Energy and Distance evaluation for Jamming Attacks in wireless networks

Emilie Bout, Valeria Loscrì, Antoine Gallais

Energy and Distance evaluation for Jamming Attacks in wireless networks

Emilie Bout and Valeria Loscri
FUN - Self-organizing Future Ubiquitous Network
Inria Lille - Nord Europe, avenue Halley
Villeneuve d'Ascq, France
{emilie.bout,valeria.loscri}@inria.fr

Antoine Gallais
LAMIH lab, CNRS
Polytechnic University Hauts-de-France, Le Mont Houy
Valenciennes, France
antoine.gallais@uphf.fr

***Abstract*—Wireless networks are prone to jamming-type attacks due to their shared medium. An attacker node can send a radio frequency signal and if this signal interferes with the "normal" signals of two communicating nodes, the communication can be severely impacted. In this paper, we examine radio interference attacks from the jamming node perspective. In particular, we assume a "greedy" jamming node, whose main twofold objectives are to attack and interfere the communication of a transmitter and a receiver node, by minimizing its energy consumption and maximizing the detection time. The two communication nodes are static during the attack window time, while the attacker node can adapt its distance from the transmitter in order to select the most suitable range for a successful interference. In order to take into account the distance factor for the effectiveness of the attack, we derive an optimization model for representing the attack and we will study the key factors that allow effective and efficient implementation of a jamming attack, namely a) the energy b) the detection time and c) the impact on the transmission in terms of lowering the PDR. Three different types of attacks will be analyzed, 1) Constant Jamming, 2) Random Jamming and 3) Reactive Jamming. Simulation results show that the effectiveness of a jamming attack in respect to the others not only depends on the position of the jamming node but also on the distance between the transmitter and receiver nodes.**

***Index Terms*—Placement jammer problem, Jamming attacks, Security, Wireless Networks.**

I. Introduction

The inherent openness of the wireless transmission medium has made wireless communication systems particularly vulnerable to a multitude of attacks. One of the biggest threats to these communication systems is the jamming attack, in part by its ease of implementation. This kind of attack consists in intentionally interfering with the communication medium to keep it occupied or to corrupt data in transit to cause a denial of service (DoS). Most research has been focused on creating new detection methods or countermeasures [1]–[4]. Nevertheless little work has been oriented towards optimizing the impact of these attacks.

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. The last point has been the subject of a few studies in recent years under the name of *jammer placement problem*. The goal of this problem is to find the optimal position of the jammer to minimize the throughput of the network. Studying this dilemma would make it possible to improve detection methods, such as the location of jamming nodes [5], [6].

In [7], the authors study the impact of several types of jammers as a function of their distance from the victim nodes and the size of packets. They deduce that the closer the attacker is to his victim, the more effective it is. However, this also leads to a high probability of detection. Panyim et al. wondered if the random positioning of a jammer can be more effective than when the choice of the position of the attacker is made strategically [8]. They conclude that the aggressor has more impact on the network when the jammer is situated next to a node where a lot of data transits. The number of jamming devices (and their locations) required to suppress a given network was also investigated [9]. They compare the impact of the jammer when it is placed at random and when it is placed on a uniform grid. This placement problem can be formulated in the form of an optimization problem where the goal is to corrupt a maximum number of packets from the target network, while keeping a low detection probability [10].

This study is inspired by those previous works but takes into account the fact that the attacker is also a constrained node (e.g., energy, computation). By considering the attacker perspective, we show here 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 [11] to compare the energy consumption spent by the 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 show that for each, the distance between the two communication nodes influences the jamming efficiency and the probability of being detected. We also expose that for each scenario, there is a position of the attacker which makes it possible to reduce its energy consumption and its probability of being detected while having a reasonable impact on the networks.

The main objective of this study is to prove that the choice of the optimal interference strategy does not only depend on

its position in the network but also on its energy consumption and its probability of being detected.

This article is organized as follows. In section II, the network model, the jamming attack strategies, and the detection issue are described. We introduce, in section III the problem formulation and we provide details of simulations and results in section IV. We conclude the paper in section V.

