Classification Adaptative des attaques IEMI et protocolaires sur les réseaux de communication IEEE 802.11 *

Jonathan VILLAIN[1], Virginie DENIAU[2], Anthony FLEURY[1], Eric Pierre SIMON[3], Cristophe GRANSART[2]

[1]IMT Lille Douai, Univ. Lille, Unité de Recherche Informatique et Automatique (URIA), F-59000 Lille, France.

[2]IFSTTAR, French Institute of Science and Technology for Transport, Development and Networks, Villeneuve d'Ascq, 59650 France.

[3]IEMN lab, TELICE group, University of Lille, F-59000 Lille, France.

jonathan.villain@imt-lille-douai.fr, virginie.deniau@ifsttar.fr, anthony.fleury@imt-lille-douai.fr, eric.simon@univ-lille.fr, christophe.gransart@ifsttar.fr

Résumé – Dans ce travail, nous avons évalué les performances d'un algorithme de classification adaptative et en ligne (SAKM – classifieur à noyau auto-adaptatif) pour la reconnaissance automatique et en ligne d'attaques sur des communications Wi-Fi (protocole 802.11n). Les résultats présentés ici font partie d'un projet plus vaste portant sur la surveillance du système sans fil. Les ondes radio sont faciles à écouter. En raison de l'évolution rapide des attaques disponibles, l'utilisation de l'algorithme d'apprentissage ne peut pas couvrir toutes les configurations. Le clustering en ligne construit des modèles évolutifs sans connaissance des différents cas à différencier. Il est donc bien adapté à ce type de problématique. Basé sur les méthodes de noyau SVM, l'algorithme SAKM utilise une procédure d'apprentissage adaptatif rapide pour prendre en compte les variations dans le temps.

Abstract – In this work, we evaluated the performances of anadaptive and online clustering algorithm (Self-Adaptative Kernel Machine SAKM) for the automatic and online recognition of attacks on wi-fi communication (802.11n protocol). The results presented here are part of a wider project dealing with wi-fi system monitoring. The radio waves are easy to listen. Due to the quick evolution in the available attacks, the use of learning algorithm cannot cover all configurations. Online clustering constructs evolving models without knowledge of the different cases to discriminate and are therefore well suited to this type of problematic. Based on SVM and kernel methods, the SAKM algorithm uses a fast adaptive learning procedure to take into account variations over time.

1 Introduction

Les communications par ondes radio sont couramment utilisées. Cependant, elles ont intrinsèquement une grande capacité à s'étendre dans toutes les directions avec une portée relativement grande. La principale conséquence de cette "propagation sauvage" des ondes radio électriques est la facilité avec laquelle une personne non autorisée écoute le réseau, éventuellement en dehors de l'emplacement où le réseau sans fil est censé être déployé et confiné. Les risques de mauvaise protection d'un réseau sans fil sont divers. Les réseaux utilisés dans le domaine du transport terrestre sont généralement hétérogènes, insuffisamment protégés et ne répondent pas aux exigences habituelles de la cybersécurité en matière de durabilité, de protection et de détection des attaques. Dans [1] nous nous sommes concentrés sur la conception d'un système de surveillance capable de détecter et classer les attaques par brouillage et les protocoles réseau attackson. Pour atteindre cet objectif, nous avons proposé d'externaliser la surveillance à partir du système et nous avons utilisé une antenne pour obtenir le spectre à chaque fois. Une étude du spectre montre que les fréquences d'intérêt sont localisées sur la fréquence centrale du canal entre 2.402 GHz et 2.422 GHz. En concentrant les analyses sur ces fréquences, cela permet de construire un modèle de classification pour résoudre le problème des interférences induites par une utilisation des canaux adjacents. Sur ces fréquences, les modèles d'estimation proposés montrent de bons résultats dans la prédiction des attaques. En raison de l'évolution rapide des attaques disponibles, l'algorithme d'apprentissage ne peut pas couvrir toutes les configurations. Dans ce cas, le regroupement en ligne construit des modèles évolutifs sans connaître les différents cas à discriminer. Dans cette étude, nous avons utilisé un algorithme en ligne pour surveiller la communication en utilisant les spectres électromagnétiques de la communication. Thealgorithm est basé sur une machine à vecteurs de

*Ce travail a été mené dans le cadre du projet ELSAT2020, cofinancé par l'Union européenne par le biais de Fonds européen de développement régional, l'État français et le Conseil régional des Hauts de France.

support appelée techniquement One-class-SVM et implémenté spécifiquement en tant qu'algorithme de nouvelle classification nommé SAKM [2]. Cet article est organisé comme suit. La section 2 présente la configuration d'expérimentation d'attaque EM considérée. La section 3 présente l'état des connaissances sur les méthodes de clustering en ligne SVM. La section 4 présente une analyse des résultats de l'algorithme et enfin nous terminons par la conclusion.

