Détection des attaques d'usurpation dans les maisons connectées par analyse du RSSI

Olivier Lourme, Michaël Hauspie

Détection des attaques d'usurpation dans les maisons connectées par analyse du RSSI

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*—Les réseaux d'objets au sein des maisons connectées constituent des écosystèmes fragiles en termes de sécurité en raison de leur hétérogénéité, de leurs faibles ressources, d'une conception économique favorisant les failles et de leur gestion par des utilisateurs peu sensibilisés. Ces objets sont particulièrement perméables aux attaques d'usurpation d'identité où un attaquant adopte l'identifiant d'un nœud légitime pour effectuer des actions privilégiées auprès d'une victime ou entrainer une rupture du service rendu. Afin de bâtir un système de détection d'intrusions (IDS) combattant ces attaques, nous associons l'identifiant logique annoncé par un objet à une empreinte fournie par sa couche physique, difficilement falsifiable. L'IDS étant destiné à l'écosystème maison connectée, la caractéristique retenue est le *Received Signal Strength Indicator* (RSSI), d'un accès facile et disponible pour tous les protocoles sans fil. Ainsi, l'IDS en écoute passive se charge de déterminer si le profil RSSI de tout objet prenant la parole est cohérent avec l'identifiant qu'il annonce. Dans le cas contraire, une alarme est générée. Les objectifs de ce papier sont triples : (i) montrer que malgré sa grande volatilité dans les environnements changeants comme ceux de la maison connectée, le RSSI est une caractéristique concourant à de bonnes métriques de détection s'il est utilisé avec un réseau à cellules récurrentes LSTM (*Long Short-Term Memory*), (ii) présenter à la communauté notre dataset Zigbee constitué pendant 10 jours et portant sur 10 objets, (iii) proposer un IDS réaliste de bout en bout, en phase avec les contraintes spécifiques de la maison connectée.**

***Index Terms*—Maison connectée, Sécurité, IDS, RSSI, Apprentissage profond, LSTM, dataset.**

I. Introduction

Une attaque par usurpation d'identité a lieu lorsqu'un attaquant prend l'identité d'un nœud légitime pour mener des actions inappropriées sur un nœud victime. Dans l'extrait de réseau Zigbee de la Figure 1, l'identité d'un objet est assurée par l'identifiant « adresse courte 16 bits » de couche liaison IEEE 802.15.4. Le capteur de mouvement 0x0A12 se réveille plusieurs fois par minute et demande à son nœud parent 0x7C77, ici une ampoule connectée, si celui-ci a reçu des données à son attention au cours de son sommeil. 0x0A12 formule cette demande avec une trame IEEE 802.15.4 dite de *Data Request*. Dans une attaque par usurpation [1] de type *Masquerade*[1], un attaquant peut usurper l'identité de 0x0A12 en forgeant à son tour des trames *Data Request* avec cette adresse source. Si cela se répète plusieurs centaines de fois par minute, la victime 0x7C77 va se mettre à manquer de réactivité dans le traitement des ordres d'allumage/extinction, une forme de déni de service. Les choses peuvent aller plus loin : L'utilisateur voyant son objet mal fonctionner le réinitialise afin de le réassocier au réseau Zigbee. Or c'est pendant cette étape que la clé de chiffrement des couches hautes est communiquée. Avec l'obtention de cette crédence par une simple écoute passive, l'attaquant peut par la suite tenter des attaques d'usurpation au niveau des couches hautes (réseau, application) et parvenir à une compromission encore plus importante du réseau.

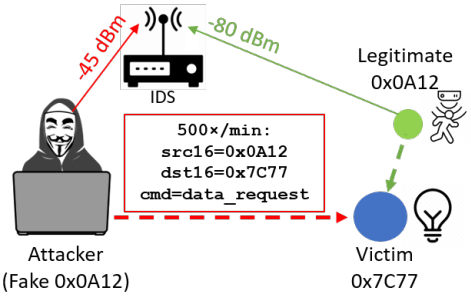

Figure 1. Usurpation d'identité dans un réseau Zigbee

Pour détecter ces attaques, une solution est d'associer une caractéristique de la couche physique à l'identifiant de l'objet. Celle-ci étant difficilement imitable, une trame avec un identifiant source (logique) ne correspondant pas à son empreinte (physique) sera symptomatique d'une attaque et une alarme pourra être déclenchée.

