A Threshold-Based Detection Approach To Detect Fake Access Points and Jamming Attacks on IEEE 802.11 Networks: Implementation, Results and Limitations

Andy Amoordon, Virginie Deniau, Christophe Gransart, Anthony Fleury, Jonathan Villain

3rd URSI AT-AP-RASC, Gran Canaria, 29 May – 3 June 2022

A Threshold-Based Detection Approach To Detect Fake Access Points and Jamming Attacks on IEEE 802.11 Networks: Implementation, Results and Limitations

Andy Amoordon [(1)], Virginie Deniau[(1)], Christophe Gransart[(1)], Anthony Fleury[(2)], Jonathan Villain[(1)]
(1) COSYS-LEOST, Univ Gustave Eiffel, IFSTTAR, Univ Lille, F-59650 Villeneuve d'Ascq, France,
(firstname.lastname)@univ-eiffel.fr
(2) IMT Lille Douai, Institut Mines-Télécom, Univ. Lille, Center for Digital Systems, F-59000 Lille, France,
Anthony.Fleury@imt-lille-douai.fr

Abstract

Wireless networks such as IEEE 802.11 networks are nowadays widely used. However, they are vulnerable to different forms of attacks such as the fake access point and the emission of intentional frequency sweeping jamming signals. In this paper, we present a Network-based Intrusion Detection System (NIDS) which uses a threshold-based approach to detect the two attacks on IEEE 802.11 networks. The NIDS analyses indicators derived from frame header information to determine the presence of the two attacks. We also discuss the limitations of this approach and give perspective for a new line of research based on a supervised learning model approach.

1 Introduction

Wireless networks are nowadays widely used as they allow mobility and the cheap and rapid expansion of computer networks. They are also essential to connect certain mobile equipment and small devices such as connected vehicles, and sensors. However, as compared to wired networks (which are often isolated in the ground, buildings...), wireless networks are more exposed and are therefore more vulnerable to certain types of attacks. IEEE 802.11 networks are, for instance, vulnerable to jamming and fake access points attacks. To protect these types of networks, we seek, in our research, to implement a Network Intrusion Detection System (NIDS) [1] to detect jamming and fake access point attacks on IEEE 802.11 networks in infrastructure mode.

A jamming attack is the intentional emission of signals in a frequency band in order to decrease the Signal to Interference ratio (SIR) and therefore degrade the reception of communications. There are different types of jamming attacks [2]. In our work, we considered frequency sweeping jammers because, even though their use is prohibited, they are relatively easy to obtain. A fake access point attack consists in the identity usurpation of a licit access point in order to trick users into thinking that the fake access point is the licit one. When a fake access point attack is successful, all the communication of devices in the 802.11 network passes through the fake access point rather than the licit access point. The attacker who is in control of the fake access point has therefore control over the communication and can read, modify or generate frames [2] [1].

To detect the two attacks, we have adopted an anomaly-based approach. This approach consists in the comparison of two situations (a normal situation and an attack situation) in order to identify differences and determine proper indicators to detect the attacks. Indicators can be determined manually using a threshold-based approach or automatically using supervised learning algorithms. In this paper, we present a threshold-based approach, its limitations and we explain why it is more interesting to adopt a supervised learning model approach.

The rest of the paper is organised as follows. In section 2, we detail our experimental setup for the normal and attack situations. In section 3, we detail the type of frames we have analyzed and the attributes and indicators we have selected. In section 4, we explain how we implemented the threshold-based approach on python and comment detection results for the fake access point attack. In section 5, we discussed the limitations of the threshold-based approach and give perspective for a new line of research based on a supervised learning model approach. Finally, in section 6, we conclude the paper.

2 Experimental Setup

To obtain data, we conducted laboratory experiments. We have configured three situations: a normal situation, a situation with a fake access point attack and a situation with a jamming attack.