II. System model

A. Network Model

We consider a wireless communication scenario with one transmitter, one receiver and one jammer. We assume that radios have equal transmit power and equal noise power. We assume that nodes are limited in energy. We define an amount of energy in the initial state E_0. At the end of each transmission or each change of state of a device, the consumed energy of a node is calculated as follows:

$$E_{i+1} = E_i + V * (t_{i+1} - t_i) * I_i, \tag{1}$$

where E_i is the energy consumption at time t_i, V is the supply voltage and I_i is the total current draw at node i.

B. 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. The energy consumption is calculated in the same way as for the other nodes of the network by following the formula 1.

A jamming attack has the purpose of causing a denial of service by preventing the exchange of packets between the legitimate nodes of the network. The jammer has the option of voluntarily occupying the channel or causing collisions in order to corrupt the packet and force the node to retransmit. Several jamming strategies [2], [3], listed below, have been developed over the years to make the jammer more efficient and less detectable.

Constant Jammer: The basic strategy is to continuously send random bits on the channel to occupy the transmission channel for a certain time. However, from an attacker's point of view, this strategy consumes a lot of energy and is easily identifiable.

Deceptive Jammer: Instead of sending random bits, the jammer injects packets continuously on the channel. The goal is to deceive the receiver so that it remains in reception status. Just like for the first strategy this one consumes a lot of battery and resource for an attacker.

Random Jammer: This method allows the attacker to save energy by going from an active state to a sleeping state at random time intervals. During the active state, the jammer can choose between the two approaches seen above.

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

We have chosen to implement three jamming approaches inspired by those mentioned above. Our first strategy: *Constant Interval Jammer* consists in injecting packets on the channel for a certain period at regular time intervals. We have chosen here a time interval between two very short jammings in order to corrupt a maximum of packets.

The second is an implementation of a *Randon jammer* which randomly draws the duration during which it will remain in an idle state after each sending of packets in a given interval. The aggressor, therefore, alternates the two states randomly. The last implementation corresponds to a *Reactive Jammer*.

Table I shows the send interval for each type of jammer during the simulation.

Parameters	**Constant Interval Jammer**	**Random Jammer**	**Reactive Jammer**
Send interval (ms)	1	Between 100 and 1	Send interval of the legitimate node
Energy (J)	55	55	55
Supply voltage (V)	3	3	3

TABLE I: Jamming node Settings.

C. Attack Detection Model

One of the most used metrics to detect a jamming attack is the Packet delivery ratio (PDR) [7], [12], mentioned below:

$$\textit{Packet Delivery Ratio} = \frac{\sum \text{Number of PSD}}{\sum \text{Number of PT}}, \tag{2}$$

where PSD is the number of packets successfully received at the destination and PT represents the actual number of packets transmitted at the source. In our case, the update of the global PDR of the network is done after each packet sent by the transmitter. Detection is done at a regular time-frequency and is based on a predefined detection threshold when the network is set up. When the PDR comes to be below the detection threshold an attack is then identified. We assume that we are in an optimal situation where the PDR ratio with no attack, is 100%. Therefore, during the simulations, we have defined the detection threshold at 99%.

III. Problem Formulation

In this section we propose a formulation of the problem 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:

$$c = W * log_2(1 + \frac{S}{N}), \tag{3}$$

where W is the system bandwidth and $\frac{S}{N}$ is the signal to noise ratio between the transmitter and receiver. We assume that in the absence of any external interference (i.e., jamming

attacker), the achieved capacity only depends on the reciprocal distance between the two communicating nodes.

Since a "greedy" jamming node is considered, its main objective is to decrease the effective Packet Delivery Ratio (PDR), by minimizing its energy expenditure (which depends on its distance from the transmitter) and increasing its detection time. Intuitively, if the attacker is close to transmission, it will be more effective by spending less energy (that is adjusted with the distance), yet its attack can be a failure since the detection time can be really fast. 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 is for characterising 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:

$$R^t(i) = x^t(i) * c^t(i), \tag{4}$$

and the function F_1 can be defined as:

$$F_1 = \sum_{t=1}^{T}\sum_{i=1}^{D} E[R^t(i)] = \sum_{t=1}^{T}\sum_{i=1}^{D} E[x^t(i) * c^t(i)], \tag{5}$$

