An adaptable module for designing jamming attacks in WiFi networks for ns-3

Emilie Bout, Valeria Loscrì

An adaptable module for designing jamming attacks in WiFi networks for ns-3

Emilie Bout
Inria Lille-Nord Europe
Villeneuve d'Ascq, Hauts-de-France, France
emilie.bout@inria.fr

Valeria Loscri
Inria Lille-Nord Europe
Villeneuve d'Ascq, Hauts-de-France, France
valeria.loscri@inria.fr

ABSTRACT

The inherent openness of wireless communication techniques has made them vulnerable to jamming attacks. However, the effectiveness of a jamming attack depends on numerous parameters and varies according to the state of the environment. At the same time, attacks are becoming increasingly sophisticated and attempt to evade basic detection methods. Consequently, there is a real need to evaluate this new type of attack to improve the robustness of the detection and mitigation methods. A simulating tool to assess the impact of jamming attacks on wireless networks has become essential to gain effectiveness against attackers. This paper proposes a module of jamming attack for the discrete network simulator 3 (ns-3). This module, adaptable to any type of jamming attack strategy, provides a set of essential metrics allowing their evaluation. We evaluate the module by comparing the impacts of different types of jamming attacks already carried out in a real environment.

CCS CONCEPTS

• **Networks** → **Network simulations**; • **Security and privacy** → **Denial-of-service attacks**.

KEYWORDS

Networks Simulator, Jamming Attacks, Wireless Networks

1 INTRODUCTION

The security of wireless networks, by their nature, still raises specific issues today. Jamming attacks attempt to intentionally occupy a channel to avoid a transmission between two nodes and lead in most cases to denials of services. This type of attack based on the vulnerabilities of the physical layer produces different behaviors according to a multitude of parameters such as the number of different networks nearby, the distance from its victim or the type of obstacle. This is why an exact study of jamming attacks requires expensive means like an anechoic chamber. In parallel, the concept of green attacks emerges in the literature, and it is now unrealistic to create energy-intensive attacks in specific contexts like Internet of Things (IoT) networks [1]. Consequently, the evaluation of energy consumption represents a significant point and can be done more easily with a simulator. Finally, the increasing use of machine learning (ML) algorithms is driving a significant change in the threat landscape [2]. Jamming attacks exploiting this technology are becoming more adaptive, more resistant, more reactive, and less identifiable by the existing detection methods.

In this context, a network simulator such as network simulator 3 (ns-3) could be extremely useful. Indeed, in addition to the reproducibility aspect, it also makes it possible to quickly evaluate essential parameters. A ns-3 jamming attacks module for WiFi networks is already present. However, this module is over 10 years old and has been unmaintained since. An update is therefore essential to take into account the latest versions of 802.11 and to respond to the new characteristics of jamming attacks. In addition, it requires many changes in the Physical Class of the WiFi module, consequently the integration of this module was extremely hazardous. Therefore, we have improved this module on various points such as a major update with the latest version of ns-3, the addition of the "ns-3 gym" module to directly create smart jamming attacks and smart mitigation methods and the implementation of new metrics.

We prove the performance of the module by implementing an smart mitigation method already approved in the literature [10]. The results show our implementation has performances close to those obtained with real experiments. The complete code of this module is available in [4] and the documentation in [5]. This paper is structured as follows. In Section 2 we describe the concept of jamming attacks and the various methods to mitigate them. We introduce the motivation and the architecture of this new module in Section 3. Then, based on works in literature, we demonstrate the case of the reproducibility of a "Smart Mitigation method" in Section 4. Finally, in Section 5 we draw a conclusion and examine the future works.

2 OVERVIEW OF JAMMING ATTACK

2.1 Jamming Attacks

Jamming attacks aim to cause a denial of service by degrading the channel's quality and preventing the exchange of packets between legitimate network nodes. Several parameters influence the effectiveness of a jamming attack such as the transmission properties, the characteristics of the network, or also the strategy employed. Several attack strategies have appeared in the literature over the last decade, summarized in [6], that it possible to classify according to their complexity:

- **Basic Jamming Methods**: This class includes all the methods developed with simple processes and logic. In this group we find the *constant jamming* or *random jamming* attack strategies.
- **Smart Jamming Methods**: This category contains all jamming attacks developed with more elaborate processes such as Machine Learning approaches. These attacks attempt to address certain issues such as countering security systems. The work of Chen Zhong et al. belongs to this category [11]. Based on deep reinforcement learning (DRL) the attacker's goal is to counter the channel hopping by predicting the future transmission channel.

