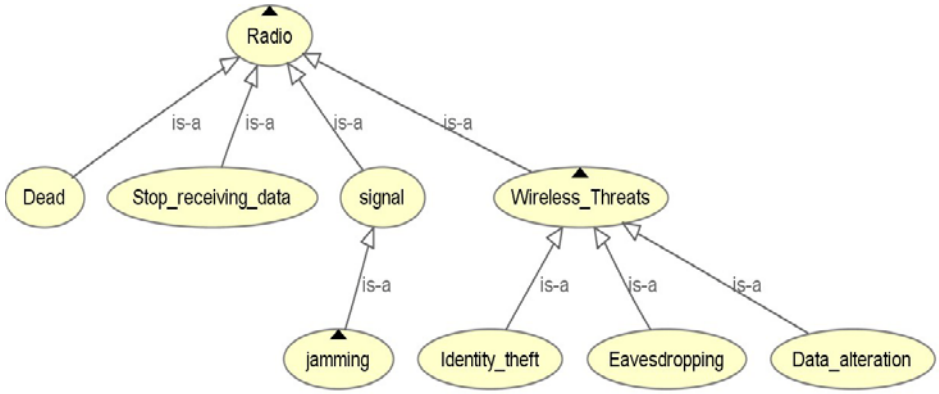

Figure 6. Ontologie opérationnelle des dysfonctionnements aléatoires

— La détection des intrusions via l'utilisation des IDS et des IPS offre de nombreux concepts qui sont regroupés dans la figure 7. Nous mettons en évidence ici uniquement les approches utilisées pour détecter d'éventuelles intrusions (classe *Detection_Approaches*). Trois principales classes sont utilisées. (1) La classe *Anomaly_Detection* consistant à utiliser des techniques allant d'heuristiques à de la fouille de données et celles basées sur les réseaux de neurones pour

comparer le comportement courant du système à un comportement antérieur précédemment qualifié de normal. (2) La classe *Misuse_Detection* utilise pratiquement les mêmes techniques pour comparer les différentes signatures générées à celles d'une base de connaissances de signatures malsaines. La *classe Specification_base_rules* permet d'utiliser des règles simples et précises pour détecter les intrusions. Certaines recherches [DAS 05][STR 07] ont optés pour des solutions hybrides et sont représentés dans la classe *hybrid.*

