Détection d'attaques par signal de brouillage et identification de son éloignement

Jonathan Villain, Virginie Deniau, Christophe Gransart, Eric Pierre Simon, Anthony Fleury

20ème Colloque International et Exposition sur la Compatibilité ÉlectroMagnétique (CEM 2020)

Détection d'attaques par signal de brouillage et identification de son éloignement

J. Villain[1], V. Deniau[1], C. Gransart[1], E.P. Simon[2], A. Fleury[3]
[1]COSYS-LEOST, Univ Gustave Eiffel, IFSTTAR, Univ. Lille, F-59650 Villeneuve d'Ascq, France
jonathan. villain@univ-eiffel.fr, virginie.deniau@univ-eiffel.fr,christophe.gransart@univ-eiffel.fr
[2]IEMN, TELICE, University of Lille, eric.simon@univ-lille.fr
[3]IMT Lille Douai, Univ. Lille, anthony.fleury@imt-lille-douai.fr

Résumé Les réseaux sans fil Wi-Fi sont aujourd'hui dans tous les espaces, aussi bien publics que privés. Ils sont souvent utilisés pour accéder à des services ou assurer des fonctions opérationnelles à distance. Cependant, ces réseaux Wi-Fi peuvent être vulnérables et utilisés par des personnes malintentionnées pour perturber les services. Des stratégies de défense doivent être développées pour éviter les abus sur ces réseaux et intercepter les personnes malveillantes. Dans ce contexte, le projet GLOCAT vise à rechercher des moyens de détecter et géo-localiser des sources d'attaque envers ces réseaux de communication sans fil. L'approche repose sur l'analyse continue des signaux électromagnétiques (EM) reçus par une antenne de surveillance et un récepteur collectant les distributions spectrales. Les premiers travaux présentés dans cet article visent à développer un protocole de classification pour distinguer si une source de brouillage intentionnel se situe dans le même espace intérieur que le réseau de communication ou à l'extérieur de l'infrastructure dans laquelle est établie la communication.

I. Introduction

Les communications par ondes radiofréquence sont de plus en plus utilisées pour la flexibilité de connexion qu'elles apportent. Cependant, elles ont intrinsèquement la capacité de s'étendre dans toutes les directions. Une des conséquences de cette "propagation sauvage" des ondes radiofréquence est la facilité avec laquelle une personne malveillante peut brouiller un réseau, même en étant en dehors de l'espace où le réseau sans fil est censé être déployé. Les conséquences associées à un éventuel brouillage sont diverses. Mais dans certains domaines, le brouillage peut permettre de rendre inopérant de nombreuses fonctions parfois liées à la sécurité. Dans [1] et [2] nous nous sommes concentrés sur la conception d'un système de surveillance capable de détecter et classer les attaques par brouillage et par de authentification forcée. Pour atteindre cet objectif, nous avons proposé d'externaliser la surveillance en utilisant une antenne pour la surveillance située dans la pièce du point d'accès pour obtenir les distributions spectrales au cours du temps. Ces travaux ont montré la difficulté de détecter des attaques par signal de brouillage de très faible puissance. Dans [3], nous avons classé et caractérisé ces dernières. En complément de ces travaux de détection, il est également important de localiser la provenance du signal de brouillage. Ainsi, le projet GLOCAT vise à mettre en place un système de surveillance capable de géo localiser une source d'attaque envers un réseau sans fils. Les travaux présentés dans cette communication sont une première étape vers cette géo localisation et visent à déterminer la proximité de la source de brouillage et d'identifier si celle-ci se situe à l'intérieur ou en dehors de l'emplacement où le réseau sans fil est déployé.

La section 2 décrit la configuration d'expérimentation adoptée pour mettre en oeuvre les attaques ElectroMagnétiques (EM). La section 3 porte sur l'analyse des caractéristiques des spectres collectés au cours des expérimentations. La section 4 présente l'approche d'identification du positionnement de la source de brouillage. Enfin, dans la section 5, les résultats sont analysés avant de conclure.

II. Expérimentation

L'expérimentation est réalisée dans un des laboratoires de l'université Gustave Eiffel, au sein duquel un point d'accès Wi-Fi a été spécifiquement installé pour l'étude. Le protocole de communication considéré est la norme IEEE 802.11n, qui utilise la modulation OFDM.