2.2 Detection methods and mitigation methods

Several metrics have been discovered in the last decade to detect jamming attacks. All the different metrics developed in the literature to detect jamming attack are summarized in [3]. Among the best known, we find the Packet Delivered Ratio (PDR) which corresponds to ratio between the total of packets correctly received over the total of packets sent. Thanks to these different metrics, detection techniques have emerged. Once the detection takes place, the victims have the possibility to react with mitigation methods in order to limit the damage of a jammer. As with jamming detection methods, several approaches of mitigation are possible [9]. However, in this section, we only discuss the mitigation method currently implemented in the simulator: the channel hopping. Channel hopping involves dynamically changing the communication channel to mitigate interference. As with jamming attacks, several strategies exist and can be classified according to their complexity:

- **Basic Channel Hopping Methods:** This group consists of simple strategies such as incremental channel hopping or random channel hopping method.
- **Smart Channel Hopping Methods:** We find in this group all the channel hopping methods based on a more complex methodology. Their main goal is to improve the effectiveness of the channel hopping by predicting the optimal future transmission channel or by misleading the strategy of a jammer. In the module proposed in this paper, we have implemented a channel hopping strategy based on a multi armed bandit (MAB) algorithm, as described in [10].

3 NS-3 IMPLEMENTATION

3.1 Motivations

The ns-3 simulator is a discrete event network simulator and its freeness, makes it an ideal tool for extending the reproducibility of results in research [8]. After some research on a complete jamming attack module, we decided to rely on this work of [7]. However, this later has not been updated for over ten years and is based on an old version of ns-3. In addition, during its installation, we had to modify certain classes belonging to other modules such as the *"WiFi-Phy"* or *"InterferenceHelper"* classes. These changes were therefore risky and time-consuming.

In this new version, we update the previous work in order to improve some elements such as the compatibilty with the latest version of ns-3 and the addition to new metrics. In addition of the two metrics already available in the previous version (PDR and RSSI), we added to this module the victim's energy expenditure and the Inter arrival time (IAT) metrics.

To finish, one of the main contributions is the integration of tools into the module to create smart jamming attacks and smart mitigation methods. Indeed, we integrated "ns-3-gym" in order to create new Subclasses of Jammer and Mitigation. Consequently, the integration of this module allowed us to easily and quickly simulate jammers and mitigation methods using reinforcement learning algorithms.

3.2 Architecture

In this section, we present the architectural model of the new jamming module. This module is integrated between the physical and MAC layers of the communication protocols. As we see in Fig 1, the jamming module is composed of four main components and provides a set of essential functions (called APIs) to exploit them. The APIs make it possible to directly control the jammer or the mitigation system from the nodes. The main components of the jamming module are the following:

- **Physical Layer Driver Class:** The main purpose of this class is to connect the jamming module with the *WiFi-Phy* class allowing to simulate the physical layer of WiFi on ns-3. Indeed, as a jamming attack relies on the vulnerabilities of the physical layer, the jammer must directly interact with the latter. Furthermore, the basic behavior of the physical layer of WiFi on ns-3 only partially takes into account the effects related to jamming. Therefore, modifications of several parameters are necessary on the physical layer of ns-3 to simulate jamming attacks. These changes have been made in the *Physical Layer Driver* class which inherits the basic functions of the *WiFi-Phy* Consequently, no modifications are needed to the ns-3 WiFi module. This class essentially improves the portability of the module.
- **Jammer Class:** This part is the heart of the module and includes all functions representatives of the behavior of a jammer. Its implementation was designed to be as extensible as possible. Indeed, with an heritage system, it is feasible to create your own jamming strategy by creating a new subClass based on the *Jammer Class*. Therefore, four basic jamming attack subclasses and one smart jamming attack subclass are implemented in this release: *Constant-Jammer* Class *Reactive-Jammer* Class, *Random-Jammer* Class *Eavesdrooping-Jammer* Class and *Smart-Jammer* Class.
- **Jamming Mitigation Class:** This component makes it possible to implement mitigation methods. This part uses the same logic as the Jammer class, i.e it is also based on an abstraction system. Consequently, all mitigation system are imaginable. In this version, one mitigation method has been implemented in a subClass : *Mitigation-channel-hopping* subClass. However, several strategies have been designed. The `IncrementChannelHopping()` and `RandomChannel-Hopping()` functions respectively simulate the behavior of the Sequential and Random channel hopping methods.
- **Wireless Utility Class:** This class is located between the different classes of the module and makes the link between them. Its strategic place makes it possible to calculate the metrics and to provide them easily to other elements.

These classes are interdependent, nevertheless, it is possible to simulate a network with several jammers which does not take into account any mitigation system and vice versa.