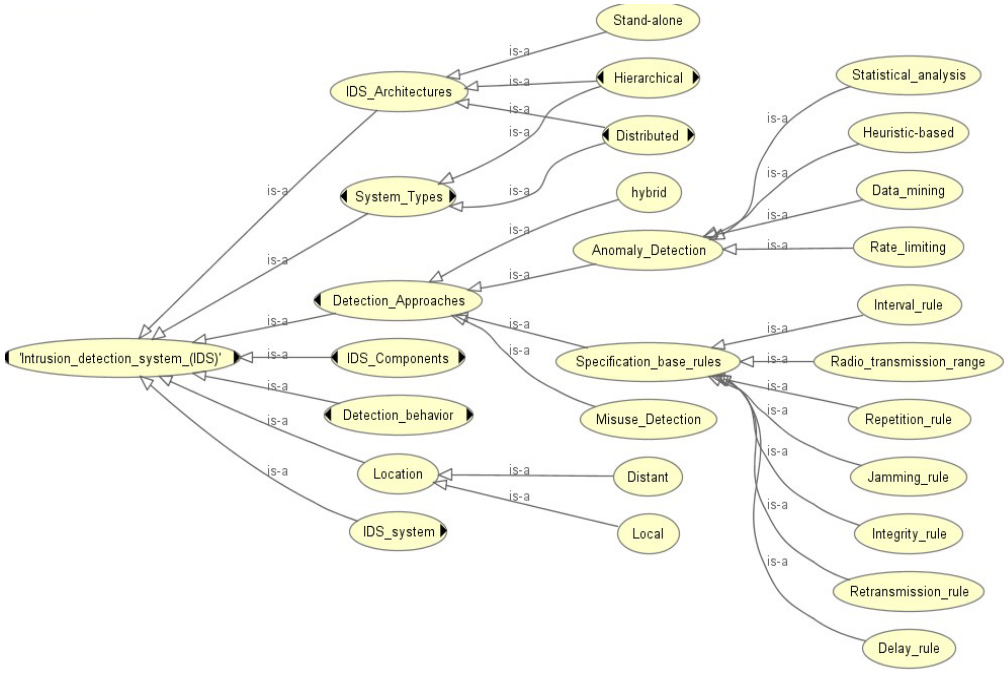

Figure 7. Ontologie opérationnelle des politiques de sécurités

4. Exploitation de l'ontologie proposée

Une ontologie est un système structuré de concepts qui permet de couvrir un champ bien défini (ici la description des intrusions) et qui permet de présenter la réalité sous la forme d'un modèle. Cette proposition va permettre de construire à partir de cette base de connaissances un moteur générique de gestion d'intrusions. La sélection et le choix des algorithmes de recherche et de mise jour de l'ontologie s'avère nécessaire pour réaliser ce moteur.

L'algorithme de mise à jour va permettre d'enrichir l'ontologie. Cela signifie que si un nouveau concept du domaine non pris en compte par l'ontologie survient, il faut que le moteur soit capable de l'ajouter à la classification.

Le but de notre ontologie d'intrusion dans les RCSFs est donc de rendre un moteur de gestion (détection/prévention) d'intrusions basé sur la sémantique des intrusions plus pertinent et fiable. Celle construite dans cet article est faite dans protégé 4.1 qui est un logiciel open source

permettant l'édition et la création des ontologies en utilisant le langage et le format OWL (*Web Ontology Language*).

5. Conclusion

Ce papier propose une description formelle de différentes intrusions dans les RCSFs en utilisant une ontologie. Dans cette ontologie nous considérons la détection d'intrusion aussi bien du point de vue *sticky_values*, du point de vue *given_services* que du point de vue *security_policy*. La description des concepts du domaine et la mise en évidence des relations existantes entre ces concepts via l'ontologie va permettre la mise en place de solutions de détection des intrusions plus efficaces et plus fiables.

Par la suite nous nous proposons de construire une plateforme de validation d'intrusion l'idée est d'offrir un procédé d'identification de l'intrusion basé sur la sémantique des intrusions survenue avant de faire appel aux différents mécanismes de détections des intrusions. Ceci pourrait fournir un moyen de réduction de la quantité de fausses alertes générées par les systèmes de détection des intrusions.

6. Bibliographie

[BYU 06] B YU, B XIAO « Detecting selective forwarding attacks in wireless sensor networks. » *IPDPS 2006: 20th International Parallel and Distributed Processing Symposium*, 2006: 8–15.

[BHA 07] BHAVIK PAREKH , ÇAM HASAN. « Minimizing False Alarms on Intrusion Detection for Wireless Sensor. », *Cam, Hasan; Military Communications Conference, 2007. MILCOM 2007. IEEE; Oct. 29-31, 2007 pp. 1-7; Digital Object Identifier 10.1109/MILCOM.2007.4455315*

[CHE 09] CHEN R HSIEH CH., HUANG Y. « A New Method for Intrusion Detection on Hierarchical Wireless Sensor Networks » *Proceedings of the ICUIMC-09, Suwon, Korea*, January 2009: 238-245.

[DAS 05] DA SILVA A. , P. MARTINS ,M. ROCHA B., LOUREIRO A., RUIZ L. , C. WONG H. « Decentralized intrusion detection in wireless sensor networks. » *in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks (Q2SWinet '05). ACM Press*, October 2005: 16–23.

[DAV 95] DAVID ICOVE, SEGER KARL , R. VONSTORCH WILLIAM. « *Computer crime: a crime fighter's handbook* ». Sebastopol CA USA : O'Reilly & Associates, Inc., 1995.

[ERM 06] ERMIS E.B , SALIGRAMA V. « Detection and Localization in Sensor Networks Using Distributed FDR. » *in proceedings of Conference on Information Sciences and Systems (CISS)*, 2006.

[FAT 07] FATIHA BENALI LEGRAND VÉRONIQUE , STÉPHANE UBÉDA. « An ontology for the management of heteregenous alerts of information system. » *In The 2007 International Conference on Security and Management (SAM'07)*, June 2007.

[FRE 97] FREDERICK B. COHEN. « Information system attacks: A preliminary classification scheme. » *In Computers and Security*, 1997: 29-46.

