Energy effective jamming attacker in wireless network

Emilie Bout and Valeria Loscri
FUN - Self-organizing Future Ubiquitous Network
Inria Lille - Nord Europe, avenue Halley
Villeneuve d'Ascq, France

Antoine Gallais
Univ. Polytechnique Hauts-de-France, LAMIH, CNRS, UMR 8201
INSA Hauts-de-France
F-59313 Valenciennes, France

***Abstract*—Composed of devices with limited resources, IoT networks have several vulnerabilities. Their increasing deployment in critical sectors and infrastructures requires appropriate security measures. Although the concept of jamming attacks is old, they remain a significant threat in wireless communications today. Targeting both data transferred over the network and the energy reserves of IoT devices, these attacks can quickly lead to denials of service. Indeed, the latter consists in intentionally interfering with the signal used by the legitimate nodes on the network. This article is a summary of several works carried out on the study of jamming attacks from an attacker's point of view. First, an analysis of the effectiveness of the various existing jamming attack strategies, as a function of certain parameters such as energy and distance was realised. From this work, we created an "intelligent" jamming attack capable of optimizing the effectiveness of its attack and minimize its energy consumption, without the need to have knowledge of the targeted wireless networks.**

***Index Terms*—Jamming attack, WiFi, energy-effective, Markov Chain Theory, Internet of Things (IoT)**

I. Introduction

Jamming attacks consist in intentionally interfering with the communication medium to keep it occupied or to corrupt data in transit. The effectiveness of a jamming attack is based on many parameters such as the transmission properties (e.g., modulation, power), the characteristics of the network (e.g., routing), or also the strategy of the jammer along with its position. Studying these different points from the attacker's point of view can allow us to find new vulnerabilities in order to improve detection methods and make the communication protocol more robust.

By admitting the attacker perspective, we show in a first study, that there exists a trade-off between the efficiency of a jammer, its distance from the communication and its energy consumption. We assume an attacking node which aims to interfere the communication as much as possible, while maximizing its impact on the network and minimizing its energy consumption and its probability of being detected. We use the simulator NS-3 to compare the energy consumption spent by three distinct jamming strategies, as a function of its distance from the victim node and the distance between the transmitter and the receiver. Our analysis highlights not only the dependence of the attacker position with the transmitter node, but also the factors that determine the efficiency of an attack. Our evaluation allowed to understand that different types of attacks can be more effective based on different distances between two communication nodes. In the specific scenarios considered, the constant attack is with more impact than the random and the reactive ones, when the distance between the two communicating nodes is small (e.g., 20 meters). On the other hand, the reactive jamming is more effective when the distance between transmitter and receiver increases. More details are available in [1].

Following these results, we design a "smart attack" based on Markov chain theory implemented in a real test-bed. The goal is to maximize its attack success while minimizing its energy cost.

II. System model

A. Attacker Model

The attacker has the same configuration as the legitimate nodes in order to reduce the probability of being detected and it is also an energy-constrained node. We have chosen to implement two jamming approaches inspired by previous works [2] and we also propose an "intelligent" jamming attack.

Constant Jammer: The attacker injects packets on the legitimate channel, for a certain period, at regular time intervals. Its main goal is to occupy the communication channel as much as possible.

Reactive Jammer: This tactic aims to minimize the risk of being detected. Therefore, the attacker jams the channel only upon packet transmission.

Intelligent Jammer: It is a reactive attack but which admits 4 states: 1) Transmitting: the node is sending data on a wireless channel; 2) Receiving: a node is listening and receive data sent from other nodes; 3) Idle: a node is neither receiving nor transmitting but can switch from its current idle state to both transmitting and receiving states; 4) Sleep: a node is at the minimum energy consumption and it cannot switch to the transmitting or receiving state. The jamming node switches from one state to the other trying to maximize the probability to send data at the same time of the transmitter. By deriving an analytical framework based on Markov Chain Theory, the attacker is allowed to compute the probability of staying in each state in order to achieve the following objectives: a) Maximization of the attack effectiveness as the probability that the jamming node transmission occurs in the same slot when a transmitter node is transmitting by minimizing the energy