Élaborer des systèmes de détection d'intrusions (IDS) est un challenge difficile dans l'écosystème maison connectée car celui-ci fait figurer sans cesse de nouveaux objets, très hétérogènes et à faibles ressources, dont la conception guidée par le coût laisse peu de place à la sécurité. Ces objets sont aussi pour la plupart d'entre eux déjà déployés et leur gestion par des utilisateurs non-experts ne permet pas d'envisager des protections réclamant beaucoup d'intervention humaine.

Pour ces raisons, nous choisissons pour notre IDS de retenir le RSSI (*Received Signal Strength Indicator*) comme empreinte de couche physique, qui, certes connu pour sa sensibilité aux changements d'environnement, est immédiatement disponible sous la forme d'un simple scalaire sur tous les protocoles (à des fins de *Clear Channel Assess-*

[1]Les attaques par usurpation de type *Sybil* ne sont pas abordées dans ce court article.

ment), à l'opposé d'autres caractérisations complexes nécessitant un travail préalable d'enregistrement non réaliste avec l'écosystème maison connectée [1].

La Section II présente le RSSI dans le contexte qui nous préoccupe. La Section III établit le modèle des attaques que nous souhaitons combattre. En Section IV, les caractéristiques du dataset Zigbee que nous avons constitué pour évaluer nos travaux sont exposées. La Section V décrit la synthèse et le test d'un IDS détectant les attaques d'usurpation. Enfin, la conclusion et les travaux futurs sont en Section VI.

II. Le RSSI pour la couche physique

Le RSSI correspond à une mesure de la puissance moyenne arrivant sur un récepteur, convertie en dBm. En extérieur sans obstacle, la puissance reçue varie avec la puissance d'émission et l'inverse du carré de la distance émetteur-récepteur. Si émetteur et récepteur restent fixes et que l'émetteur ne change pas sa puissance d'émission, un récepteur mesure toujours la même valeur de RSSI pour un émetteur donné, ce qui est une sorte d'authentification. Cette idée est traduite sur la FIGURE 1 où le récepteur est la sonde d'un IDS.

À l'intérieur, dans un environnement statique, le principe reste applicable même si les réflexions du signal génèrent des chemins multiples pour les ondes, avec des interférences inter-symboles à l'arrivée et donc un signal de plus faible qualité. En outre, l'association identifiant-RSSI n'est pas du tout bijective. Pour pallier ces points, on peut déployer plusieurs sondes dans le domicile et caractériser un émetteur par un tuple de RSSI. Ce type de détection n'est pas neuve, elle a par exemple été explorée dans [2]. Cela dit, dans ce travail et dans beaucoup d'autres, les mesures de validation se déploient dans des environnements peu en rapport avec ceux sans cesse redessinés d'une maison connectée vivante où les phénomènes physiques précités semblent rendre le RSSI stochastique. En outre, la question de la centralisation des informations des sondes par un autre réseau, lui aussi vulnérable, reste entière.

Sur la FIGURE 2 en bas, on peut observer le RSSI de l'identifiant 0x0A12 capturé sur toute la journée du 08/07/2022 par une des 4 sondes implantées dans une maison de test. On voit que le RSSI est très stable pendant la nuit où la maison dort mais que pendant le reste de la journée il est très difficile d'associer à 0x0A12 une valeur emblématique de RSSI.

III. Modèle d'attaque

Nous considérons dans un premier temps le cas d'un attaquant positionné fixement à côté de la maison victime, émettant des trames illégitimes à puissance constante. Les objets qu'il souhaite attaquer sont fixes et ne varient pas leur puissance d'émission. L'attaquant n'est pas muni de la clé réseau ; il tente seulement des attaques d'usurpation très simples sur la couche liaison comme celle décrite dans le premier paragraphe de la Section I.

IV. Dataset Zigbee disponible en open data

Afin d'établir pour chaque objet des modèles de normalité en termes de RSSI puis de les tester, nous avons constitué un jeu de données Zigbee que nous avons rendu disponible à la communauté afin qu'elle puisse tester dessus ses propres algorithmes de détection[2]. Les jeux de données Zigbee sont extrêmement rares dans la littérature. Le nôtre présente les caractéristiques suivantes :

- 10 jours de capture dans une maison à deux étages ;
- en conditions réelles : personnes, meubles, réseaux ;
- 10 objets Zigbee : fichiers PCAP par sonde et par heure ;
- 4 sondes (CC2531[3]-Raspberry Pi) en écoute passive réparties dans la maison ;
- pour l'entraînement et le test : périodes sans attaque et périodes avec diverses attaques référencées.

