Contribution à l'adoption des IDS dans l'IoT

Olivier Lourme, Michaël Hauspie
Université de Lille, CNRS, IRCICA, Centrale Lille, UMR9189 - CRIStAL
Centre de Recherche en Informatique Signal et Automatique de Lille, F-59000 Lille
prenom.nom@univ-lille.fr

***Abstract*—L'Internet des Objets (*Internet of Things*, IoT) est un modèle en plein essor dans le traitement de l'information. En termes de sécurité, l'hétérogénéité et la spécificité des protocoles utilisés, la variété des objets et leurs faibles ressources, combinées aux pressions commerciales, conduisent à des solutions moins matures et moins robustes que celles disponibles dans l'IT (*Information Technologies*), offrant ainsi une nouvelle surface d'attaque, souvent exploitée. Dans ce cadre, le développement de Systèmes de Détection d'Intrusions (IDS) adoptés à l'IoT est un champ de recherche foisonnant ; il est cela dit rarement abordé sous l'angle de l'adoption grand public, faisant par exemple abstraction du caractère éminemment hétérogène de ce contexte. Nous rappelons dans cet article une taxonomie des IDS pour recenser ensuite formellement les caractéristiques d'un IDS candidat à une adoption dans un environnement grand public de type *smart home*. Une architecture est également proposée.**

I. Introduction

Au déploiement du modèle IoT s'associent logiquement de nombreuses attaques, conduisant par exemple à des fuites de données, des dénis de service ou des détournements d'usage. Protéger les réseaux d'objets est un défi majeur car ceux-ci sont essentiellement caractérisés par :

- des ressources contraintes en termes de mémoires, capacités de traitement et débits d'émission-réception, induisant des implémentations de sécurité dégradées, souvent accentués par des exigences de basse consommation énergétique ;
- une forte hétérogénéité des microcontrôleurs, des topologies de réseau et des modulations et protocoles – ouverts ou propriétaires – utilisés par les puces radio, dispersant les efforts de sécurisation.

Certes, les fabricants de solutions IoT sont de plus en plus conscients de l'intérêt de commercialiser des produits sûrs mais de nombreux biais subsistent, surtout dans les segments grand public, par exemple de type *smart home*. D'abord, la culture de la sécurité et l'expertise dans l'écriture de *firmwares* peuvent être faibles ; ensuite, la possibilité de mise à jour de ceux-ci pour pallier une vulnérabilité découverte est rarement envisagée. Les lignes directrices guidant la conception semblent plutôt être la réduction du *time to market* et des coûts, l'offre de nouvelles fonctionnalités et la recherche d'une utilisation sans friction. En outre, de manière générale, le mode promiscuité naturel des réseaux sans fil utilisés permet facilement le brouillage, l'écoute passive voire l'injection de messages, sans que l'attaquant – à ressources illimitées – ne se fasse remarquer physiquement.

En attendant une meilleure considération des points critiques de la sécurité dans l'IoT, un grand nombre d'attaques couronnées de succès a lieu, à l'image de celles décrites et classées dans [1]. Pour un IoT plus sûr, d'astucieux systèmes de détection d'intrusion (*Intrusion Detection Systems*, IDS) identifiant les attaques et les remontant sont proposés dans la littérature mais très peu ont comme approche le caractère hétérogène des environnements IoT, ce qui restreint leur diffusion. Ainsi, la Section II rappelle une taxonomie des IDS dans l'IoT afin d'établir dans la Section III les exigences d'un IDS à spectre plus large, susceptible d'être adopté dans des contextes grand public. La Section IV propose une architecture réaliste pour un tel IDS et la Section V conclut cet article tout en présentant nos travaux futurs.

II. Une taxonomie des IDS dans l'IoT

A. Définition d'un IDS

Un IDS est un outil de protection censé détecter les attaques contre un réseau ou un hôte en analysant l'activité dans le réseau (*Network* IDS) ou dans l'hôte (*Host* IDS).