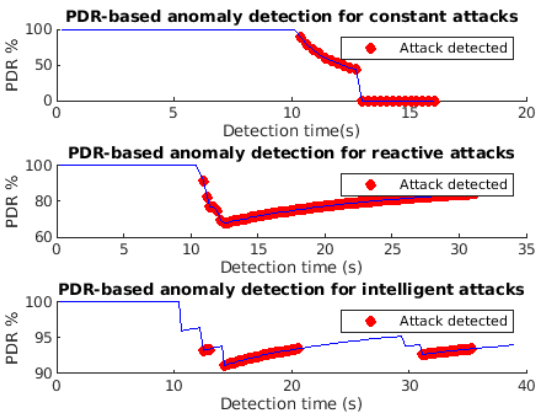

Fig. 1. PDR-based anomaly detection for each attack

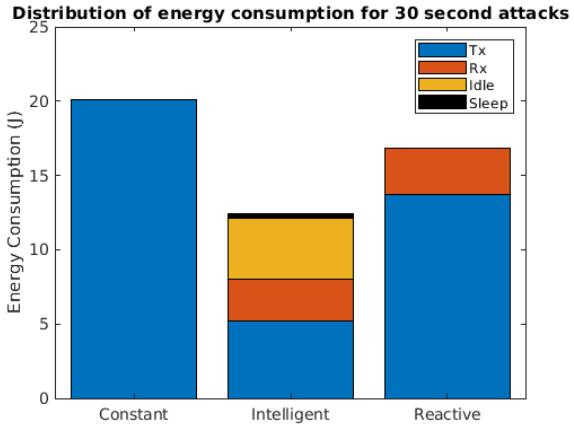

Fig. 2. Distribution of energy consumption for each attack performed during 30 seconds

expenditure; b) Given a certain limitation cost (in terms of energy), the maximization of the probability that the attack is occurring in a certain time interval.

III. Performance Evaluation

We implemented the three types of jamming strategies in a test-bed composed of a transmitter, a receiver and an attacker with the Wi-Fi protocol. The attacker is equipped with Alfa AWUS036h device and Realtek RTL8187L wireless chip. In order to implement jamming attacks, we have modified the driver of the wireless chip to get direct control over MAC layer parameters. The distance between the three nodes of the network is the same during all the experiments. In order to estimate the effectiveness of each attack strategy, we used the Packet Delivery Ratio (PDR) as a metric. PDR corresponds to the ratio of the number of packets that have been successfully delivered and acknowledged by the destination node over the number of packets sent [3]. In this study, the attack was detected after 1 observation. We evaluate the constant, reactive and ”intelligent” jammer by considering the three factors a) Detection Time; b) Energy Spent; c) Packet Delivery Ratio (PDR) in a sinergic way. Each attack was performed for 30 seconds and begins after 10 seconds of transmission.

Among the three types of attacks, the ”intelligent” jamming is less detectable than the constant and the reactive ones, as presented in 1. Indeed, the constant attack is immediately detected after 0.4 seconds from the start of the attack. The PDR drops significantly and after 5 seconds the transmitter and receiver lose connection with the access point. The reactive jammer is detected after 0.92 seconds from the start of the attack. The communication between sender and receiver is not lost, but this type of attack is quickly detected. ”Smart” attack is detectable 2.48 seconds after the start of the attack and has consequences as the attacker's PDR decreases by approximately 15%.

Moreover, as shown in Figure 2, the energy depleted by the ”intelligent” jamming node is lower than the other two types of attacks. Indeed, the ”intelligent” attack consumes a total of 12.4058 J for a 30 seconds attack, unlike the constant attack which consumes 20.1 J and the reactive 16.865 J.

Based on the results obtained from our experimentation, this ”smart” jamming attack is interesting because the attacker has the possibility of minimizing its energy consumption and its probability of being detectable while maximizing its impact on the network. In addition, this attack is less detectable than the other type of jamming attack and has a long-term impact. In fact, during these experimentations, this type of attack can reduce the flow by 15%.

IV. Conclusion

In this work, we considered that the main objective of reactive jamming is to perform an efficient attack with minimal energy expenditure. This type of attack is based on Markov Chain Theory with four macro-states of a typical wireless node. The combination of the quadruple probabilities are derived by imposing limitations in terms of energy that a jamming node can spend for attack and in terms of time interval for the attack to occur. Thereby this kind of attack is general and can be applied to different wireless networks by considering different energy consumption associated with the different states in order to derive the optimal values. In addition, this type of attack does not need knowledge about its victim. In future work, we aim to analyze this type of attack in more detail based on several energy consumption costs. A study will be carried out on the various solutions to be considered in the face of this type of attack.

References

[1] E. Bout, V. Loscri, and A. Gallais, “Energy and distance evaluation for jamming attacks in wireless networks,” in *2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, 2020, pp. 1–5.

[2] S. Jaitly, H. Malhotra, and B. Bhushan, “Security vulnerabilities and countermeasures against jamming attacks in wireless sensor networks: A survey,” in *2017 International Conference on Computer, Communications and Electronics (Comptelix)*, 2017.

[3] O. Osanaiye, A. Alfa, and G. Hancke, “A statistical approach to detect jamming attacks in wireless sensor networks,” *Sensors*, 2018.