Détection de cyber attaques sur réseau Wi-Fi par classification de données spectrales

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

Détection de cyber attaques sur réseau Wi-Fi par classification de données spectrales

Virginie Deniau[(1)], Jonathan Villain[(2)], Eric Simon[(3)], Anthony Fleury[(2)], Christophe Gransart[(1)]

(1) IFSTTAR-COSYS, Villeneuve d'Ascq, France, (2) IMT Lille Douai, France, (3) Groupe IEMN-TELICE, Université de Lille, France

Résumé :

Dans de nombreux domaines, les réseaux de communication ou informatiques comportent à la fois des sections filaires et sans fil. Ici, on s'intéresse à la partie sans fil qui peut être victime d'attaques ciblées, visant du déni de service en empêchant la bonne réception des signaux de communication ou bien des attaques « man-in-the-loop » visant à intercepter des informations. Dans cette communication, nous présentons des travaux qui se basent sur l'analyse de l'activité électromagnétique pour détecter de telles attaques sur un réseau Wi-Fi IEEE 802.11n. L'approche repose sur l'analyse de données spectrales par technique de classification.

Introduction :

Les réseaux de communication Wi-Fi sont aujourd'hui largement déployés dans les espaces publiques, personnels ou professionnelles. Ainsi, pour les hackers, ils représentent des moyens d'accès à certaines informations qui permettront ensuite d'organiser des attaques plus ciblées ou avec une meilleure réussite. Dans certains secteurs professionnels, les réseaux Wi-Fi sont également employés pour des applications opérationnelles, souvent liés à de la maintenance et de simples attaques par déni de service peuvent engendrer des conséquences immédiates. Ainsi, l'objectif de nos travaux est de détecter ces attaques au moment où elles s'exécutent.

Les scénarios d'attaque étudiés correspondent à des attaquants qui utiliseraient des brouilleurs pour provoquer un déni de service ou qui émettraient des trames de dé authentification pour déconnecter un client d'un point d'accès licite. L'attaquant peut chercher à bénéficier de l'ensemble de la ressource Wi-Fi ou, chercher à connecter le poste client à un point d'accès illicite et ainsi intercepter ses données privées. L'attaque par trames de dé authentification est une attaque protocolaire. Dans ce travail, nous souhaitons développer une approche capable de détecter et de distinguer les attaques par brouillage et les attaques protocolaires.

Mises en œuvre des attaques par brouillage et par trames de dé authentification

L'attaque par brouillage consiste à émettre intentionnellement un signal qui couvre les fréquences utilisées par le système de communication afin de dégrader la qualité du signal reçu par un dispositif de communication. Les signaux de brouillage sont des interférences électromagnétiques intentionnelles (IEMI) relativement peu puissantes qui dégradent les performances des réseaux de communication sans les endommager. Différents types de signaux de brouillage peuvent être utilisés [1]. La majorité des brouilleurs commerciaux génère un signal qui balaye de manière répétée une bande de fréquence [f_1, f_2] dans une durée T. Ce type de signaux peut être exprimé par:

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

où *A* est l'amplitude du signal d'interférence. Dans notre étude, le signal de brouillage balaie la bande de fréquences 2,4 GHz à 2,5 GHz dans un intervalle de temps $T = 10\ \mu s$.

L'attaque par trames de dé authentification utilise des trames définis dans la norme IEEE 802.11. Dans un réseau composé de plusieurs points d'accès(AP), lorsqu'un poste client se déplace il peut se trouver déconnecté d'un AP et reconnecté à un autre. Si le client est connecté à un AP et s'en éloigne, la puissance du signal Wi-Fi reçu diminue et il peut également détecter le signal de balise Wi-Fi d'un autre AP avec une puissance croissante. Dans ce cas, une procédure d'itinérance est lancée. Elle consiste à déconnecter le client du premier AP et à le reconnecter au second AP à l'aide des trames d'authentification et de dé authentification IEEE 802.11. L'attaque par dé authentification envoie à un poste client une trame de dé authentification même si celui-ci ne se déplace pas.

Pour nos travaux, ces attaques ont été mises en œuvre en chambre anéchoïque pour ne pas perturber les réseaux environnants. Un canal Wi-Fi de 20 MHz centré à la fréquence 2.412 GHz a été utilisé. Des acquisitions spectrales de 20 MHz de largeur centrées à la fréquence 2.412 GHz, ont été effectuées au cours des attaques. Les attaques par brouillage ont été mises en œuvre avec trois niveau de puissance : une puissance faible rendant le signal de brouillage totalement inefficace, une puissance intermédiaire créant une légère baisse de débit et une puissance mettant le système Wi-Fi en limite d''interruption.

