Évaluation de l'énergie et de la distance pour les attaques de brouillage dans les réseaux sans fil

Emilie Bout, Valeria Loscri, Antoine Gallais

Évaluation de l'énergie et de la distance pour les attaques de brouillage dans les réseaux sans fil

Emilie Bout[1], Valeria Loscri[1] et Antoine Gallais[2]

[1] *Inria, 40 Avenue Halley, 59650 Villeneuve-d'Ascq, France*
[2] *UPHF, LAMIH, INSA Hauts-de-France, Valenciennes, France*

Composés d'appareils fortement limités en ressources, les réseaux sans fil présentent de nombreuses vulnérabilités. Leur déploiement croissant dans des secteurs et infrastructures critiques impose des mesures de sécurité adaptées. Parmi les menaces de sécurité les plus graves dans le domaine des communications sans fil, les attaques de brouillage peuvent mener à des dénis de service ou à l'arrêt total d'un appareil. En effet, ces dernières consistent à interférer intentionnellement avec le signal utilisé par les nœuds légitimes sur le réseau. Cet article résume notre analyse sur l'efficacité des différentes stratégies d'attaques de brouillage existantes, en fonction de certains paramètres comme l'énergie et la distance. Contrairement à d'autres travaux, nous avons choisi de porter l'analyse suivant le point de vue de l'attaquant, afin de minimiser sa consommation d'énergie et sa probabilité de détection, tout en maximisant son impact sur ses victimes.

Mots-clefs : Attaque de brouillage, Sécurité, WSN

1 Introduction

Jamming attacks consist in intentionally interfering with the communication medium to keep it occupied or to corrupt data in transit to cause a denial of service (DoS). 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 allows to improve detection methods, such as the location of jamming nodes [WLWF18].

By admitting the attacker perspective, we show 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. Multiple factors are evaluated all together, such as detection time, energy consumption and effectiveness to impact the communication. More details and a deeper analysis are available on [BLG20].

2 System model

2.1 Attacker Model

The attacker has the same configuration as the legitimate nodes in order to reduce the probability of being detected. To best correspond to reality, the attacking device is also an energy-constrained node. We have chosen to implement three jamming approaches inspired by previous works [JMB17].

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.

Random Jammer : Considering its limited resources (e.g., computation, energy), an attacker can save energy by going from an active state to an idle state, at random time intervals.

Reactive Jammer : This tactic aims to minimize the risk of being detected. Therefore, the attacker jams the channel only upon packet transmission. In theory, this strategy reduces attack time and increases its effectiveness because the attacker no longer blindly jams the network.

2.2 Attack Detection Model and Problem Formulation

In this work we consider a problem formulation from an attacker point of view in the discrete-time domain.

For each time slot t, we define a variable $x^t(i) \in [0,1]$ for all the positions/distances of the jamming node. We assume that the achievable rate between the transmitter and receiver can be approximated with link capacity c defined as :

$$c = W * log_2(1 + \frac{S}{N}), \tag{1}$$

where W is the system bandwidth and $\frac{S}{N}$ is the signal to noise ratio between the transmitter and receiver.

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 [OAH18]. In this study, the detection time correspond to the time needed to detect a attack. Detection takes place when the PDR exceeds a certain threshold. Since a "greedy" jamming node is considered, its main objective is to decrease the effective Packet Delivery Ratio (PDR), while minimizing its energy expenditure (which depends on its distance from the transmitter) and increasing its detection time. Intuitively, if the attacker is closer to the transmission, it can reduce its transmission power, thus spending less energy. However, its attack may fail since the detection time could be really short. Since we consider three different aspects that can be opposite to each other, we formulate three different functions F_1, F_2 and F_3. F_1 characterises the goal of impacting the PDR of the communication. In particular, in time slot t, the achieved rate in respect of the distance i is :

$$R^t(i) = x^t(i) * c^t(i), \tag{2}$$

and the function F_1 can be defined as :

$$F_1 = \sum_{t=1}^{T} \sum_{i=1}^{D} E[R^t(i)] = \sum_{t=1}^{T} \sum_{i=1}^{D} E[x^t(i) * c^t(i)], \tag{3}$$