Nous avons placé une antenne de surveillance raccordée à un analyseur temps réel à proximité du client, lui-même dans la même pièce. Pour émettre le signal de brouillage, une autre antenne connectée à un générateur de forme d'onde arbitraire a été utilisée. Nous considérons deux configurations d'attaques : l'attaque par brouillage située en trajet direct d'accés (que l'on notera LoS), c'est à dire qu'aucun obstacle n'est présent sur la trajectoire du signal de brouillage, et l'attaque par brouillage indirect (que l'on notera OS) qui correspond à une configuration où un mur est présent entre l'antenne d'émission du signal de brouillage et la pièce où s'effectue la communication (voir la Figure 1). Pour ces 2 configurations, l'antenne qui émet le signal de brouillage est située à différentes distances du client afin de faire varier la puissance du signal de brouillage. L'analyseur de spectre est configuré avec une plage de fréquences de 40 MHz, une fréquence centrale de $2,422$ GHz, une largeur de bande de résolution de 100kHz. Le temps de balayage de l'analyseur de spectre était de $38,2$ μs.

L'attaque par brouillage consiste à émettre un signal qui

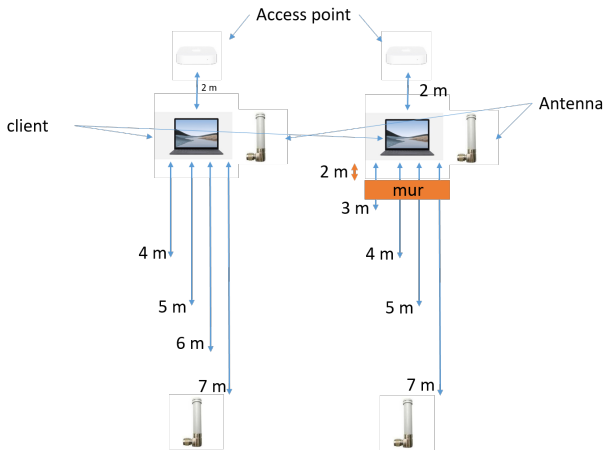

FIGURE *1*. *Configuration de l'environnement d'expérimentation.*

couvre les bandes de fréquence utilisées par le système de communication (voir Figure 2). Différents types de signaux de brouillage peuvent être utilisés [4] mais la majorité des brouilleurs produisent un signal qui balaie une bande de fréquence $[f_1, f_2]$ sur une période de temps T et pouvant être donnée par

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

avec A l'amplitude du signal d'interférence. Le signal de brouillage que nous considérons balaie les fréquences situées entre $[2,4; 2,5]$ GHz en 10 μs.

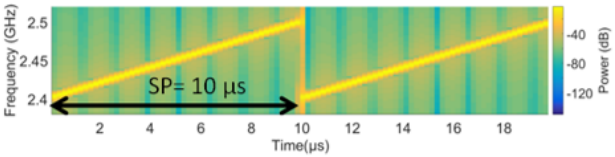

FIGURE *2*. *Configuration de l'environnement d'expérimentation.*

III. Analyse des Spectres

Les spectres (voir Figure 3) sont collectés par un analyseur de spectre connecté à l'antenne de surveillance proche du client. Les mesures ont été réalisées sur 1601 points de fréquence dans une bande de 40 MHz centrée sur la fréquence centrale du canal de communication utilisé par le point d'accès et le client.

La puissance mesurée sur ces fréquences varie entre -114dBm et -49dBm. Comme le montre la Figure 4, les puissances mesurées se concentrent majoritairement autour de 2 niveaux de puissance, -68dBm et -109dBm, qui correspondent aux fréquences présentes dans la bande centrale de $20MHz$ du canal de communication et les 2 bandes de fréquence de 10MHz situées aux alentours du