Figure 1 describes the normal situation. In this situation, there is an observer, a client, an IEEE 802.11 access point, and a server. The client is connected to the access point via a Wi-Fi link on channel 13 (2.472 GHz). We have ensured

[1] A Network Intrusion Detection System is a system that analyzes incoming network traffic to detect anomalies, https://en.wikipedia.org/wiki/Intrusion$_{d}etection_{s}ystem$

[2] Frame, https://en.wikipedia.org/wiki/Frame$_{(}networking)$

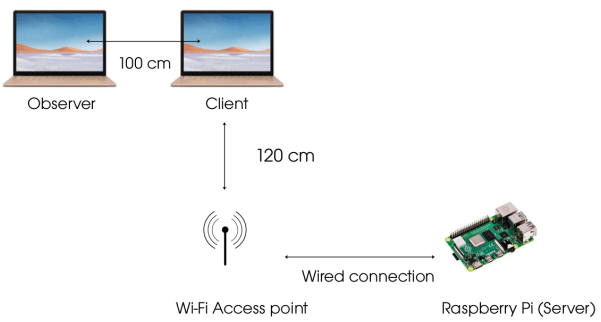

Figure 1. Setup in normal situation

that no other surrounding devices in the laboratory were communicating on channel 13. The server is connected to the access point via an ethernet cable (wired connection). Data is transmitted at a rate of 100 Mbps, using iPerf3 [3], by the server to the client via the access point. The client is at a distance of 120 cm from the access point and at a distance of 100 cm from the observer. The observer is a computer with a Wi-FI card in monitor mode. Monitor mode allows a device to capture all frames sent within a frequency channel. The observer is capturing all frames transmitted by the client and the access point during the experiment. The experiment lasts two minutes.

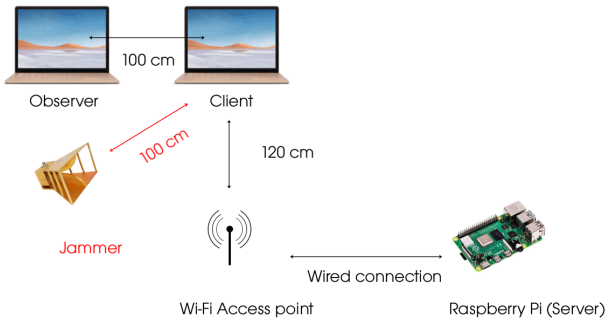

Figure 2. Setup with jamming attack

In the jamming attack situation, as shown in Figure 2, we have added a jamming signal generated by a signal generator and emitted using a directional antenna at a distance of 100 cm from the client. The rest of the configuration remains unchanged.

In the fake access point attack situation, as shown in Figure 3, we have added a fake access point, at a distance of 120 cm between the client and the server. The fake access point emits the same identification information (beacon frames) at the same interval and on the same frequency channel (channel 13) as the licit access point.

[3]iPerf3 is a tool for active measurements of the maximum achievable bandwidth on IP networks, https://iperf.fr/

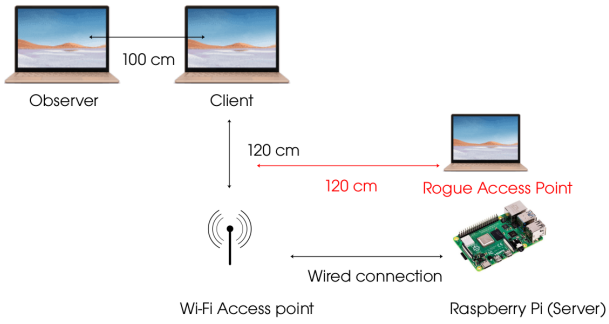

Figure 3. Setup with fake access point

3 Analysis and indicators selection

After the experiments, we have a two-minute capture for each situation. The observer has captured all frames transmitted on channel 13. According to the IEEE 802.11 specification, there are three types of frames: management frames, data frames, and control frames. Data frames are frames that contain user data while management frames are frames that are sent to handle discovery, connection, and disconnection with the access point. Control frames are frames sent to coordinate the emission of data frames. In our analysis, we have analysed only management and data frames.