where T is the total number of time slots, D is the distance, E is the expectation and is with the respect of randomness of $c^t(i)$, computed as in (1). Hereafter, $E[.]$ will indicate the average. F_1 accounts the fact that if the transmissions of both the emitting and the jamming nodes happen in the same time slot, they will collide with high probability. This means that if the packet reaches the receiver, it will fail the CRC control, thus getting discarded, with a negative effect on the PDR. The function F_2 accounts the energy expenditure of the jamming node, depending on its distance to the transmission, and can be expressed as :

$$F_2 = \sum_{i=1}^{D} E[i^2] \tag{4}$$

The function F_3 accounts for the detection time, that is proportional to the distance of the jamming node. The greater the distance of the attacker, the longer it would take to detect the attack. However, if the attacker is too far, an effective attack would have a smaller impact while requiring more energy consumption for the attacker node. We thus compute F_3 as follows :

$$F_3 = \sum_{i=1}^{D} E[E_n(i)], \tag{5}$$

where $E_n(i)$ is a function proportional to the distance.

We then compute :

$$\min(F_1 + \lambda_e * F_2 - \lambda_d * F_3) \tag{6}$$

subject to

$$\sum_{i=1}^{D} 1x^j(i) < \delta, \tag{7}$$

$$\sum_{i=1}^{D} \Pi^i x^j(i) = 0, \tag{8}$$

where δ is a threshold distance (beyond this distance the attack has no effect on the transmission), λ_e is a parameter for considering the importance of the energy consumption, while λ_d is to consider the detection factor. The equation (8) means that for each distance there is at least one slot where the transmitter and the attacker send data in the same slot.

3 Performance Evaluation

Our objective is to evaluate the impact of the different kinds of jamming attacks on the network as a function of both the malicious nodes placement as well as their energy consumption. In particular, we evaluate the constant, random and reactive jammer by considering the three factors a) Detection Time ; b) Energy Spent ; c) Packet Delivery Ratio (PDR) in a sinergic way. Threrefore, we have implemented the functions F_1, F_2 and F_3 and we evaluated them for the different types of attacks by using the discrete event simulator NS-3 (Network Simulator-3). F_1 determines the type of attack by specifying the jamming attack slots. For example, the constant jamming sends packets periodically, so we implement the F_1 by considering the specific slots occupied by the jammer. In this case the time slots are always the same. Moreover ; if we consider the reactive, the slots will be adapted based on the transmitter slots that the jammer intercepts and we account for these slots in the computation of the function F_1. Concerning the function F_2 and F_3 we have considered equal weight in our simulation for the factors λ_e and λ_e in order to not prioritize the detection or the energy. Of course, based on its current situation, the jammer has the faculty to apply an higher weight to a factor.The first type of simulations are based on a 20 meter distance between the transmitter and the receiver. In Figure 1, we report the a) Detection Time as function of distance, the b) Total Energy Spent for an attack by the jamming node and the c) Packet Delivery Ratio of the communication between the transmitter and the receiver.

Among the three types of attacks, the reactive jamming is less detectable than the constant and the random ones. On the other hand, the energy depleted by the reactive jamming node is much higher than for the other two types of attacks. Moreover, the detection time increases for constant and random attacks when the attacker is positioned around $25-35$ meters from the receiver (the victim). In particular, the constant jamming is more effective in this distance interval, since the energy wasted for the attacks is less than 2 Joules. The detection time increases and achieves 3 seconds around 35 meters. The PDR is sensibly impacted by considering that, up to 30 meters of the attacker distance, the PDR is smaller than 80%.