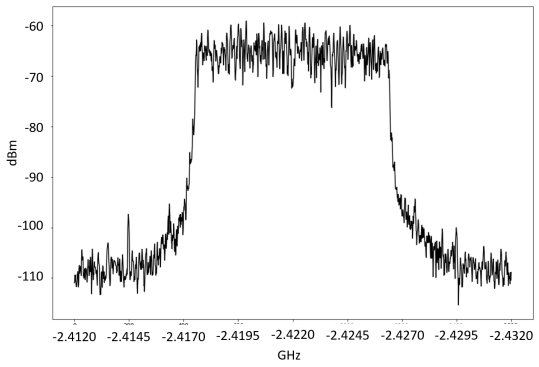

FIGURE *3*. *Spectre d'une communication Wi-Fi standard.*

canal de communication. Ces valeurs ainsi que leur taux d'observation varient légèrement selon la configuration de la communication et nous souhaitons exploiter ces variations pour identifier la provenance du signal. Ayant

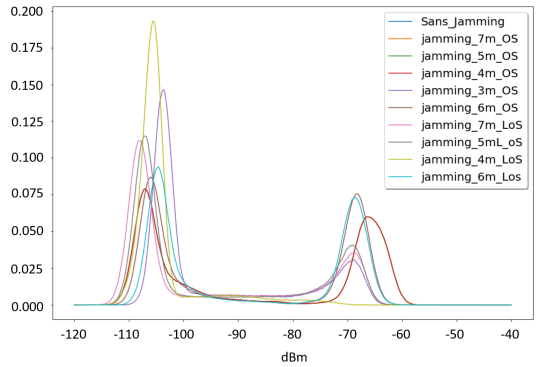

FIGURE *4*. *Densité de répartition de la puissance par configuration.*

mis en évidence les différences entre les configurations présentées, nous allons chercher à distinguer trois types de configuration. La première est une communication sans perturbation volontaire, la seconde configuration est une communication perturbée par un signal de brouillage en OS et la dernière configuration, une communication en présence d'un signal de brouillage en LoS.

IV. Détection

Dans ces travaux, nous comparons deux algorithmes de classification par apprentissage sur leur capacité à détecter la présence d'un signal de brouillage et déterminer si la source de ce dernier est localisée à l'intérieur ou à l'extérieur de la salle où est située la communication. Les algorithmes comparés ici sont les approches de Séparateur à Vaste Marge et les approches par forêt aléatoire.

IV.1. Séparateur à Vaste Marge (SVM)

SVM (voir Figure 5) est une classe d'algorithmes d'apprentissage définis à l'origine pour la discrimination, c'est-à-dire la prédiction d'une variable qualitative binaire. Dans le cas de la discrimination (Support Vector classification ou SVc) d'une variable dichotomique, l'algorithme repose sur la recherche de l'hyperplan optimal, qui, lorsque cela est possible, classe ou sépare les données correctement en étant le plus loin possible de toutes les observations. Le principe est donc de trouver un classificateur, ou une fonction de discrimination, dont la capacité de généralisation est la plus grande possible.

Le principe de base de SVM consiste à réduire le problème de la discrimination à celui, linéaire, de la recherche d'un hyperplan optimal. Pour cela, Vapnik et Chervonenkis [5] ont mis en place un algorithme permettant de mettre en place un hyperplan séparateur dans un espace transformé en un espace de plus grande dimension. Dans cet algorithme, une première étape consiste à définir l'hyperplan comme une solution à un problème d'optimisation sous contraintes dont la fonction objective n'est exprimée qu'à l'aide de produits scalaires entre vecteurs et dans laquelle le nombre de contraintes " actives " ou vecteurs supports contrôle la complexité du modèle. Le passage à la recherche de surfaces de séparation non linéaires est obtenu par l'introduction d'une fonction noyau dans le produit scalaire induisant implicitement une transformation non linéaire des données vers un espace de caractéristiques de plus grande dimension.

Cet outil est utilisé dans de nombreux types d'applications et s'avère être un concurrent sérieux des algorithmes les plus efficaces. L'introduction de cœurs, spécifiquement adaptés à un problème donné, lui donne une grande souplesse pour s'adapter à des situations très diverses comme la reconnaissance de formes.