V. IDS proposé

A. Description: implémentation et type d'apprentissage

Tel que montré dans [3], un IDS réaliste de maison connectée doit être centralisé (non distribué dans les objets), non intrusif, autonome dans sa découverte d'un réseau déjà déployé et doté de suffisamment de ressources pour supporter l'algorithme de détection et ses mises à jour. Outre présenter des bonnes métriques de détection, ce dernier doit être basé sur des méthodes d'apprentissage non supervisées pour concourir à un coût global modique, la labellisation des situations d'entraînement propres à chaque domicile étant onéreuse et laborieuse. Cela dit, utiliser un algorithme comme One-Class SVM reposant uniquement sur les valeurs du RSSI génère des résultats décevants [4]. Effectivement, les RSSI ne sont ni stationnaires, ni IID (*Independent and Identically Distributed*), ils font partie de séquences temporelles que les modèles doivent intégrer. Poursuivant une idée amorcée dans [4], nous optons pour une solution d'apprentissage profond de type auto-encodeur à cellules LSTM (*Long Short-Term Memory*) [5, p. 580]. L'auto-encodeur est entraîné avec en entrée des séquences de RSSI standardisé, sans attaque, et ajuste au mieux ses poids pour reconstruire en sortie des séquences les plus proches possibles de celles en entrée. Ainsi, en test, une erreur « de reconstruction » trop importante entre la sortie prédite (à l'aide du modèle et de l'entrée effective) et la sortie effective témoigne d'une séquence anormale et donc probablement d'une attaque. Les réseaux à base de LSTM sont une branche des RNN (*Recursive Neural Networks*) qui adresse la faible capacité de mémorisation à long terme de ces derniers.

B. Expérimentation et résultats

1) Établissement du modèle: À partir de notre dataset, nous avons recensé sur la journée du 02/07/2022 sans attaque, toutes les trames correctes présentant comme identifiant source 0x0A12, depuis une des 4 sondes installées. Nous avons bâti des séquences glissantes de 30 RSSI successifs. Celles-ci ont constitué le jeu d'entraînement d'un auto-encodeur à deux couches de 128 LSTM, avec un optimiseur de type Adam. La plus grande des erreurs de reconstruction obtenue sur le

