Clustering Study in order to Analyse Wi-fi Communications Affected by Low Power Jamming Attacks

J. Villain[(1)], V. Deniau[(1)], C. Gransart[(1)], A. Fleury[(2)] and E. Simon[(3)]
(1) COSYS-LEOST, Univ Gustave Eiffel, IFSTTAR, Univ Lille, F-59650 Villeneuve d'Ascq, France, https://leost.univ-gustave-eiffel.fr
(2) IMT, Douai, France, https://imt-lille-douai.fr/
(3) IEMN, Université de Lille, Villeneuve d'ascq, France, http://fedmecalille.univ-lille.fr/unites/institut-delectronique-de-microelectronique-et-de-nanotechnologie-iemn-umr-8520

Wireless connections are more and more used for numerous applications in public areas for general public services but also for handling sensitive communications. The wireless communication networks can have to face different kind of attacks that target the behind services. Although the use of communication jammers is prohibited, they are generally employed for malicious actions. Our work aims to detect, as soon as possible and online, attacks that can occur on wireless networks, to be able to react very quickly. In this presentation, we present some results published in [1] of data analysis methods, on Wi-Fi signals, to differentiate the ones with attacks from the ones without. This study focuses on low power jamming attacks with a slight or even no impact on Wi-Fi communications and acquired in uncontrolled conditions (figure 1). This is more challenging than detecting high power jamming attacks which have already been addressed in the literature. Being able to detect a low impact attack is a crucial issue in a global security strategy, making it possible to launch countermeasures before the interruption of the communication.

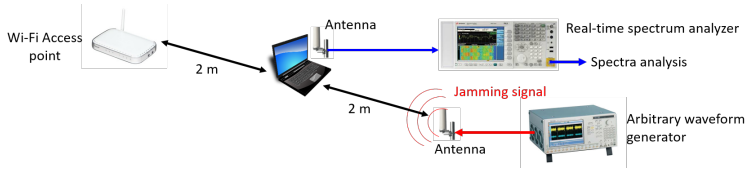

Figure 1. Experimentation with a 802.11n communication in the presence of jamming attack.

The Wi-Fi bands are also in the ISM frequencies, making the environment complicated to analyze. Clustering methods such as Agglomerative Hierarchical Clustering are used to identify some clusters and then to map them to the real classes (with or without attacks). A deep analysis of the clusters obtained (see Table 1) is carried out. This is done in order to understand what is responsible of the clustering assignment of the different points and to extract the clusters which can be used to design a detection attack strategy.

cluster	Wi-Fi only	Wi-Fi + low jamming
1	27 / 23%	91 / 77%
2	0 / 0%	122 / 100%
3	50 / 27%	125 / 73%
4	123 / 25%	366 / 75%
5	1019 / 31%	2259 / 69%
6	8304 / 90%	962 / 10%
7	65 / 2%	3983 / 98%
8	1410 / 6%	22088 / 94%
Sum	10998 / 27%	29996 / 73%

Table 1. Cluster distribution

References

[1] 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 non controlled environment based on a clustering study," *IEEE Systems Journal*, January 2021, doi:10.1109/JSYST.2020.3045365.