Evolution of IoT Security: the era of smart attacks

Emilie Bout, Valeria Loscrì, Antoine Gallais

Evolution of IoT Security: the era of smart attacks

Emilie Bout, Valeria Loscri and Antoine Gallais

Index Terms—**Smart attacks, IoT Networks, Machine Learning, Energy-Effective.**

***Abstract*—Internet of things (IoT) devices have become the new privileged targets for cyberattackers these recent years. This is in part due to the amount of sensitive data they provide. In parallel, the security systems are becoming more and more robust with the help of Machine Learning (ML) algorithms. However, this advance can also benefit malicious people. In recent years, ML-based smart attacks have emerged and are significantly changing the threat landscape. This paper focuses on the point of view of the attacker. We have designed a new attack framework based on Markov chain theory. The goal of this latter is to maximize the success probability of attacks while minimizing energy consumption. We tested this framework on both passive and active jamming attacks, thus exhibiting the effectiveness of our approach when compared against basic eavesdropping and jamming attacks. We show that this new type of attack can cut by half the energy consumption of an eavesdropping attack, while maintaining an 88% attack efficiency.**

I. Introduction

The security of internet of things (IoT) networks has become a critical issue in recent years. Indeed, these daily objects provide sensitive and confidential information which represent ideal targets for attackers. In addition, this type of device plays an important and vital role in some areas (e.g., insulin pumps in a health monitoring system). Moreover, according to Cisco, in 2030, more than 500 billion connected objects should be present in the world [1]. Consequently, ensuring the security of these devices has become essential and new robust solutions have started to appear in recent years. Among these solutions, we can find those based on Machine Learning (ML) algorithms. These have made it possible to create more robust, reactive and autonomous defense methods. Indeed, it is possible to use ML algorithms to automate repetitive tasks as well as to improve human analysis.

Hence, attacks must face increasingly robust defense solutions and must also evolve. A new category of attack based on recent technological advances is emerging. This new type of attack, called "smart attacks" allows to circumvent the countermeasures by being more reactive, and less dependent of human actor. Moreover, a smart attack has the capacity to converge as quickly as possible to the optimal solution. Unthinkable a few years ago, these smart attacks are changing the attack landscape and becoming a serious threats. Based primarily on game Theory, Markov Chain theory and ML algorithms, these new attacks are improvements to existing attacks. However, these approaches have also made it possible to create attacks previously unattainable due to their high data demand or excessive manual processing time. Consequently, it becomes urgent to study this new type of attacks, in order to better understand and counter them.

This work was partially supported by a grant from CPER DATA and by the General Armament Direction, France and the Defense Innovation Agency, France

This article takes the point of view of an attacker and focuses on the creation of a smart attack on IoT networks. In particular, we have developed a framework based on a Markov Chain approach, where the attacker moves among four different states: Idle, Receiving, Transmitting and Sleep. The main objective of the attacker is to implement an attack by maximizing the effectiveness and minimizing the associated cost. The framework can be adapted for different types of attacks, both passive and active. The process allows the attacker node to achieve the following objective: maximize its efficiency while minimizing the energy expenditure. In section II we give a brief overview of smart attacks on IoT networks and the different technologies available in the literature to design them. After this analysis, we introduce a new framework of smart attack and derive it for different types of attacks in section III. We demonstrate the effectiveness of this new smart attack in terms of success rate and energy consumption in section IV. Finally, we conclude the paper and provide some future research directions in section V.

II. Smart Attack in the literature

Due to the development of intelligent detection solutions and the resistance of new protocols against conventional attacks, assailants are forced to design more effective attacks, i.e., smart attacks. These attacks have the ability to satisfy several criteria (not necessarily all of them), described below:

- **Targeted:** A sophisticated attack is designed to target one or more well-defined victims. For example, the attacker focuses on a specific type of IoT device or precise communication protocol. This type of attack is not deployed in an arbitrary location but is defined in advance. They are generally created to evade traditional security defenses and frequently employ advanced techniques.
- **Inconspicuous:** attackers must be able to have long-term access to victims in order to perform actions at specific times. In particular, they have to develop sophisticated approaches for escaping the vigilance of the defense systems as long as possible, by developing sophisticated strategies.
- **Flexible:** An effective attack must be able to adapt to a defense scenario. Indeed, even if the attack has been detected and a defensive reaction takes place, the attacker has the possibility of bypassing it by adapting its strategy. Moreover, an elaborate attack can also adjust its approach depending on network parameters such as the number of nodes or transmission frequency.
- **Autonomous:** An attack should be as autonomous as possible and require little interaction with its creators.