4 VALIDATION AND USES CASE

4.1 Network model

The test-bed is composed of an attacker and two legitimate nodes. These two nodes are connected to an access point(AP) with the

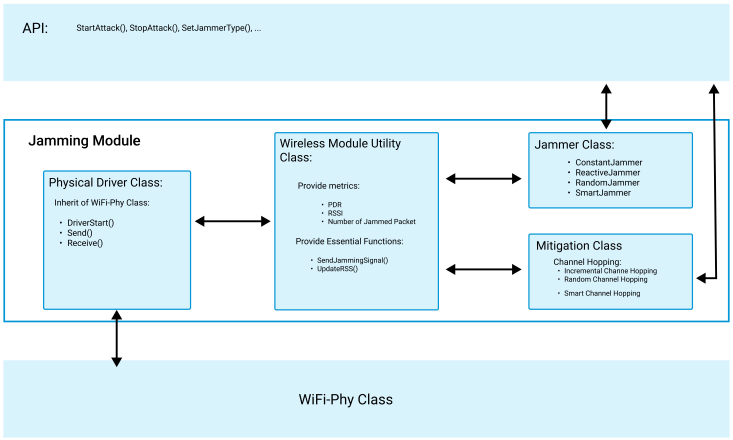

Figure 1: NS-3 Jamming Module Architecture

IEEE 802.11 protocol. On the AP several channel hopping strategies has been implemented such as Smart channel hopping method.

On the side of the simulator, we have implemented the same composition of the network: i.e., two legitimate nodes communicating thanks to an access point and an attacker. The simulations are conducted on a 64-bit Ubuntu distribution and a generic Linux 4.4.0-210 kernel. The central processing unit model is an Intel(R) Core(TM) i7-8650U at 1.90Ghz.

4.2 Evaluation of basic Jamming Attacks

We focus our first evaluation on the performance of simple jamming strategies attacks. The simulation and experimentation are performed in three different conditions a) communication without attack, b) Communication under constant Jamming attack, and c) communication under reactive attack. A constant jamming attack continuously jams a channel and a reactive jamming attacks performs its attack only when a communication is present on the channel.

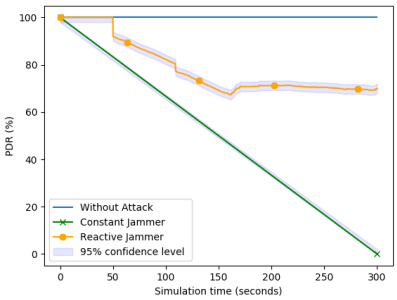

Figure 2: PDR for different type of jamming attacks in network simulates in ns-3

The Fig 2 describes the performance degradation of constant and reactive jamming attack in terms of Packet Delivery Ratio

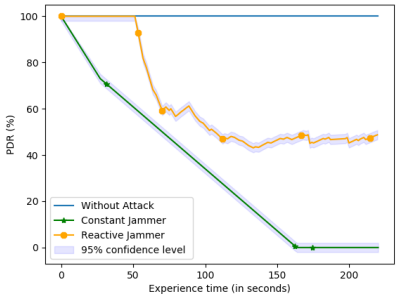

Figure 3: PDR for different type of jamming attacks in a real environment

(PDR) in a simulated network. We see that for a network without attack, the PDR is equal throughout the simulation to 100%. Indeed, the scenario presented is an idealistic scenario without any other disturbance (no additional noise) on the network. Therefore all packets are successfully received. We also observe that the constant attack constantly degrades the PDR and at the end of the simulation the PDR is equal to 0%. The reactive jamming attack has a strong effect at the start of the attack. However after 150 seconds of the simulation, the PDR varies between 60% and 70%. These results are confirmed by experimentation. Indeed, we observe in Fig3, the same behavior for the different attacks in real environment. At the end of the experiment, the PDR for the constant jamming attack is the same as for the simulation environment, i.e 0%. This is due to the fact that the transmitter and the receiver lost the connection a few seconds after the start of the attack. For the reactive attack, after few seconds of the simulation the PDR significantly drops. However, after some time, it increases again to stabilize around 50-60%. For the reactive attack to be successful, the reaction and attack time must be less than the transmission time. However, in these two scenarios, the packet size varies randomly and the transmission

time depends on the packet size. Therefore, the PDR of the reactive attack converges between a threshold in time.

4.3 Evaluation of Smart Channel Hopping Method

The second analysis concerns the evaluation of a smart channel hopping method. To evaluate our module, we implement the same algorithms presented in [10] on the simulator side and on the experiment side. In this paper, the authors implement a channel hopping strategy based on Multi Armed Bandit algorithm with a Thompson Sampling policy. The goal of this algorithm is to converge to the best possible choice in order to maximize the sum of the rewards. The authors prove that their method converges faster to the best channel than the existing algorithms and achieves higher average throughput.