2 Protocol Experimental

Dans cette étude, l'acquisition des spectres est réalisée dans une chambre anéchoïde (voir Figure 1).

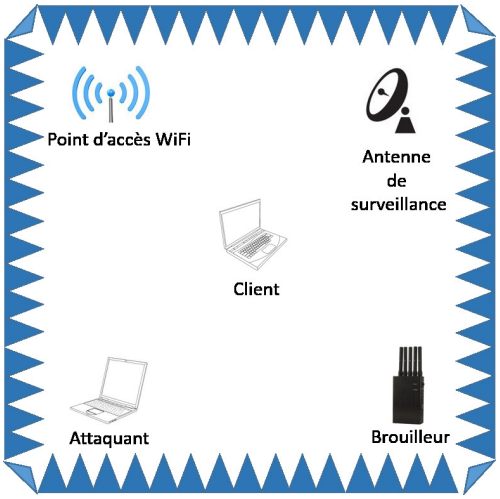


FIGURE 1 – Configuration des acquisitions

Le protocole de communication considéré est la norme IEEE 802.11n, qui utilise le schéma de modulation OFDM. Nous considérons deux modes d'attaque principaux : l'attaque par brouillage et l'attaque par désauthentification qui correspondent à une attaque de protocole. L'attaque par brouillage consiste à émettre un signal qui couvre les bandes de fréquences utilisées par le système de communication. Différents types de signaux de brouillage peuvent être utilisés [3]. La majorité des brouilleurs utilisent un signal d'interférence qui balaie une bande de fréquence $[f_1, f_2]$ sur une période de temps T pouvant être donnée par

$$s(t) = A\cos\left(2\pi\left(\frac{f_2 - f_1}{2T} + f_1\right)\right), \quad 0 < t < T, \qquad (1)$$

avec A l'amplitude du signal d'interférence. Le signal de brouillage que nous considérons balaie une bande de fréquences située entre $[2,4; 2,5]$ GHz en 10 μs. L'attaque par désauthentification consiste en une attaque par usurpation d'identité. Un attaquant envoie une trame de désauthentification à un périphérique sans fil, avec une adresse usurpée à partir du point d'accès. Le protocole ne nécessite aucun cryptage pour cette trame, même lorsque la session a été établie avec WEP (Wired Equivalent Privacy) ou avec des protocoles de cryptage renforcés. L'attaquant n'a besoin que de connaître l'adresse MAC de la victime, disponible en clair via le réseau sans fil. La communication wifi a été réalisée dans une chambre anéchoïque en installant un serveur, un point d'accès et un ordinateur client. Le canal à $2,412$ GHz (canal 1) a été utilisé. Nous avons inclus une antenne de surveillance à proximité du client. L'antenne de surveillance est connectée à un analyseur de spectre situé à l'extérieur de la chambre. Pour mettre en œuvre les attaques par brouillage, une autre antenne connectée à un générateur de forme d'onde arbitraire a été placée dans la chambre pour émettre le signal de brouillage. Pour les attaques de désauthentification, l'ordinateur qui émet le signal de désauthentification est placé près du client. L'analyseur de spectre est configuré comme suit : une plage de fréquences de 40 USD, une fréquence centrale de $2,412$ GHz, une largeur de bande de résolution de 100kHz. Le temps de balayage de l'analyseur de spectre était de $38,2$ μs. Pour évaluer les performances de la classification, nous mettons en œuvre 6 configurations distinctes. Une première configuration correspond à des acquisitions de spectres représentant uniquement des communications Wi-Fi. Une deuxième configuration consiste à dégrader la qualité de la communication mais sans aucune attaque. Pour cela, des absorbants électromagnétiques sont placés autour du point d'accès afin de dégrader la qualité du signal. Une troisième configuration avec un signal d'interférence faible. Le débit est toujours au niveau maximal (environ 95 Mbits/s). Une quatrième configuration utilise un niveau de puissance de signal d'interférence qui dégrade légèrement la qualité de la communication. Le débit est réduit à environ 75 Mbits/s. Une cinquième configuration utilise un niveau de puissance de signal d'interférence qui interrompt totalement la communication. La dernière configuration correspond à l'attaque de désauthentification. En raison du système d'acquisition des données dans le temps, la procédure d'acquisition est organisée en neuf étapes. Nous commençons par une communication wi-fi uniquement (39 spectres) suivie d'une communication en présence d'absorbeur (99 spectres). Nous passons ensuite à une communication Wi-Fi (20 spectres) suivie d'une phase d'attaque par désauthentification (99 spectres) et d'une phase de brouillage générant une perte de communication (99 spectres). Ensuite, nous revenons dans une phase de communication wi-fi (20 spectres) qui est suivie par une phase de brouillage qui fournit une modification de la communication. De nouveau, nous revenons sur une phase avec une communication wi-fi uniquement (20 spectres) suivie d'une phase de brouillage qui n'a aucun effet sur la communication (ce qui signifie que le taux de transfert n'est pas réduit par l'attaque (99 spectres)).