Beacon frames are a subtype of management frames that are sent periodically by an access point to inform, devices in the channel, of its presence. According to the IEEE 802.11 specifications, beacon frames should be sent at an interval of 102.4 ms. A fake access point tries to send the same beacon frames at the same interval as the licit access point. Therefore when there is a fake access point attack operating on the same channel as the licit access point, devices in the channel should receive twice as many beacons. For this reason, we chose to study the distribution of attribute "beacon interval " during the two-minute experiment in the normal situation and the fake access point situation.

During the comparison, we have indeed noticed, as shown in Figure 4, that the mean beacon interval is around 51.2 ms in the fake access point situation and around 102.4 ms in the normal situation. Moreover, in beacon frames, there is a counter called the sequence number and this counter is incremented each a management frame is generated. When an attacker creates a fake access point, even though he can easily copy off some important "static" information of the licit's access point beacon frames, he cannot easily copy the sequence number. During the comparison, by further analyzing the attribute *sequence number gap*, we also noticed, as shown in Figure 5, that the gap range is higher when there is a fake access point attack.

We have concluded that based on our experiments, the following indicators can be used to detect a fake access point attack on IEEE 802.11 networks: Beacon Interval < 51.2 ms and Sequence Number gap > 8.

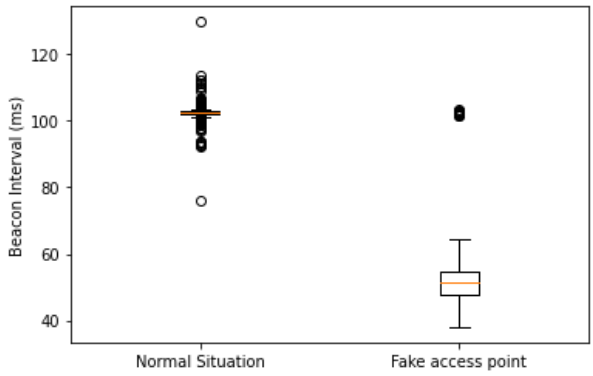

Figure 4. Data analysis- Beacon Interval

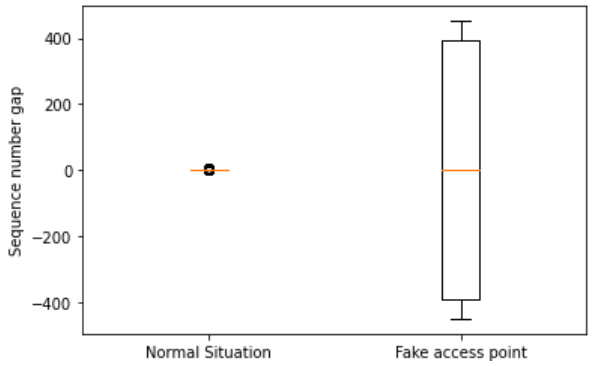

Figure 5. Data analysis- Sequence number gap

Concerning the jamming attack, we were expecting to receive little to no frames. However, as per our observations, we, actually, continue to receive management frames in the jamming situation. We have tried to modify the orientation of the jamming to make it face the observer, for instance, but the latter still receives the management frames. After further analysis, we found that management frames in the 2.4 GHz band are sent at a lower bit rate than data and control frames and are sent as Direct-Sequence spread spectrum Modulated Signals. These signals are resilient to frequency sweeping jamming signals. For this reason, we could not observe a significant change in the beacon interval between the normal and the jamming attack situation.