[2]https://doi.org/10.57745/NDW74U

[3]Précision RSSI : +/-4 dB (plage d'env. 40 dB) ; quantification : 1 dBm

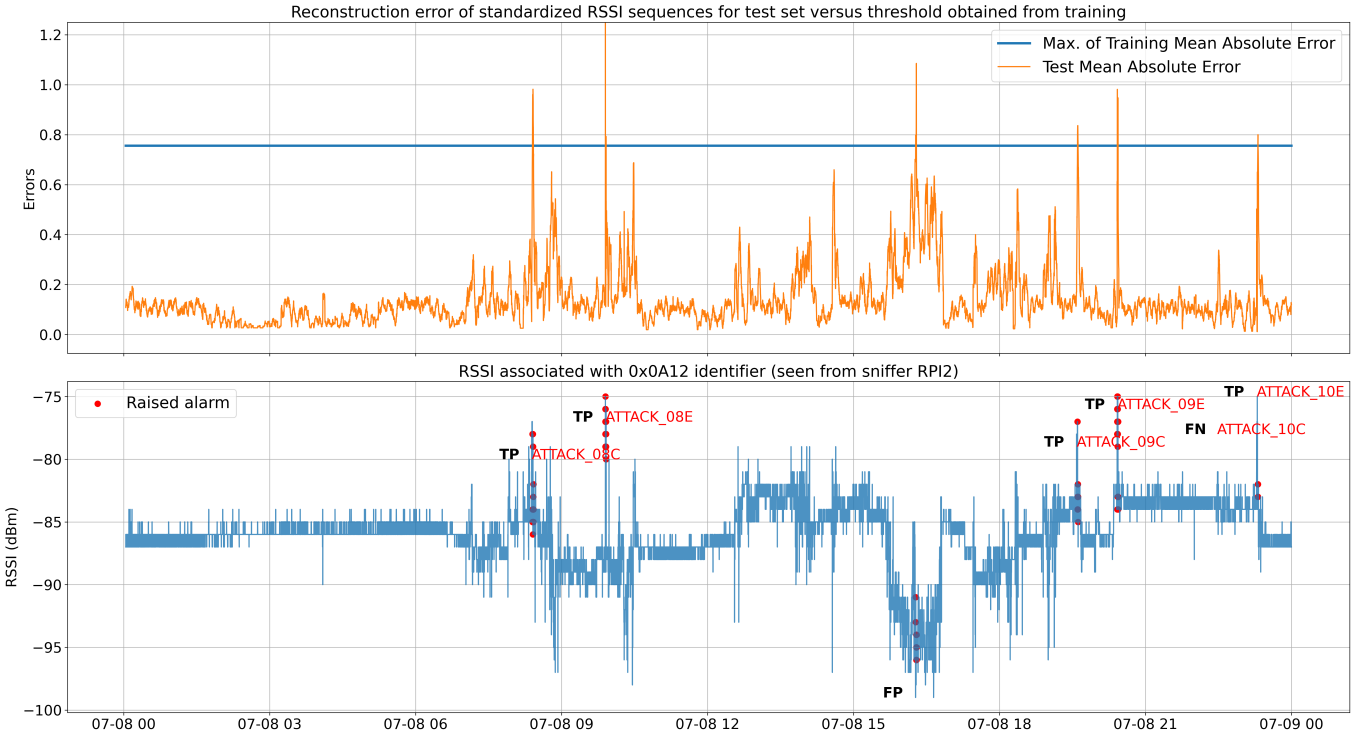

FIGURE 2. Test du 08/07/2022 : Erreur de reconstruction des séquences RSSI (en haut) et RSSI associé à l'id. 0x0A12, vu du sniffer RPI2 (en bas)

jeu d'entraînement a été retenue pour définir le seuil que celle de test doit dépasser pour considérer qu'une attaque a lieu.

2) Test: Sur toute la journée du 08/07/2022, en marge des activités normales, nous avons injecté dans le réseau Zigbee 6 attaques à base de *Data Request* contre la victime 0x7C77, depuis un attaquant usurpant l'adresse source 0x0A12. Les attaques dont la référence finit par C sont à 12 trames illégitimes par minute (du même ordre que les trames légitimes), celles dont la référence finit par E sont à 500 trames illégitimes par minute. Le RSSI de cette journée de test est tracé sur la FIGURE 2 en bas. L'erreur de reconstruction ainsi que le seuil d'alarme sont tracés sur la FIGURE 2 en haut.

3) Métriques: Par la suite, nous découpons le temps en tranches de 10 minutes pour relever dans chacune attaques effectives et alarmes levées et ainsi établir les nombres de vrais négatifs (TN), vrais positifs (TP), faux négatifs (FN) et faux positifs (FP) ainsi que les métriques classiques « justesse » (Acc), « précision » (Prec), « rappel » (Rec), « Taux de Vrais Négatifs » (TNR) et « Taux de Faux Positifs » (FPR) [5, p. 91]. Celles-ci sont données dans le TABLEAU I. Ces bons résultats montrent que, malgré le caractère volatile du RSSI en environnement changeant, le choix de cette empreinte de couche physique aisément accessible s'avère pertinent en termes de détection.

TABLEAU I
MÉTRIQUES DE L'IDS ÉTUDIÉ

TN	TP	FN	FP	Acc	Prec	Rec	TNR	FPR
136	5	1	1	98.6%	83.3%	83.3%	99.3%	0.7%

VI. CONCLUSION

Dans cet article, nous avons montré que dans le contexte de la maison connectée, le RSSI est un candidat de couche physique réaliste, malgré son caractère volatile. Proposant des choix d'implémentation et un algorithme d'apprentissage adaptés au contexte, nous avons obtenu un IDS dont le modèle de détection a été établi et testé grâce à un dataset rendu public. Très encourageantes, les métriques obtenues pourraient sans doute être améliorées par une construction incrémentale du modèle et la corrélation d'informations issues d'au moins deux sondes.

REFERENCES

[1] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device Fingerprinting in Wireless Networks: Challenges and Opportunities," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 94–104, 2016.

[2] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proceedings of the 5th ACM workshop on Wireless security*, ser. WiSe '06. New York, NY, USA: Association for Computing Machinery, Sep. 2006, pp. 43–52. [Online]. Available: http://doi.org/10.1145/1161289.1161298

[3] O. Lourme and M. Hauspie, "Toward a realistic Intrusion Detection System dedicated to smart-home environments," in *2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct. 2021, pp. 80–85, iSSN: 2160-4894.

[4] P. Madani and N. Vlajic, "RSSI-Based MAC-Layer Spoofing Detection: Deep Learning Approach," *Journal of Cybersecurity and Privacy*, vol. 1, no. 3, pp. 453–469, Sep. 2021, number: 3 Publisher: Multidisciplinary Digital Publishing Institute.

[5] A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, 2nd Edition [Book]*. O'REILLY, 2019.