The main goal is to avoid human error and thus decrease the chances of being detected.

- **Frugal:** In the IoT context, energy and computational resources are limited. Therefore, a realistic attack should consume as few resources as possible in order to last over time.
- **Complex:** An optimal attack has the potential to exploit multiple vulnerabilities at the same time using complex algorithms. For example, a developed attack, based on its own analysis, can choose the type of attack to execute at a precise moment.

One of the most significant challenges in creating smart attacks is satisfying all of the characteristics listed above. For example, designing attacks that consume little energy while having remarkable efficiency is an open problem in the literature. Nevertheless, a smart attack must not lose sight of its primary aim, which is its effectiveness. Therefore, an intelligent attack must try to maximize its efficiency while trying to satisfy most of the criteria. In the literature, we have identified three main approaches that allow creating smart attacks.

One of the oldest is the use of theoretical games, where the attacker models the interactions between itself and its victim. Both agents (attacker and defender) aim to achieve their optimal strategies by choosing their own actions, in order to maximize their reward. Several works have been carried out in this direction recently [2], especially on jamming and spoofing attacks. In this article, the defender aims to thwart the jamming attack by distributing its power among the sub-carries, while the jammer aims to disrupt the system by allocating its jamming power to different frequency bands. The authors resolve this theory game with a Nash equilibrium and the Blotto game. For an attacker, the main advantage of using this method is that it allows to react to a defense method, thus being as flexible as possible. Therefore, the attacker reduces the probability of being detected while maintaining maximum efficiency.

The second approach is the use of Markov Chain theory. Indeed, this performance model can be employed to monitor the behavior of an IoT device and realize probabilistic predictions about its actions. In [3], authors present a malware attack based on Markov Chain theory. The model reproduces an epidemic model and represents the different possible states of a node: infected, dead, recovered and susceptible. Based on these states, the attacker attempts to determine which nodes to infect, while minimizing its probability of being detected and its power consumption. Therefore, Markov Chain theory allows the attacker to deduce information about its victim and thus choose the opportune moment to attack. This technique essentially improves the discretion and the autonomy of an attack without reducing its effectiveness.

In parallel, ML-based smart attacks have emerged, to drastically change the threat landscape [4]. Thanks to tools allowing the rapid creation of ML algorithms, this technology has become accessible to all. Indeed, a malicious person can easily design an ML-based attack with little knowledge, thanks to free and open-source frameworks such as Tensorflow or OpenAi-Gym [5], [6]. In general, the use of ML algorithms in attack design can be applied for four main reasons: data analysis, behavior analysis, data production and behavior diversion. Many attacks are based on deductions from data collected upstream. This is the case for privacy attacks where the attacker deduces information from data obtained on IoT devices. In [7], authors prove that it is possible to deduce the type of IoT device and its activity thanks to a classification algorithm. They tested their approaches with 81 IoT devices deployed on two different continents and protected by a virtual private network (VPN). Following the same idea, other works ([8], [9]) are also focused on deducing the type and activity of IoT devices. One of the other goals of using machine learning algorithms for attackers, is to infer the behavior of their victims. Indeed, many attacks can only be effective if they use the same configurations as their victim (e.g., same communication protocol, same frequency). In a traditional attack, if an attacker ignores the parameters of the targeted IoT network, it will begin its attack with an approach phase which consists of randomly testing several parameters until an optimal configuration is reached. In [10], the authors design a jamming attack called "Jamming-Bandit" where the goal is to find the optimal attack strategy while considering a reasonable computational complexity. With reinforcement learning algorithms, the search for the optimal strategy can be automated and performed faster, which limits the likelihood of being detected.