We, therefore, analysed only data frames and when studying the mean data frame interval, we noticed that, as shown in Figure 6, it drastically increases from 0.2 ms to 10000 ms. We concluded that based on our experiment and the data transmission rate (100 Mbps), the following indicator could reasonably be used to detect the presence of frequency sweeping jamming signals: data frame interval > 100 ms.

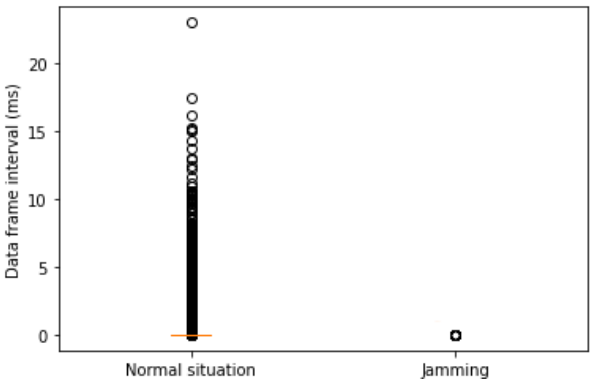

Figure 6. Data analysis- Data frame interval

4 Implementation and results

Based on these indicators, we have implemented a first version of the NIDS using Python [4]. The NIDS can detect the attack on a live stream or a capture file. In both cases, the NIDS analyses the live stream or capture file using a 10-second read buffer. It then decides based on the indicators whether there is the presence of a fake access point or frequency sweeping jamming signals in the 10-second buffer. The procedure is repeated continuously for the live stream and until the end of the file for the capture file. The result is displayed using a graphical interface as shown in Figure 7.

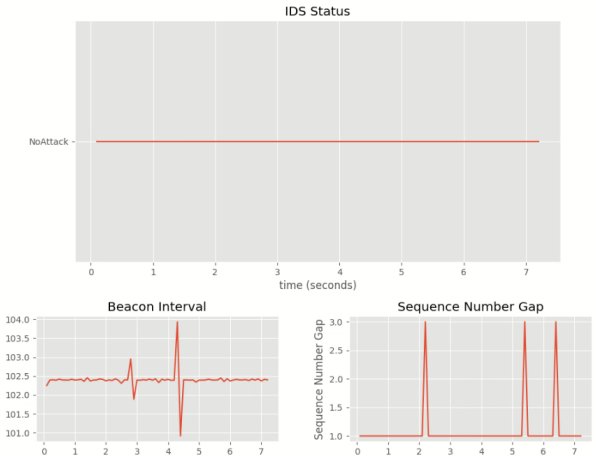

Figure 7. Monitoring the normal situation

We observe, as shown in Figure 7, that in the normal situation, the IDS Status is set to *NoAttack*. The NIDS supports its decision by displaying the graphs of beacon interval and sequence number gap against time. When we analyze the two graphs, we observe some fluctuations in both cases but values do not cross our predefined thresholds for attacks.

In the presence of a fake access point, as shown in Figure 8 the values cross our predefined thresholds, we observe that for instance, the beacon interval has been divided by 2 and

[4]Python is a programming language that lets you work quickly and integrate systems more effectively, https://www.python.org/

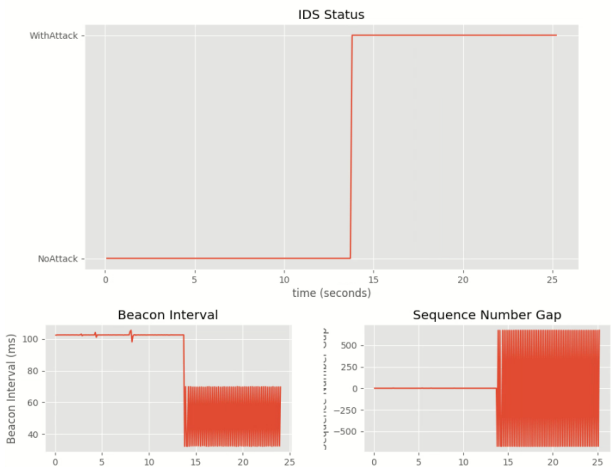

Figure 8. A Fake access point detection

that sequence number gap is greater than 8 and fluctuates between high intervals.