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 (3). Hereafter, $E[.]$ will indicate the average. F_1 is for accounting 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 is for accounting the energy expenditure of the jamming node, depending on its distance to the transmission, and can be expressed as:

$$F_2 = \sum_{i=1}^{D} E[i^2] \tag{6}$$

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:

$$F_3 = \sum_{i=1}^{D} E[E_n(i)], \tag{7}$$

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

We then compute:

$$\min(F_1 + \lambda_e * F_2 - \lambda_d * F_3) \tag{8}$$

subject to

$$\sum_{i=1}^{D} 1x^t(i) < \delta, \tag{9}$$

$$\sum_{i=1}^{D} \Pi^i x^t(i) = 0, \tag{10}$$

where δ is a threshold distance (beyond this distance the attack has no effect on the transmission), λ_e is a variable for considering the importance of the energy consumption, while the variable λ_d is to consider the detection factor. The equation (10) means that for each distance there is at least one slot where the transmitter and the attacker send data in the same slot. This optimization problem is non-linear and the different types of attacks considered will not be optimal. Such as an example, the reactive jamming tries to "intercept" the transmission, but in order to do that the energy consumption will be larger.

Hereafter, we evaluate the different types of attacks in respect of the impact on the PDR, the energy consumption of the attacker node and the detection time. In particular, we implement the different functions F_1, F_2 and F_3 and we evaluate them for the different types of attacks.

IV. Performance Evaluation

A. Simulation Details

The jamming attacks were simulated using the discrete event simulator NS-3 (Network Simulator-3). The parameters set during simulations are shown in Table II. The transmitter constantly transmits packets every 0.1 seconds and begins its transmission at the start of the simulation ($t = 0$). The jammer aims to jam the transmitter node.

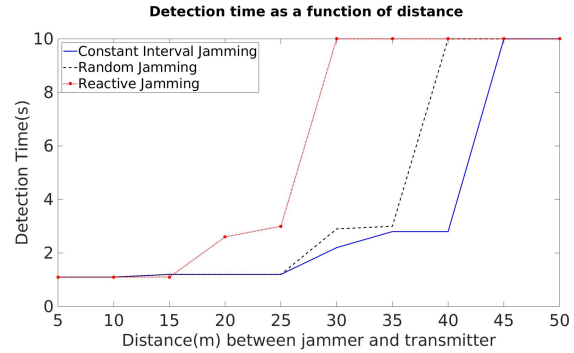
Parameter Name	Setting Used
Radio Propagation Model	Friis Propagation Loss Model
Routing protocol	Ad-hoc routing
Energy Model	EnergyBasicModel
Size of Legitimate Packet(octets)	1000
Send interval legitimate nodes(s)	0.1

TABLE II: Simulation and Node Parameters.

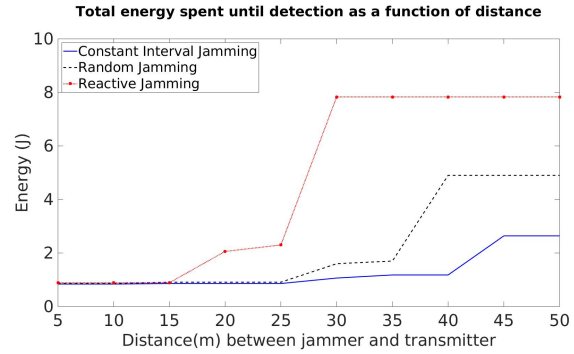
B. Results and Analysis

Our objective is to evaluate the impact of the different kinds of jamming attacks on the network as function of the placement of the malicious node. A study about energy consumption as a function of the placement of the attacker is also carried. In particular, we evaluate the three different types of jamming attacks, the constant interval jammer, the random jamming and the reactive jamming by considering the three factors a) Detection Time; b) Energy Spent; c) Packet Delivery Ratio (PDR) in a sinergic way. Indeed, in order to be effective, an attack has to be detected as late as possible (high detection time), the attacker has to minimize its energy consumption and the PDR between transmitter and receiver has to be impacted as much as possible.