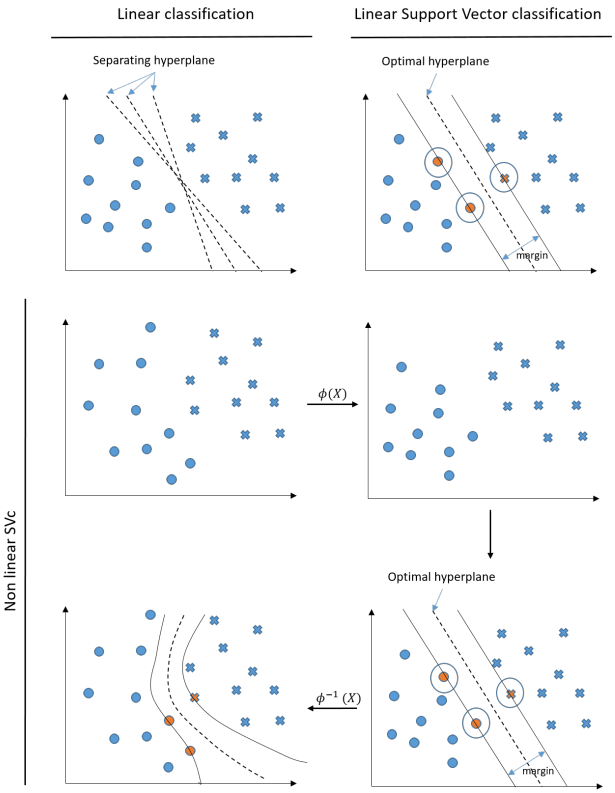

FIGURE 5. *Algorithme SVM.*

IV.2. Algorithme Forêt aléatoire (Random Forest (RF))

Les algorithmes RF [6] (voir Figure 6) sont basés sur des stratégies adaptatives ou aléatoires permettant d'améliorer l'ajustement en combinant ou en agrégeant un grand nombre de modèles tout en évitant ou en contrôlant le sur-ajustement. Ces algorithmes sont basés sur une construction aléatoire (Bagging : agrégation bootstrap) [7] et boosting [8]. Le concept de Bagging trouve son application dans le domaine de l'exploration de données prédictives, pour combiner des classifications prédites à partir de plusieurs modèles, ou à partir d'un même type de modèle pour différentes données d'apprentissage. Dans le cas spécifique des modèles d'arbres de décision binaires, Breiman [6] propose une amélioration du Bagging en ajoutant une composante aléatoire. L'objet se manifeste pour rendre les aggrégations d'arbres plus indépendantes en ajoutant de l'aléatoire dans le choix des variables qui interviennent dans les modèles. Le principe est élémentaire, la moyenne des prévisions de plusieurs modèles indépendants permet de réduire la variance et donc de réduire l'erreur de prévision. Dans de nombreux articles d'apprentissage automatique, la forêt aléatoire est devenue la méthode à battre pour prévoir la qualité sur de petits ensembles de données. Cependant, cela peut également conduire à de mauvais résultats, en particulier lorsque le problème sous-jacent est linéaire.

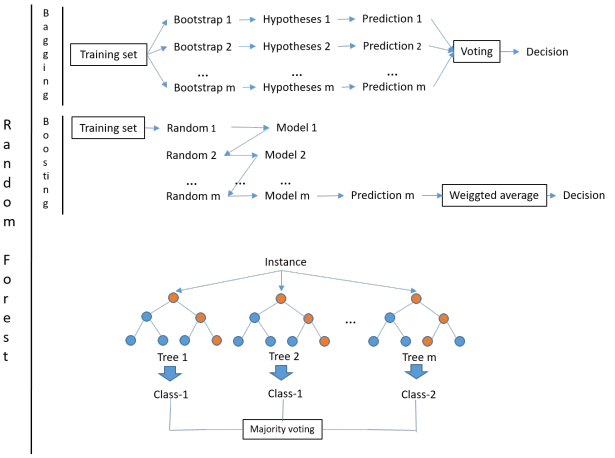

FIGURE 6. *Algorithme RF.*

V. Résultats et discussion

La classification est effectuée sur les 40MHz de la bande de fréquence. Nous voulons identifier si le réseau de communication est confronté ou non à une attaque et identifier si sa source est localisée dans la salle où se situent le point d'accès et le client ou en dehors de cette dernière. Nous devons identifier les 3 configurations présentées dans la section II. Nous estimons le profil d'attaque en utilisant les algorithmes présentés sur les figures 5 et 6. Pour vérifier la qualité des modèles, les spectres sont répartis en 2 sets de données, un set d'apprentissage (80%) et un set de test (20%) obtenus par tirage aléatoire sans remise. La phase d'apprentissage est la phase où le modèle apprend les caractéristiques de la séparation sur le set d'apprentissage. La phase de test est la phase où l'on vérifie la qualité du modèle. Dans cette phase, on calcule l'erreur de prédiction du modèle sur le set de test. La Table 1. représente la répartition des différentes configurations dans les trois classes sans brouillage, OS et LoS que l'on souhaite prédire.