5 Limitations and Future Work

The detection fake access points and jamming attacks is not new in scientific research. Several authors have presented different ways to detect these attacks including the threshold-based approach based on beacon interval, sequence number gap and data frame interval [4, 5, 6, 7]. We want to differentiate our work by adopting a holistic approach to detect the attacks. Jamming attacks can be combined with a fake access point attack to increase the latter's effectiveness [1]. Deauthentication attacks [1] have a similar effect on fake access point attacks. We would like to have a single Network Intrusion Detection System that can detect the three attacks when they are perpetrated independently and simultaneously. Moreover, when detection is based on only one indicator, attackers can more easily adopt counter measurements. For this reason, we would also like to adopt a detection approach that analyses several indicators simultaneously. Finally, concerning the jamming attack, the effect of a jamming attack varies according to the transmission power. In this paper, we have studied the effect of jamming signals with strong transmission power. We would like to be able to study and detect the effect of various jamming power.

However, it is tedious to implement a threshold detection approach that can detect the three attacks independently and simultaneously by analysing several indicators simultaneously. For this reason, we have planned to adopt a machine learning approach [3] that will also allow us to consider multiple indicators, multiple attacks, multiple jamming effects, and combined attacks. We have also planned to integrate Software Defined Radio equipment (SDR) as an input source to our NIDS. Software Defined Radio equipment as opposed to Wi-Fi card in monitor mode will allow us to analyse signal characteristics that can be combined with frame header information to increase detection efficiency.

6 Conclusion

We have shown that it is possible to detect fake access points and frequency sweeping jamming attack situations on IEEE 802.11 networks using a threshold-based approach with indicators such as beacon interval, data frame interval, and sequence number gap. We have also highlighted that this detection approach has limitations and that it is difficult to implement when detecting combined attacks using several indicators. For these reasons, we have planned to adopt a machine learning approach in future work. We have also planned to integrate software radio equipment as an input source to our NIDS to increase detection efficiency.

7 Acknowledgements

This work is part of a thesis co-financed by the Region Hauts-de-France, University Gustave Eiffel and the GLOCAT project sponsored by the Region Hauts-de-France (Stimule project). The authors would like to thank the financiers for their support.

References

[1] A. Amoordon, C. Gransart and V. Deniau, "Characterizing Wi-Fi Man-In-the-Middle Attacks," *2020 XXXIIIrd General Assembly and Scientific Symposium of the International Union of Radio Science. IEEE*, 2020.

[2] K; Grover, A. Lim and Q. Yang, "Jamming and anti–jamming techniques in wireless networks: a survey," *International Journal of Ad Hoc and Ubiquitous Computing 17, 197–215*.

[3] S. Shalev-Shwartz and S. Ben-David, "Understanding Machine Learning: From Theory to Algorithms," *Cambridge University Press*, 2014.

[4] Guo, Fanglu and Chiueh, Tzi-cker, "Sequence number-based MAC address spoof detection, " *Springer, International Workshop on Recent Advances in Intrusion Detection pages 48 309–329*, 2005.

[5] Changdong Han and Jeong In-Jang and Jia-feng Shao and Kangsuk Chae and Bae Seong-Soo and Souhwan Jung, "A Scheme of Detection and Prevention Rogue AP using Comparison Security Condition of AP, ", 2012.

[6] Alotaibi, Bandar and Elleithy, Khaled, "Rogue access point detection: Taxonomy, challenges, and future directions, " *Springer, Wireless Personal Communications, volume 90 number 3 pages 1261–1290*, 2016.

[7] Pirayesh, Hossein and Zeng, Huacheng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey, " *arXiv preprint arXiv:2101.00292*, 2021