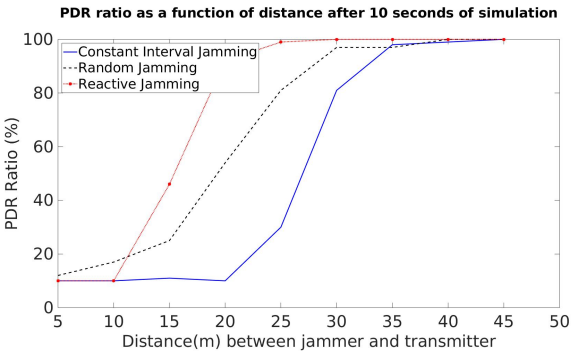
The first type of simulations are based on a distance between the transmitter and the receiver of 20 meters. In Figure 1, we report the a) Detection Time as function of distance, the b) Total Energy Spent for an attack by the jamming node and the c) Packet Delivery Ratio of the communication between the transmitter and the receiver.



(*a*)



(*b*)



(*c*)

Fig. 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.

Among the three types of attacks, the reactive jamming is less detectable than the constant and random ones. On the other hand, the energy depleted by the reactive jamming node is much higher than for the others two types of attacks. Moreover, the detection time increases for constant and random attacks when the attacker is positioned around $25 - 35$ meters.

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 is increasing and achieves 3 seconds around 35 meters but the PDR is sensibly impacted by considering that up to 30 meters of the attacker distance, the PDR is smaller than 80%. It is worth to recall that we are considering an ideal scenario, where no other communication interfere with the channel of the transmitter and receiver, so we expect 100% as PDR. The constant jamming impacts the channel of a 20% in terms of PDR.

In order to evaluate how the distance between the transmitter and receiver impacts on the effectiveness of a jamming attack, when the same power level of the transmitter is considered, we increase the distance between the sending node and the receiver to 60 meters. This scenario confirms that the most effective attack is the reactive jamming.

Indeed, when the jamming node is positioned at around 50 meters from the transmitter, detection time is around 2.4 seconds and achieves 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 others two attacks have a low energy consumption, but their attacks are not effective since the detection time is almost constant and equal to 1 second (i.e., the attack is soon detected) and just increases a little bit around 80 meters.

C. Discussion

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. A jamming node can easily implements the three different types of attacks by switching from one to the other, based on the specific situation of the two nodes that are communicating. It is sufficient for the attacker node to listen for a sufficient time in order to acquire the needed data and infer information as the distance between the two nodes.

In this work we have considered an ”ideal” scenario where only two nodes are exchanging data, so no external interference is considered; the detection is also ideal, in the sense that it is with a fixed threshold and we assume it is able to perfectly detect the jamming attack with no false alarm. This is not true in a realistic scenario, where lower PDR can be caused for different reasons and the detection scheme needs to account for all these situations. The main objective of this analysis was to highlight not only the dependence of the attacker position