B. Critères pour la taxonomie des IDS

Les trois critères d'une taxonomie communément admise pour les IDS dans l'IoT [2] sont décrits ci-après :

1) Critère « stratégies de placement » : Ce critère correspond à la répartition réalisée entre HIDS et NIDS. Un HIDS est placé sur l'hôte et en partage les faibles ressources. Il a cependant accès à des données fines de ce dernier tels les journaux ou appels système, voire à des données auxiliaires comme la consommation électrique ou la température. Un accès à de la donnée déchiffrée est envisageable. Au contraire, en s'intégrant dans un nœud du réseau comme la passerelle ou dans un système dédié, les NIDS disposent en général de capacités de traitement et de stockage importantes, laissant entrevoir une utilisation confortable des méthodes de détection abordées peu après. Ils ont accès à un autre type de données que les HIDS mais parfois ces données sont chiffrées. Ainsi, en combinant HIDS et NIDS pour constituer un IDS complet, on obtient par exemple : un « placement distribué » en implémentant un HIDS léger dans chaque objet, un « placement centralisé » avec un NIDS exploitant les données d'une ou plusieurs sondes [3] ou un « placement hybride » avec un NIDS et des HIDS, l'ensemble collaborant.

2) Critère « méthodes de détection » : La « détection de signatures » compare la charge utile des messages à des signatures d'attaques enregistrées dans une base de données. Cette méthode ne détecte que des attaques connues et sa performance est conditionnée à une maintenance rigoureuse

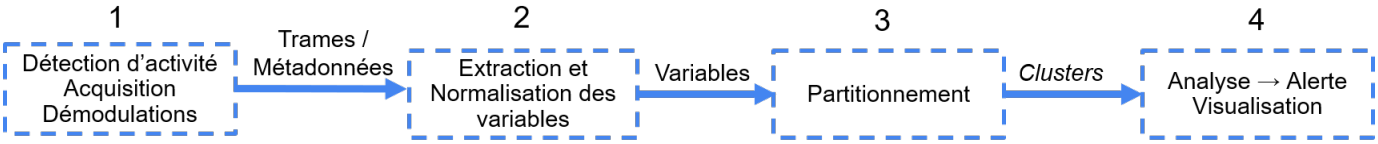

Fig. 1. Architecture de l'IDS proposé

de la base sous peine d'obtenir beaucoup de faux négatifs. Elle souffre en outre d'un coût conséquent de stockage et de traitement, non compatible avec des systèmes contraints. D'un autre côté, la « détection d'anomalies » compare le comportement du système à un modèle normal, le dépassement d'un seuil d'écart traduisant une attaque. Cette méthode est efficace pour détecter les nouvelles attaques, nombreuses dans l'IoT, y comprises les attaques *zero-day*. Logiquement, cette méthode peut souffrir d'un nombre excessif de faux positifs. Dispensant de la synthèse complexe d'un modèle par un expert, les techniques d'apprentissage de l'intelligence artificielle sont souvent employées mais elles ne peuvent être hébergées que dans des nœuds avec assez de ressources. Des approches hybrides mêlant les deux méthodes existent dans la littérature.

3) Critère « attaques détectées » : Généralement, les IDS rencontrés dans l'état de l'art se concentrent sur une technologie IoT, puis, au sein de celle-ci, adressent un ou deux cas d'attaques, par exemple « *DoS attack in 6LoWPAN* ». Nous choisissons plutôt de nous inscrire dans une approche basée sur l'hétérogénéité de l'IoT, à l'image de travaux plus rares [3] [4], espérant que celle-ci, plus en phase avec la réalité de ce modèle, conduise à une meilleure diffusion des IDS.