We have adapted this method to the 802.11 protocol with a number of channels equal to 12. In this situation, the access point employed the smart mitigation method and based its reward on the PDR metrics. Indeed, if the PDR is below a certain threshold, the access point can deduce that a problem occurs in the channel. In the same logic, if the access point loses the connection with a certain number of nodes, it can deduce that a possible attack is taking place in the network. Therefore, we based the reward on these two metrics and we set the pdr threshold to 60%. Thereby, the reward is negative if the PDR is less than 60% or if the access point loses connection with at least one node in the network. The jammer also has the ability to change the transmission channel with a frequency hopping method. Indeed, at regular time intervals, the jammer hops to the next communication channel. In this scenario with fixed the interval hopping for the attacker at 1 seconds. Therefore, every 1 second a new channel is jammed and its performance is drastically reduced. Fig 4, demonstrates the accuracy of the smart channel

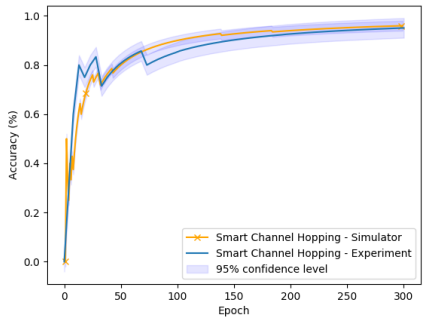

Figure 4: Accuracy of Smart Channel Hopping Model with 12 accessible channels.

methods according to the number of epoch for the experiment and simulation time. Accuracy is calculated as the ratio of the sum of positive rewards to the total number of rewards. We observe that the Multi-Armed Bandit algorithm in both environments converges to 80% after 70 epochs and achieves 93% after 300 epochs. We observe the same behavior of smart attenuation channel hopping when simulated or experimented.

5 CONCLUSION AND FUTURE WORKS

In this paper, we introduced a jamming module for the ns-3 simulator. We have set up a system that is not only as extensible but also includes new methods of mitigation and jammer strategies. Indeed, it is now possible to create smarter attacks based on more advanced algorithms such as reinforcement learning. We prove its scalability by developing an intelligent channel hopping method and a jamming attack based on existing works. In this way, we also demonstrate the implementations of the different metrics. In future work, we will extend this module with additional functionality such with another mitigation method: the attenuation transmit power.

ACKNOWLEDGMENTS

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

REFERENCES

[1] Bhawna Ahuja, Deepak Mishra, and Ranjan Bose. 2020. Optimal Green Hybrid Attacks in Secure IoT. *IEEE Wireless Communications Letters* 9, 4 (2020), 457–460. https://doi.org/10.1109/LWC.2019.2958910

[2] Emilie Bout, Valeria Loscri, and Antoine Gallais. 2021. How Machine Learning changes the nature of cyberattacks on IoT networks: A survey. *IEEE Communications Surveys Tutorials* (2021), 1–1. https://doi.org/10.1109/COMST.2021.3127267

[3] Alejandro Cortés-Leal, Carolina Del-Valle-Soto, Cesar Cardenas, Leonardo J Valdivia, Del Puerto-Flores, and Jose Alberto. 2022. Performance Metric Analysis for a Jamming Detection Mechanism under Collaborative and Cooperative Schemes in Industrial Wireless Sensor Networks. *Sensors* 22, 1 (2022), 178.

[4] Valeria Loscri Emilie Bout. 2022. *Jamming Module Wifi.* Inria. Retrieved February 2, 2022 from https://github.com/JammingWiFiNs3/JammingWifiModule

[5] Valeria Loscri Emilie Bout. 2022. *Website documentation.* Inria. Retrieved February 2, 2022 from https://ns3-jamming-documentation.herokuapp.com/

[6] Kanika Grover, Alvin Lim, and Qing Yang. 2014. Jamming and anti–jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing* 17, 4 (2014), 197–215. https://doi.org/10.1504/IJAHUC.2014.066419

[7] NS-3 Organization. 2012. *Wireless Jamming model.* NS-3. Retrieved February 2, 2022 from ttps://www.nsnam.org/wiki/Wireless_jamming_model

[8] NS-3 Organization. 2022. *NS-3 home page.* NS-3. Retrieved February 2, 2022 from https://www.nsnam.org/

[9] Hossein Pirayesh and Huacheng Zeng. 2021. Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey. arXiv:2101.00292 [cs.CR]

[10] Viktor Toldov, Laurent Clavier, Valeria Loscrí, and Nathalie Mitton. 2016. A Thompson Sampling approach to channel exploration-exploitation problem in multihop cognitive radio networks. In *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 1–6.

[11] Chen Zhong, Feng Wang, M. Cenk Gursoy, and Senem Velipasalar. 2020. Adversarial Jamming Attacks on Deep Reinforcement Learning Based Dynamic Multichannel Access. *2020 IEEE Wireless Communications and Networking Conference (WCNC)* (2020), 1–6.