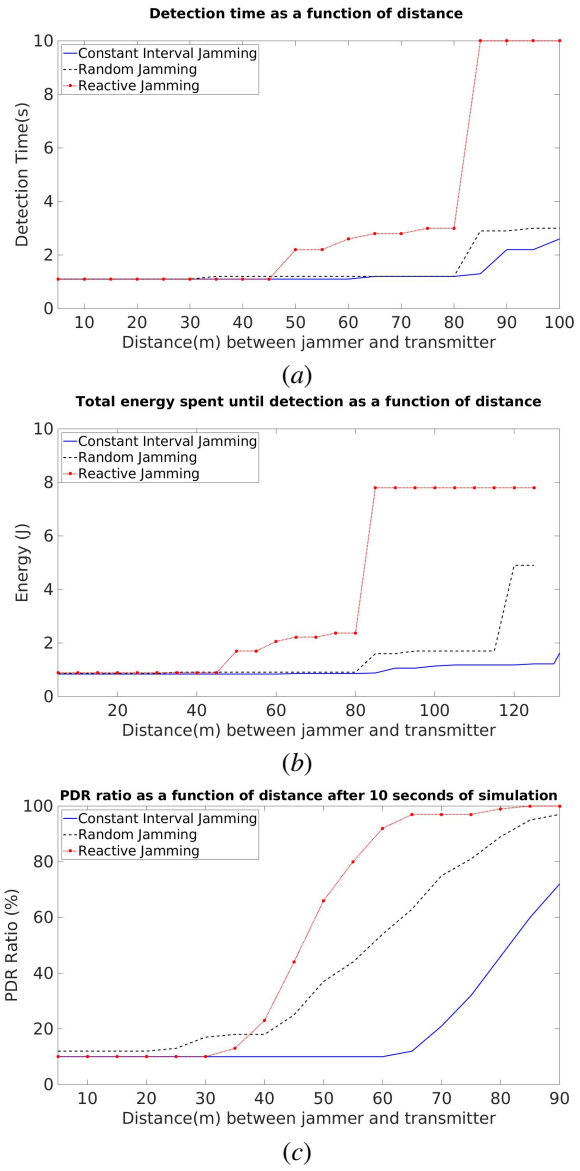


Fig. 2: Distance between Transmitter and Receiver equal to 60 meters (*a*) Detection Time, and (*b*) Total Energy spent by the jamming node. (*c*) Packet Delivery Ratio.

with the transmitter node, but also the fact that an attack can be more effective than others depending on the specific scenarios when multiple factors are evaluated all together, such as detection time, energy consumption and effectiveness to impact the communication.

V. Conclusion

In this paper, we have studied the impact of the position of three kinds of jammer as a function of the distance between the legitimate nodes of the networks. In order to evaluate the performance of the different jamming nodes, we have considered not only the impact on the PDR of the "legitimate" nodes, but also the detection time and the energy spent by the attacker node. The key factors, namely, the energy consumption, the impact of the attack in terms of PDR and the detection time have to be considered in a unique framework in order to evaluate the best positioning and also the best type of jamming. Indeed, results have shown that a type of jamming attack can be more effective than others, depending on the relative distance of the transmitter and receiver nodes. Based on these results, it would be interesting thereafter to consider an attacker which would select the most appropriate jamming strategy and its position in the networks according to these studied parameters. Our future work will be based on a network composed of numerous nodes or mobile nodes or both. It would also be interesting to study this problem on multi-channel networks. Indeed, all these parameters can vary the impact of each attack strategy.

Acknowledgment

This work was partially supported by the *General Armament Direction, France* and the *Defense Innovation Agency, France*.

References

[1] S. R. Ratna and R. Ravi, "Survey on jamming wireless networks: Attacks and prevention strategies," *International Journal of Computer and Information Engineering*, vol. 9, no. 2, pp. 642 – 648, 2015. [Online]. Available: https://publications.waset.org/vol/98

[2] T. Hamza, G. Kaddoum, A. Meddeb, and G. Matar, "A survey on intelligent mac layer jamming attacks and countermeasures in wsns," in *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, 2016, pp. 1–5.

[3] 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, pp. 559–564.

[4] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 17, no. 4, p. 197–215, Dec. 2014. [Online]. Available: https://doi.org/10.1504/IJAHUC.2014.066419

[5] Q. M. Ashraf, M. H. Habaebi, and M. R. Islam, "Jammer localization using wireless devices with mitigation by self-configuration," *PLOS ONE*, vol. 11, no. 9, pp. 1–21, 09 2016. [Online]. Available: https://doi.org/10.1371/journal.pone.0160311

[6] 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, pp. 198–202.

[7] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. MobiHoc '05. New York, NY, USA: Association for Computing Machinery, 2005, p. 46–57. [Online]. Available: https://doi.org/10.1145/1062689.1062697

[8] K. Panyim, T. Hayajneh, P. Krishnamurthy, and D. Tipper, "On limited-range strategic/random jamming attacks in wireless ad hoc networks," in *2009 IEEE 34th Conference on Local Computer Networks*, 2009, pp. 922–929.

[9] C. Commander, P. Pardalos, V. Ryabchenko, O. Shylo, S. Uryasev, and G. Zrazhevsky, "Jamming communication networks under complete uncertainty," *Optimization Letters*, vol. 2, pp. 53–70, 01 2008.

[10] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, 2007, pp. 1307–1315.

[11] "Ns-3 website," https://www.nsnam.org/, last accessed 14 June 2020.

[12] O. Osanaiye, A. Alfa, and G. Hancke, "A statistical approach to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 18, 05 2018.