URSI GASS 2020, Rome, Italy, 29 August - 5 September 2020

Detection of cyber-attacks on Wi-Fi networks by classification of spectral data

Jonathan Villain[(1)], Virginie Deniau [(1)], Anthony Fleury[(2)], Christophe Gransart[(1)] and Eric Pierre Simon[(3)]
(1) COSYS-LEOST, Université Gustave Eiffel, campus Lille, France
(2) IMT Lille Douai, Univ. Lille, Unité de Recherche Informatique et Automatique (URIA),
F-59000 Lille, France
(3) IEMN lab, TELICE group, University of Lille, F-59000 Lille, France.

Abstract

In many areas, communications or computer networks include both wired and wireless sections. In this research, we are interested in the wireless network sections.

This part of the networks can targeted by denial of service attacks, affecting the reception quality of communication signals, or by "man-in-the-loop" attacks aiming to intercept information. This paper presents a work based on the analysis of wireless electromagnetic activity to detect such attacks against an IEEE 802.11n Wi-Fi network.

The approach is based on the analysis of spectral occupation by classification technics. Experimentations were performed in anechoic chamber in applying jamming attacks and de authentication attacks. In a first step, in performing the Principal component analysis of the spectra measured for the different tested situations, we analyse if the different classes can be separated. In a second step, we assess the ability of a Self Adaptative Kernel Machine to classify the different attacks without a preliminary learning phase of the attack situations.

1 Introduction

Wi-Fi communication networks are widely deployed in public, personal and professional spaces. Thus, for hackers, they represent means of access to certain information, which can allow implementing more targeted or more successful attacks. In certain professional sectors, Wi-Fi networks are also used for operational applications, often linked to maintenance activities, and simple denial of service attacks can involve immediate consequences. Thus, the objective of our work is to detect these attacks when they are executed.

The attack scenarios studied correspond to attackers who would activate communication jammers to cause a denial of service or who would emit de authentication frames to disconnect a client from a licit access point. Attacks by de authentication frames are generally used by hackers in order to benefit from the entire Wi-Fi resource over a shared network or, to connect the client workstation to an illicit access point and thus intercept his private data. The de-authentication frame attack is a based-protocol attack. In this work, we aim to develop an approach capable of detecting and distinguishing between jamming attacks and based-protocol attacks.

2 Implementation of jamming and de-authentication frame attacks

Jamming attack consists in intentionally transmitting a disturbing signal that covers the frequencies used by the communication system in order to degrade the quality of the signal received by a communication device. Jamming signals are intentional electromagnetic interferences (IEMI) that degrade the performance of communication networks without damaging them. Different types of interference signals can be used [1]. The majority of commercial jammers generates a signal which repeatedly scans a frequency band [*f1*, *f2*] in a duration *T*. This type of jamming signal can be expressed by:

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

where A is the amplitude of the interference signal. In our study, the interference signal scans the 2.4 GHz to 2.5 GHz frequency band in a *T* = 10 µs time duration.

The de authentication frame attack uses frames defined in the IEEE 802.11 standard. In a network composed of several access points (AP), de authentication frames are used in order to disconnected a client station from one AP and reconnected it to another. If the client is connected to an AP and moves away from this AP, the strength of the received Wi-Fi signal decreases and it can also detect the Wi-Fi beacon signal of another AP with an increasing power. In this case, a roaming procedure is launched. It consists of disconnecting the client from the first AP and reconnecting it to the second AP using IEEE 802.11 authentication and de-authentication frames. The de-authentication attack sends to a client station a de-authentication frame even if it does not move.

For our work, these attacks were implemented in an anechoic chamber so as not to disturb the surrounding networks. A 20 MHz Wi-Fi channel centered at the 2.412 GHz frequency was used. Spectral acquisitions of 40 MHz in width centered at the frequency 2.412 GHz, were carried out during the attacks. Jamming attacks have been implemented with three power levels: low power making the jamming signal ineffective, intermediate power creating a slight impact on the bit rate of the Wi-Fi communication and jamming power putting the Wi-Fi system at the limit of communication interruption.

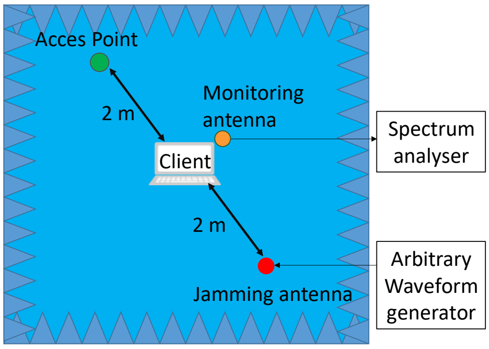

Figure 1. Configuration of the Jamming attack experiments.

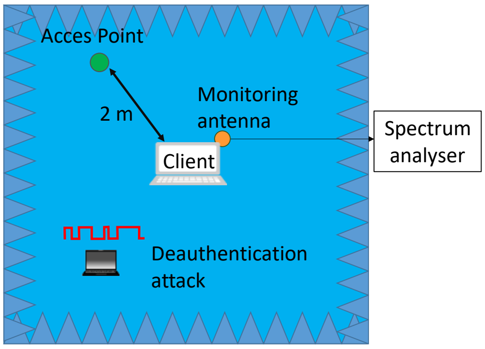

Figure 2. Configuration of the De authentication attack experiments.