3 Self Adaptative Kernel Machine

SVM est une méthode permettant de déterminer un hyperplan optimal (en tenant compte de la marge) pour séparer deux classes [4]. L'estimation d'un support de distribution est introduite dans l'apprentissage supervisé par Schölkopf et al. [5].

Cela peut être vu comme une classification sans étiquette et l'estimateur développé s'appelle One-class-SVM. Le principe au-delà de la classification One-class est de détecter les nouveautés. La détection de nouveautés a de nombreuses applications pratiques dans la vie réelle dans différents domaines. Elle revêt une importance cruciale pour les applications impliquant de grands ensembles de données acquises à partir de systèmes critiques. Dans les applications en ligne, l'objectif est d'incorporer progressivement de nouvelles informations pour adapter la fonction d'apprentissage au fil du temps. Afin de pénaliser la fonction d'apprentissage d'un support de densité à classe unique, une fonction de perte est utilisée [6]. SAKM est développé comme un nouvel algorithme basé sur un noyau pour regrouper des données non stationnaires dans un contexte multi-classes [2]. Pour faire face aux difficultés de la mise en cluster non supervisée, le réseau SAKM utilise une architecture neurale de type feed-forward. Selon une nouvelle mesure de similarité induite par le noyau, les données sont regroupées dans des modèles de grappes décrits par leurs supports de densité dans le RKHS (Reproducing Kernel Hilbert Space). Les clusters en évolution sont mis à jour de manière itérative en incorporant de nouvelles informations via des règles de mise à jour SAKM. Les procédures d'apprentissage SAKM sont décrites en quatre étapes principales. La première étape consiste en une procédure de création permettant l'insertion de nouveaux clusters avec un mécanisme d'initialisation adéquat. La deuxième étape est une procédure d'adaptation basée sur la technique de la descente de gradient stochastique dans l'espace de Hilbert. Dans cette procédure, une règle de mise à jour rapide et efficace est définie pour incorporer de nouvelles informations aux clusters en évolution. La troisième étape est une procédure de fusion développée pour gérer des informations mutuelles entre des groupes similaires. Enfin, la quatrième étape est une procédure d'élimination utile pour éliminer les clusters non représentatifs et ensuite assurer la robustesse du clustering en ligne. Ainsi, lorsqu'une nouvelle donnée est présentée, le choix de la procédure d'apprentissage est résumé dans le tableau 1 en utilisant le critère suivant :

$$\Omega^{win} = \{C_m^t \in \Omega^t | \mu\phi(X_t, C_m^t) \leq \epsilon_{th}\}$$