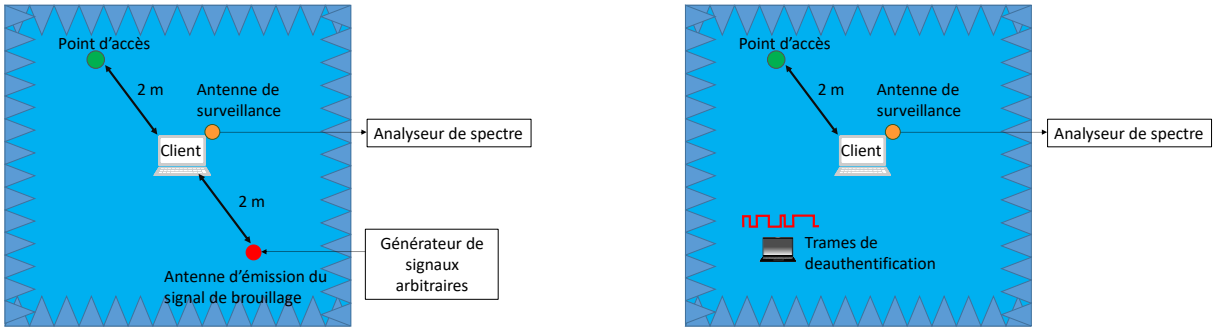

Figure 1 : Expérimentations d'attaques par brouillage (à gauche) et par dé authentification (à droite)

L'analyse en composantes principales sur les données des spectres

La classification des données est réalisée en déterminant préalablement les relations qui lient des variables explicatives, c'est-à-dire des grandeurs observées (Ici les spectres collectés pendant les attaques) à un critère que l'on cherche à classer (le type d'attaque). Une étape préalable est d'étudier les profils que l'on souhaite identifier. Dans cette étude nous voulons identifier 6 profils: une communication Wi-Fi sans attaque, une dégradation des performances en plaçant des matériaux absorbants autour de l'AP, 3 différentes puissances de brouillage et une attaque par dé authentification [2].

Une analyse en composantes principales (ACP) sur les données des spectres (ici 99 spectres par profil) met en avant la différence entre ces profils afin de vérifier si les différentes classes peuvent être séparées [3]. A l'issue de l'ACP, les spectres sont projetés dans un nouvel espace à partir des composantes associées aux vecteurs propre. Le plan vectoriel, représenté figure 2, associé aux 2 vecteurs propre possédant les valeurs propres les plus élevées, représente 95,17% de la variabilité des spectres.

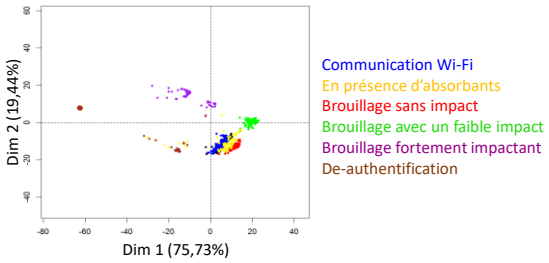

Figure 2 : Représentation des spectres en fonction des deux premières composantes de l'ACP

On observe sur ce plan (Figure 2) que l'attaque par dé authentification est pour partie bien séparée des autres classes. Ce résultat est intéressant car la nature du signal d'attaque par dé authentification n'est pas différente d'une communication normale. Néanmoins, une partie des spectres se positionnent dans un espace bien séparé de celui de la communication Wi-Fi seule. Nous observons également une bonne séparation des situations de brouillage fort et modéré. Ce résultat est encourageant pour développer une approche de détection capable de distinguer différents types d'attaques. Au cours de la présentation ces différents résultats seront analysés en détail.

[1] 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 EMC, vol. 59, no. 5, pp. 1625-1633, 2017.
[2] 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 802.11n Communication Networks, IEEE Transactions on Electromagnetic Compatibility, 2019 , Early Access.
[3] S. Wold, K. Esbensen, and P. Geladi, Principal component analysis, Chemometrics and intelligent laboratory systems, vol. 2, no. 1-3, pp.3752, 1987.