[GAN 04] GANERIWAL S , M B SRIVASTAVA. « Reputation-based Framework for High Integrity Sensor Networks. » *in ACM Security for Ad-hoc and Sensor Networks (SASN 2004)*, 2004.

[GUL 05] GU L., AL. « Lightweight detection and classification for wireless sensor networks in realistic environments. » *In: Proc. of the 3rd international conference on Embedded networked sensor systems (SenSys '05)*, November 2005: 205-217.

[IOA 07] IOANNIS CHATZIGIANNAKIS , STRIKOS ANDREAS. « A Decentralized Intrusion Detection System for Increasing Security of Wireless Sensor Networks. » *12th IEEE Conference of Emerging Technologies and Factory Automation*, 2007: 1408-1411.

[JIN 09] JING-WEN TIAN, GAO MEI-JUAN, HE LING-FANG , ZHOU SHI-RU. « community intrusion detection system based on wavelet. » *Proceedings of the Eighth International Conference on Machine Learning and Cybernetics Baoding*, July 2009: 12-15.

[KAC 02] KACHIRSKI OLEG , RATAN GUHA. « Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks. » *in Proceedings of the IEEE of the 36th Hawaii International Conference on System Sciences*, 2002.

[KET 08] KETEL MOHAMMED. «Applying the Mobile Agent Paradigm to Distributed Intrusion Detection in Wireless Sensor networks.» *40th Southeastern Symposium on System Theory, IEEE.*, 2008: 16-18.

[MAJ 08] MAJORCZYK FRÉDÉRIC. « Détection d'intrusions comportementale par diversification de COTS : application au cas des serveurs web. » Thèse de doctorat, Matisse SSIR, Université de Rennes 1, Rennes, 2008.

[MAR 09] MARKUS WÄLCHLI , BRAUN TORSTEN. « Building Intrusion Detection with a Wireless Sensor Network. », *First International Conference on Ad Hoc Networks , Niagara Falls, Ontario, Canada, September 23 - 25, 2009, pp. 607-622*

[MEC 03] MECHITOV K. SUNDRESH S. KWON Y. , AGHA G. « Cooperative tracking with binary-detection sensor networks. » *in proceedings of UIUCDCS-R-2003-2379, (Computer Science Dept., University of Illinois at Urbana-Champaign)*, 2003.

[NEU 95] NEUMANN PETER G. « Computer related risks. » *ACM Press/Addison-Wesley Publishing Co*, 1995.

[ONA 05] ONAT I , A MIRI. « An intrusion detection system for wireless sensor networks. » *in Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2005 August: 253–259.

[CHE 09] R. CHEN HSIEH CH. , HUANG Y. « A New Method for Intrusion Detection on Hierarchical Wireless Sensor Networks. » *Proceedings of the ICUIMC-09, Suwon, Korea*, January 2009: 238-245.

[ROM 05] ROMAN R , AL. « Applying Intrusion Detection Systems to Wireless Sensor Networks. » *Proceedings of 2005 ICCSA Workshop on Internet Communications Security, LNCS 3482*, 2005 May: 681-690.

[SOB 06] SOBH T S. « Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. » *computer Standards & interfaces* 28 2006: 670-694.

[STR 07] STRIKOS A. A. « A full approach for intrusion detection in wireless sensor networks. » *School of Information and Communication Technology*, KTH, Mar. 2007.

[SUM 08] SUMANTA SAHA , SAIFUL ISLAM MAMUN MOHAMMAD. « A novel overlay IDS for wireless sensor networks. » *IADIS International Conference Wireless Applications and Computing*, 2008: 144-148.

[SUN 07] SUN BO OSBORNE LAWRENCE XIAO YANG , GUIZANI SGHAIER. « Intrusion detection techniques in mobile ad hoc and wireless sensor networks. » *IEEE Wireless Communications*, 2007 October: 45-63.

[ULF 97] ULF LINDQVIST , JONSSON ERLAND. « How to systematically classify computer security intrusions. In SP '97. » *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, 1997: 154.

[VAS 10] VASSEUR J.P, DUNKELS A. « Interconnecting Smart Objects with IP » *Elsevier edition ISBN 978-0-12-375165-2, 2010.*