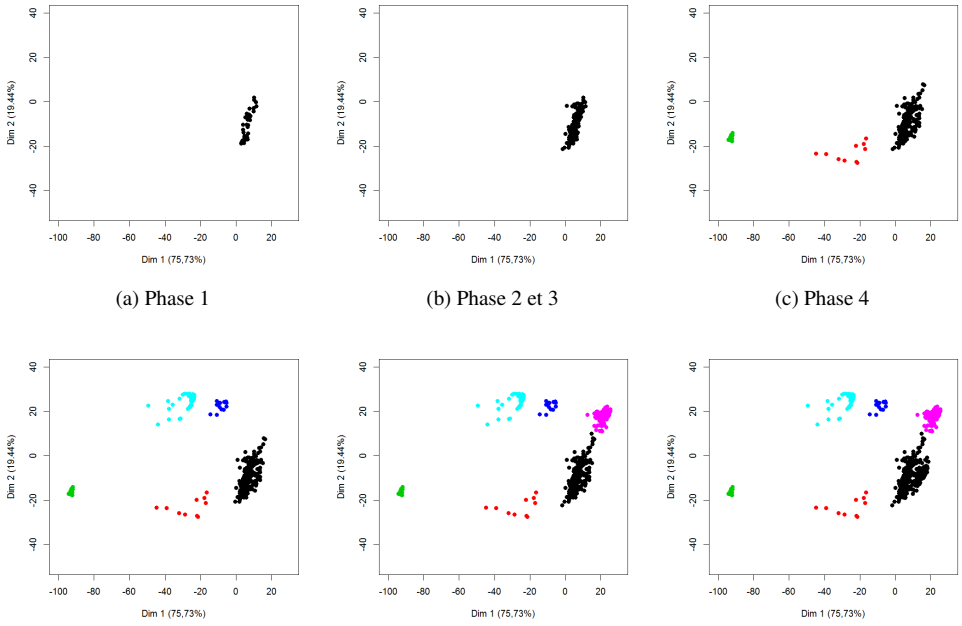
avec $\omega^t = C_1^t, \ldots, C_m^t, \ldots, C_M^t$ un ensemble de clusters à un instant t et $\mu\phi(X_t, C_m^t)$ la fonction de similarité induite par le noyau pour évaluer la distance d'une nouvelle donnée X_t avec chaque cluster C_m^t. Ce tableau donne pour chaque cas la procédure d'apprentissage appropriée. L'algorithme SAKM nécessite quatre paramètres et quatre seuils. Les quatre paramètres λ, η, ν and ϵ_{th} sont respectivement la largeur du noyau inverse (traduit la rigidité de l'hyperplan séparateur), le taux d'apprentissage (un faible taux d'apprentissage entraîne la stabilité, mais le système perd de l'adaptabilité alors qu'un taux d'apprentissage plus grand gagne en adaptabilité, mais perd en stabilité), la fraction des vecteurs de support de marge et le seuil d'acceptation. Le seuil τ détermine le nombre de termes qui seront tronqués lors de l'apprentissage, N_c est le nombre sous lequel un cluster est considéré comme incohérent et doit être supprimé et T est la période après laquelle un cluster de taille inférieure à N_c est supprimé.

TABLE 1 – SAKM : règle de décision et procédures.

cas 1	$card(\Omega^{win}) = 0$	Initialisation-creation
cas 2	$card(\Omega^{win}) = 1$	Adaptation
cas 3	$card(\Omega^{win}) \geq 2$	Fusion