3 Principal component analysis on spectral data

The classification of the data is carried out by determining beforehand the relations which link explanatory variables, i.e. observed quantities (Here the spectra collected during the attacks) with a criterion to classify according to the kind of attack. A preliminary step is to define the profiles to identify. In this study, we want to identify 6 profiles: Wi-Fi communication without attack, performance degradation by placing absorbant materials around the AP, 3 different jamming power levels and attack by de authentication frames [2].

A principal component analysis (PCA) on the spectral data (here 99 spectra per profile) highlights the difference between these profiles in order to check if the different classes can be separated [3]. At the end of the PCA, the spectra are projected into a two dimensions space based on the components associated with the eigenvectors. The vectorial plane, represented in Fig. 3, associated with the 2 eigenvectors having the highest eigenvalues, represents 95.17% of the variability of the spectra.

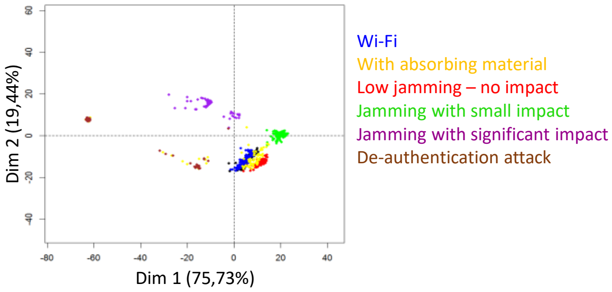

Figure 3. Representation of the spectra according to the first two components of the PCA.

Through this representation Fig. 3, we notice that the attack by deauthentication is clearly separated from the other classes. This result is interesting because the nature of the deauthentication signal is not different from normal communication signal due to it is a part of the protocol. We also observe a good separation of strong and moderate jamming situations while low power jamming and absorbing material situations are adjacent to the Wi-Fi without attack situation. This result is encouraging to develop a detection approach capable of distinguishing different types of attacks.

In this test configuration, we perfectly master the situations. In practice and in public environment, different situations, not previously learned, can occur. As new (unpresented/unlearned) attacks can appear very quickly, we decided to use machine learning techniques which allow to identify new classes without preliminary learning phase of these classes.

4 Self Adaptative Kernel Machine (SAKM)

This technic includes adaptive classification algorithms, able to change the models after their creation as well as the number of classes over time. By learning the standard behavior of the Wi-Fi communication, which is the Wi-Fi without any attack, the algorithm analyzes the successive data and try to classify them as standard communication or not. If the communication is not standard, a new class is created and considered as an unknown attack.

SAKM is a new kernel-based algorithm for grouping non-stationary data in a multi-class context [4]. By measures of similarity associated to the kernel, the data are grouped in cluster models. Evolving clusters are updated iteratively by incorporating new information via SAKM update rules. SAKM rules can involve creation, adaptation or fusion of clusters.

We tested this approach over the previous spectral data presented in section 3 but in considering only the 20 MHz frequency band centered over the Wi-Fi channel.

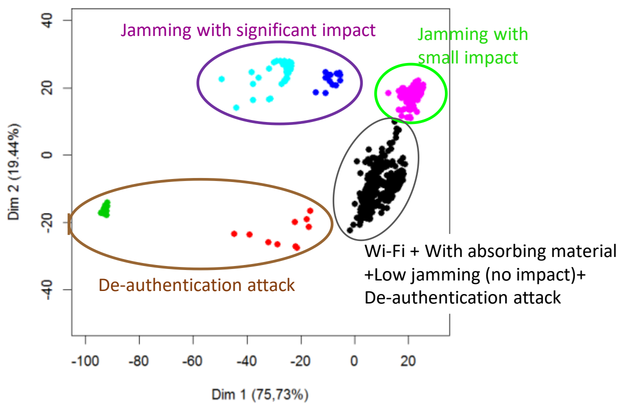

Figure 4. Representation of the spectra according to the first two components of the PCA and identification of the classes with SAKM

The results are presented Fig. 4. Each color corresponds to one class identified by the SAKM algorithm. Therefore, we notice that the jamming with significant impact appears as two different classes and jamming which small impact is well grouped into a single class. The fact that the jamming with significant impact is identified as two different classes can be explained by the fact that there is short communication interruptions which impact the spectrum pattern.

We also observe that Wi-Fi alone, with absorbing material and jamming without impact are considered as a single classe (black color). This class also includes certain spectra obtained with the de authentication attack.

The deauthentication attack spectra are then distributed into three classes (green, red and black in Fig. 4). That illustrates the attack process that regularly disconnects the client to reconnect it. Then, the presence of the three classes appearing alternatively can be a means to detect the presence of such attacks.

5 Conclusions

In this work, we have showed that jamming attacks and de authentication attacks can be detected and identified by classification technics based on preliminary learning phases. Knowing that certain attacks can be unlearned previously, we also tested an adaptative classification algorithm able to form different classes without preliminary learning of the attacks.

Both approaches give satisfying results but we have to keep in mind that the measurements were performed in anechoic chamber. In realistic environment, the situations are significantly more variable. We can have jamming situations coming from the use of jammers but also coming from the smart phone used as AP without attack intentions. To deal with these difficulties, we have to analyze the spectra parameters which allows us to separate them into different classes and then analyze the miss classifications.

6 Acknowledgements

This work was performed in the framework the ELSAT2020 project which is co-financed by the European Union with the European Regional Development Fund, the French state and the Hauts de France Region Council.

7 References

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.

4. H.A. Boubacar, S. Lecoeuche, S. Maouche, Sakm : Self adaptive kernel machine a kernel-based algorithm for online clustering. Neural Networks, 2008.