We evaluate how the distance between the transmitter and receiver impacts the effectiveness of a jamming attack, when the same power level of the transmitter is considered. We consider distances of 40 and 60 meters between the two nodes. In both scenarios, the reactive jammer is the most effective. In particular, for the case of a 60 meter distance, when the jamming node is positioned at around 50 meters from the transmitter, detection time is around 2.4 seconds (resp. 3 seconds at 65 meters). The PDR is highly impacted since it reaches 70% at 50 meters, and 90% at 65 meters. In practice, the optimal position of the reactive jamming in this scenario is around 50 meters with an energy consumption around 2 joules. The other two attacks have a low energy consumption, but the detection time intervenes before the PDR is significantly impacted. More details on the results for 40 and 60 meters are provided in [BLG20].

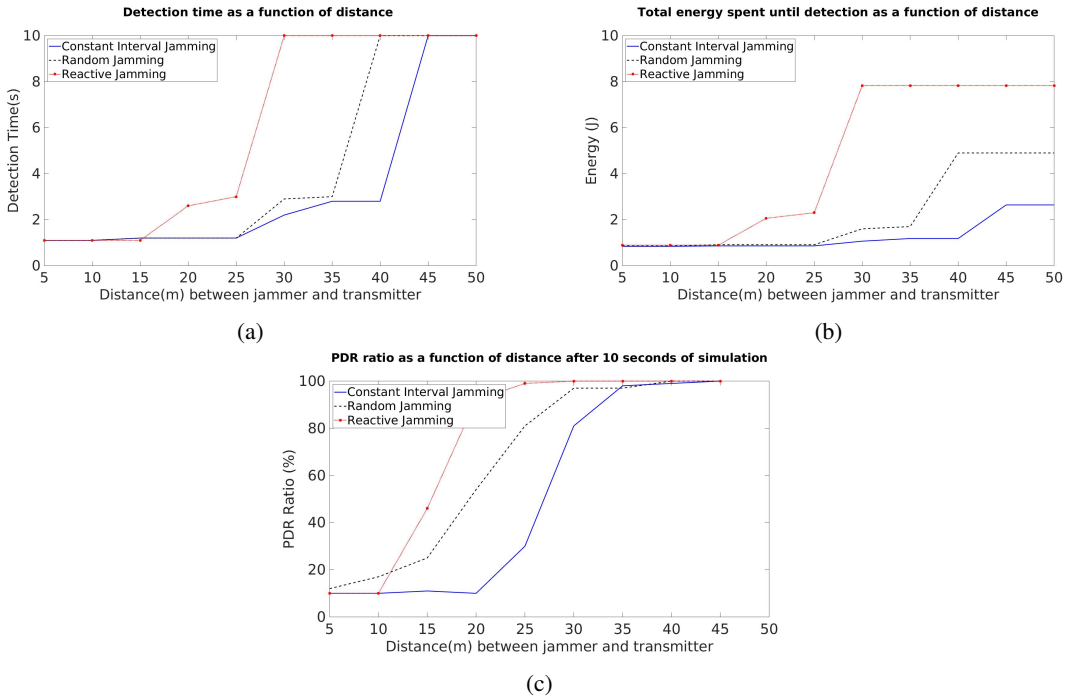

FIGURE 1: Distance between Transmitter and Receiver equal to 20 meters (a) Detection Time ; (b) Total Energy spent by the jamming node. (c) Packet Delivery Ratio.

4 Conclusion

The analysis dealt in the different scenarios arises some interesting observations. First of all, as already assessed in other previous works, there is a strong relation between the position of an attacker and its effectiveness in a wireless context. As the attacker considered in this work is a greedy node, aiming at being effective in terms of impact (i.e. by lowering the PDR) but with the minimum energy consumption, 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.

Based on these results, it would be interesting thereafter to consider an ”smart attack” which would select the most appropriate jamming strategy and its position in the networks according to these studied parameters.

Références

[BLG20] Emilie Bout, Valeria Loscri, and Antoine 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.

[JMB17] 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.

[OAH18] Opeyemi Osanaiye, Attahiru Alfa, and Gerhard Hancke. A statistical approach to detect jamming attacks in wireless sensor networks. *Sensors*, 2018.

[WLWF18] T. Wang, T. Liang, X. Wei, and J. Fan. Localization of directional jammer in wireless sensor networks. In *2018 International Conference on Robots Intelligent System (ICRIS)*, 2018.