4 Résultat et discussion

Nous proposons d'utiliser une architecture basée sur une approche de reconnaissance de modèle pour étudier le spectre d'une communication Wi-Fi devant faire face à différents scénarios d'attaque. Notre objectif est d'améliorer la détection des attaques en utilisant des modèles de mise à jour. L'algorithme SAKM est déployé sur les données décrites dans la section 2. La première étape, qui correspond au premier spectre de 39 décrivant une utilisation normale de la communication Wi-Fi, est utilisée pour initialiser notre algorithme. Dans cette étude, les différents modèles SVM à une classe de l'algorithme SAKM utilisent un noyau gaussien (RBF) [7] avec $\lambda = 0.326$ la largeur de fenêtre du noyau estimée par l'algorithme sigest [8]. Pour le taux d'apprentissage η de l'algorithme SAKM, la valeur a été estimée par validation croisée et fixée à 0.127. Le paramètre ν qui définit la fraction des vecteurs de support et des valeurs aberrantes qui se trouvent en dehors de la classe est fixé à 0.1 et ϵ_{th} qui est le seuil d'acceptation, prend la valeur 0.8. Pour le processus d'élimination nous posons $N_c = 5$ et $T = 20$. Ce processus correspond à la durée pendant laquelle un groupe peut contenir moins de N_c trames de communications. En utilisant les deux premières composantes principales de l'APC nous illustrons sur la figure 2 l'évolution des clusters après chacune des neuf phases. Il s'agit d'une technique SVM unique dédiée à la mise en cluster de données non stationnaires. Dans notre cas, il est important de distinguer les attaques de protocole, de l'attaque de brouillage. En ce sens, SAKM a créé 5 clusters. Le premier groupe couvre le début de l'attaque de désauthentification en violet, le second correspond à une reconnexion du client après une attaque de désauthentification en bleu clair, un correspondant à un brouillage qui perturbe la communication en vert et deux groupes représentés en rouge et en bleu sont ceux correspondant à une attaque par brouillage avec perte de communication. Le plus gros problème de cette classification est que le cluster contient des spectres décrivant uniquement une communication Wi-Fi, une communication Wi-Fi en présence d'absorbeur et une communication Wi-Fi en présence de brouillage (mais sans effet). A partir de ces résultats, nous n'avons pu que constater que le réseau SAKM a une bonne capacité d'apprentissage et permet de bien discriminer le comportement des ondes électromagnétiques acquises en chambre anéchoïque. Mais la difficulté de cette approche est de choisir le seuil pour lequel SAKM fusionnera deux clusters.



(a) Phase 1 (b) Phase 2 et 3 (c) Phase 4

(d) Phase 5 et 6 (e) Phase 7 et 8 (f) Phase 9

FIGURE 2 – Evolution de la classification

5 Conclusion

Ce document présente l'utilisation de SAKM (Self-Adaptive Kernel Machine) pour surveiller les communications Wi-Fi et détecter d'éventuelles attaques. Dans cette configuration, SAKM présente un avantage significatif : sa règle de mise à jour rapide et efficace permet un apprentissage évolutif, essentiel pour la surveillance du réseau wi-fi. L'algorithme prend en compte les variations dans le temps de nouveaux groupes en fournissant séquentiellement des modèles optimaux. Grâce à l'application, l'algorithme SAKM montre sa capacité à apprendre efficacement des groupes et à prendre en compte leurs évolutions dans un environnement non stationnaire. Son application à la sécurité du réseau Wi-Fi pour détecter les attaques montre de bonnes performances. Dans les travaux futurs, nous prévoyons de vérifier le comportement de notre modèle sur les données acquises en dehors de la chambre anéchoïque et de vérifier si notre approche est capable de discriminer plus d'attaques EM différentes.

Références

[1] J. Villain, V. Deniau, A. Fleury, E. Simon, C. Gransart, R. Kousri, *EM Monitoring and classification of IEMI and protocol-based attacks on IEEE* 802.11*n communication networks*, IEEE Transactions on Electromagnetic Compatibility, 2019.

[2] H.A. Boubacar, S. Lecoeuche, S. Maouche, *SAKM : Self-adaptive kernel machine a kernel-based algorithm for online clustering.* Neural Networks, 2008.

[3] V. Deniau, C. Gransart, G.L. Romero, E.P. Simon, J. Farah, J., *Ieee 802.11 n communications in the presence of frequency-sweeping interference signals.* IEEE Transactions on Electromagnetic Compatibility, 2017.

[4] V. Vapnik, *The nature of statistical learning theory*, Springer, 2000.

[5] B. Schölkopf, R.C. Williamson, A.J. Smola, J. Shawe-Taylor, J.C. Platt, *Support vector method for novelty detection*, In : Advances in neural information processing systems, 2000.

[6] J. Kivinen, A.J. Smola, R.C. Williamson, *Online learning with kernels*, IEEE transactions on signal processing, 2004.

[7] B. Schölkopf, A.J. Smola, *Learning with kernels : support vector machines, regularization, optimization, and beyond*, MIT press, 2002.

[8] B. Caputo, K. Sim, F. Furesjo, A. Smola, *Appearance-based object recognition using svms : which kernel should i use ?*, In : Proc of NIPS workshop on Statistical methods for computational experiments in visual processing and computer vision, 2002.