TABLE *1. Matrice de confusion*

	Conf\Classes	sans brouillage	OS	LoS
	sans brouillage	357	144	0
	7m OS	15	486	0
	5m OS	20	476	0
S	4m OS	0	490	0
V	3m OS	0	251	2
c	7m LoS	0	91	151
	6m LoS	0	321	703
	5m LoS	0	55	189
	4m LoS	0	21	223
	sans brouillage	332	169	0
	7m OS	30	470	1
	5m OS	37	457	2
R	4m OS	11	470	9
F	3m OS	2	243	8
	7m LoS	2	107	137
	6m LoS	86	278	660
	5m LoS	1	49	194
	4m LoS	0	38	206

Les deux approches de classification par apprentissage apportent des résultats différents. En effet, sur le set de test le score pour l'erreur de classification obtenu par l'algorithme SVc est de 16,7% alors que l'algorithme de classification RF obtient un score de 22%. Sur ce type de données, il semble donc plus judicieux d'utiliser une approche SVc pour identifier les 3 configurations sans brouillage, avec signal de brouillage émis en OS et avec signal de brouillage émis en LoS. Pour ces deux approches de classification, les erreurs les plus fréquentes correspondent à des spectres de la configuration sans brouillage classés en OS, des spectres de la configuration OS classés sans brouillage et des spectres de la configuration LoS classés en OS. Nous constatons également que plus l'antenne de brouillage est proche de l'antenne de surveillance plus l'erreur de classification est faible. On peut donc en déduire que ces erreurs sont dues à une perception du signal de brouillage trop faible.

Plusieurs pistes sont envisagées pour la suite de ces travaux. Tout d'abord étudier la distance pour laquelle il est possible de mesurer avec une antenne de surveillance le signal de brouillage afin d'améliorer les résultats des algorithmes de classification en associant à ces derniers des matrices de coût plus adéquates. Dans ces travaux nous avons étudié des configurations pour lesquelles les signaux de brouillage provenaient tous de la même direction, il sera donc important d'étudier d'autres configurations pour élargir le cas d'étude. Dans de futurs travaux, afin d'améliorer ces résultats et de pouvoir localiser les attaquants, nous étudierons l'utilisation d'un système de surveillance multi-antennes.

VI. Remerciement

Le projet GLOCAT est partiellement financé par la région Hauts-de-France.

Références

[1] J. Villain, V. Deniau, A. Fleury, E. P. 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] J. Villain, A. Fleury, V. Deniau, C. Gransart, E. Simon, *Online EM Monitoring of 802.11 n Networks using Self Adaptive Kernel Machine*, 18th IEEE International Conference On Machine Learning And Applications (ICMLA), pp. 1136-1142, IEEE, 2019.

[3] J. Villain, V. Deniau, C. Gransart, A. Fleury and E. Simon *Characterization of IEEE 802.11 Communications and Detection of Low-Power Jamming Attacks in Noncontrolled Environment Based on a Clustering Study*, IEEE Systems Journal, 2021.

[4] V. Deniau, C. Gransart, G. L. Romero, E. P. Simon, and J. Farah, *IEEE 802.11n Communications in the Presence of Frequency-Sweeping Interference Signals*, IEEE Transactions on Electromagnetic Compatibility, vol. 59(5), pp. 1625–1633, 2017.

[5] V. Vapnik, *The nature of statistical learning theory*, Red Bank : Springer, 2, 2000.

[6] L. Breiman,*Statistical modeling : The two cultures*, Statistical science, 16(3), 199-231, 2001.

[7] L. Breiman, *Bagging predictors*, Machine learning, 24(2), 123-140, 1996.

[8] R. E. Schapire, Y. Freund, P. Bartlett and W. S. Lee,*Boosting the margin : A new explanation for the effectiveness of voting methods*, Annals of statistics, 26(5), 1651-1686, 1998.