III. Caractéristiques d'un IDS pour l'IoT susceptible d'être adopté

Nous intéressant à un contexte *smart home* faisant figurer des technologies Zigbee, BLE, WiFi, 433 MHz, etc., l'IDS à synthétiser se doit d'être multi-technologies, simple d'usage et bon marché. Ces trois critères permettent de reparcourir la taxonomie en y arrêtant aisément les choix initiaux suivants : L'IDS recherché doit être un NIDS centralisé (son caractère unique permettant une maîtrise des coûts de développement et d'exploitation), couvrir plusieurs technologies et pouvoir être mis à jour. En outre, l'IDS doit être non invasif et ne pas nécessiter de connaissance *a priori* de l'environnement où il est placé : canaux, identifiants de réseau et clés de chiffrement. Par ailleurs, maintenir une base des signatures d'attaques est complexe dans le cadre hétérogène de l'IoT et nous souhaitons détecter même les nouvelles attaques. De ce fait, notre IDS sera d'abord basé sur la détection d'anomalies. Dans ce domaine, les algorithmes de *Machine Learning* et de *Deep Learning* sont réputés efficaces mais doivent être implémentés dans un hôte puissant. Retenir un algorithme n'est pas trivial mais nous optons sans surprise pour un critère économique : Dans les méthodes supervisées, l'obtention de données d'entraînement et de validation, puis leur étiquetage en « Intrusion effective » ou en « Absence d'intrusion » sont des étapes amont manuelles très coûteuses, surtout lorsqu'il faut les reproduire pour différentes technologies. Dans un contexte IT, [5] a au contraire utilisé pour son IDS une méthode d'apprentissage non supervisée, le partitionnement. Ainsi, les données n'ont pas à être étiquetées et des *clusters* sont établis automatiquement, groupant les situations selon leurs ressemblances. En faisant l'hypothèse réaliste que les attaques sont rares et statistiquement différentes des situations normales, ces premières vont se retrouver dans des *clusters* spécifiques à faible densité, ce qui permettra de les détecter.

IV. Architecture proposée

L'architecture de l'IDS que nous proposons, en phase avec la section précédente, est donnée Fig. 1. Le bloc 1 est implémenté *a priori* par une sonde de type *Software-Defined Radio* avec autant de démodulateurs logiciels en aval que de technologies à couvrir, laissant entrevoir un système évolutif *via* des mises à jour à distance, à coût matériel maîtrisé.

V. Conclusion

Après avoir rappelé les faiblesses intrinsèques de sécurité du modèle IoT et montré la nécessité de solutions de protection, nous avons pu à travers une taxonomie des IDS recenser formellement les caractéristiques que devrait revêtir un IDS adopté significativement dans les contextes hétérogènes grand public de type *smart home*. Le placement centralisé et la détection d'anomalies *via* un algorithme de partitionnement nous semblent être une combinaison intéressante dont nous allons évaluer la pertinence dans nos travaux futurs.

References

[1] H. Tschofenig and E. Baccelli, "Cyberphysical Security for the Masses: A Survey of the Internet Protocol Suite for Internet of Things Security," *IEEE Security Privacy*, vol. 17, no. 5, pp. 47–57, Sep. 2019, conference Name: IEEE Security Privacy.

[2] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, Apr. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517300802

[3] J. Roux, E. Alata, G. Auriol, M. Kaâniche, V. Nicomette, and R. Cayre, "RadIoT: Radio Communications Intrusion Detection for IoT - A Protocol Independent Approach," in *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, Nov. 2018, pp. 1–8.

[4] S. Siby, R. R. Maiti, and N. O. Tippenhauer, "IoTScanner: Detecting Privacy Threats in IoT Neighborhoods," in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*, ser. IoTPTS '17. New York, NY, USA: Association for Computing Machinery, Apr. 2017, pp. 23–30. [Online]. Available: http://doi.org/10.1145/3055245.3055253

[5] L. Portnoy, "Intrusion detection with unlabeled data using clustering," Ph.D. dissertation, Columbia University, 2000. [Online]. Available: https://doi.org/10.7916/D8MP5904