Additionally, in IoT networks, many attacks rely on the creation or tampering of data that devices transmit to each other. One example of this type of attack is false injection data attack. An attacker attempts to generate data similar to those originated from IoT devices in order to disrupt the entire network behavior. Designing data corresponding to existing data but resulting on a different outcome for an attacker is a very complex task. Therefore, ML algorithms allowing to generate data (e.g., Generative Algorithm Network - GAN) can prove useful in this process. In [11], authors demonstrate that GAN can allow to generate similar data and intentionally deceive the system with a false injection attack. The final motivation for using ML algorithms when creating an attack is that they can be used to modify the behavior of an IoT network. More and more IoT communication protocols and security solutions are also beginning to use ML algorithms. However, the latter have become new attack vectors for attackers. Lately, a new type of attack, the adversarial attack, has emerged and targets ML algorithms. This new type of attack attempts to modify the behavior of ML algorithms and most of them are themselves based on this type of algorithms. This point is demonstrated in [12], where authors use a Q-learning algorithm to create an adversarial attack on system detection.

Most of these three approaches have flaws and qualities. Attacks based on theoretical games make it possible to respond effectively to a defense strategy. However, this implies that the victim is static and has a well-defined scope of action in advance, that the attacker also knows. Markov Chain theory makes it possible to problematically predict the state of the victim, at a given time. The attack can therefore become more autonomous and be triggered at an appropriate period.

ML Paradigms	Examples of ML algorithms	Type of Attacks	Main application
Supervised	• Decision Tree Learning • Random Forest • K-nearest neighbors algorithm • Extra-Tree	• Cryptanalysis Attacks • Side Channel Attacks • Traffic Analysis Attack • Social Network Attack	Data Analysis
Unsupervised	• K-means • Generative Algorithm Network	• Replay Attacks • False Injection Attacks • Evasion Attack • Exploratory Attack	Data Production and Behavior Diversion
Reinforcement learning	• Multi-Armed-Bandit • Temporal-Learning • Q-Learning	• Cloning Attacks • Sybil Attacks • Jamming Attack • Spoofing Attack	Behavior Analysis

TABLE I: Machine Learning algorithms exploited for generating smart attacks.

However, this technique requires the knowledge of the basic functioning of the IoT device, as well as the protocol used. Eventually, ML algorithms can improve many types of classic attacks, as mentioned in table I, but also be the origin of new attacks that were previously unfeasible, due to e.g., resource constraints. One of the largest black spots in this type of creation, may be the high data demand required for the attack conception. A second could be the consumption of resources (energy and computing) needed to run certain algorithms on restricted devices. In the following section, we explain the implementation of a framework to generate multiple smart attacks.

III. A Smart Attack based on Markov Chain Theory

Many attacks rely on the interception of a packet at a precise moment in order to visualize the information it contains or to modify it. It is the case for eavesdropping attacks whose objective is to record the most packets in order to deduce information about the users. In a jamming attack, being able to predict when the packet will be present on a communication channel, is also important in order to successfully corrupt it. Nevertheless, most of these attacks consume a lot of energy as the attacker must remain active for the duration of the attack.

Based on these facts, we have developed a framework that allows an attacker to predict the opportune moment of attack while minimizing its energy consumption. Consequently, the purpose of this framework is to anticipate when a packet is in transit on the communication channel in order to perform the attack. Therefore, we try to respond as much as possible to the characteristics of an intelligent attack. Indeed, this new type of attack aims to remain as discrete and autonomous as possible by being triggered at the optimal time. In addition, our attack is frugal because our model is based on an attacker's energy consumption reduced as much as possible. Finally, it is a framework that can be derived for different types of attacks, thus also addressing the complexity matter.

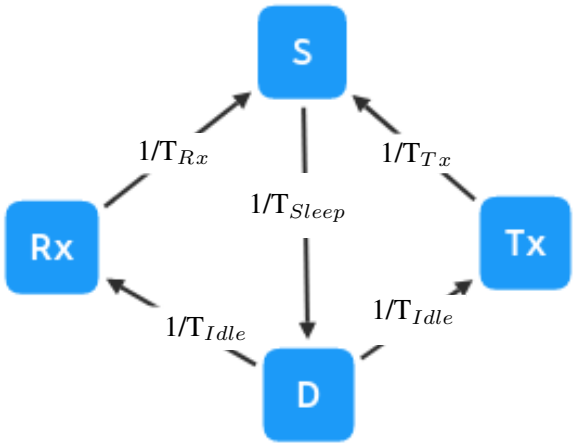
A. Model

In [13], [14], a neighbor discovery process based on the alternating/switching states of the wireless interface is developed. Based on these works, we derive a similar theoretical framework specific for modeling the process of several types of attack. Several communication protocols use power saving modes (e.g., WiFi, Bluetooth). Consequently, a node possesses four operating modes which are:

- **Transmitting(T_x):** The node emits one or more packets during a specific time.
- **Receiving(R_x):** The device is listening: it receives the packets or evaluates the performance of the network (e.g., the occupation of the channel)
- **Idle(D):** The node is inactive, it does not receive or transmit information. This mode consumes less energy than the previous two.
- **Sleep(S):** The communicating object switches to this state to reduce power consumption. The amount of energy consumed associated with this state is often considered to be zero.

On the basis of these states and the theory of Markov chains, it is possible to represent the transition state of an attacker node and of a victim node, respectively named Attacker Node Model (ANM) and Victim Node Model (VNM). Indeed, even though the goals of an attacker and a victim are different, they possess the same state transition process. Fig. 1(a) represents a generic modeling of the ANM and the VNM with the respective probability of passing from one macro state to another. T_{mode} represents the average time spent by the node in each respective state. For a jamming attack, the attacker will try to be in transmitting state at the same time as the victim. For the eavesdropping attack, the attacker will try to be listening when the transmitter will transmit in order to acquire as much data as possible with the minimum impact in terms of energy cost.

As already outlined, the success of an attack depends on the interaction between the victim and the attacker. Hence, the process of an attacker, called Interaction Attacker Victim Model (IAVM) corresponds to the interaction between the two models ANM and VNM. By considering that the attacker and the victim alternate between the four different states, we can represent the interaction between them at a specific time, as shown in Fig. 1(b). In the case of an active attack, the attacker



((a)) Markov Chain of the power saving process of a node

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_i
Attacker	R$_x$	S	D	T$_x$	S	D	R$_x$	...
Victim	T$_x$	S	D	T$_x$	S	D	T$_x$	...
IATM								...

Passive Attack
Active Attack

((b)) Example of the merge process for the attacker node and the victim node

Fig. 1: Attacking Process Model.

and the victim have to be in the Transmit state (T_x) at the same time. In Fig. 1(b), the slot in the IAVM process marked as red(s_4) corresponds to a time slot where the attack has a high success probability. With the same reasoning, the time slots in green(s_1, s_7) correspond to the times when a passive attack could be successful. Indeed, in passive attacks, the IAVM process is feasible when the attacker is in the listening state (R_x) while the victim is in transmission mode (T_x).

Consequently, IAVM is the result of the merger of the two independent models which corresponds to the Cartesian product of the ANM and VNM spaces. The state space of the IAVM process is given by Table II.

$RX_1 - RX_2$	$RX_1 - Tx_2$	$RX_1 - D_2$	$RX_1 - S_2$
$TX_1 - RX_2$	$TX_1 - Tx_2$	$TX_1 - D_2$	$TX_1 - S_2$
$Idle_1 - RX_2$	$D_1 - Tx_2$	$D_1 - D_2$	$D_1 - S_2$
$S_1 - RX_2$	$S_1 - Tx_2$	$S_1 - D_2$	$S_1 - S_2$

TABLE II: Different states for the merging process.

Based on this reasoning, we can represent the probability that the attack process at the time t is $[S_1, S_2]$ can be computed as the Cartesian product of the steady states of each process.

B. Application of this model

We derived this framework to maximize the attack probability in a certain interval time $[0, t]$, with an energy consumption lower than a certain threshold, meaning $cost \leq c$. We define a cycle time as the period between two sleep states of the interfering node. We can calculate the probability that the attacker operates into each state. The probability of each state corresponds to the time spent in that state over the duration of a cycle. For example, the probability that the attacker is in the sleep state corresponds to the ratio between the time spent in the sleep state to the duration of the cycle. Moreover, the time of one cycle corresponds to the sum of the time spent by the attacker in each state.

The cost depends on the percentage of time that a node spends in each of the four states considered above (TX, RX, Idle and Sleep). In addition, each operating state has its own energy consumption that can be found in the characteristics of a network interface controller card. Therefore, the total energy consumption of a state corresponds to the product between its energy consumption and the time spent in that state. Hence, the total cost is the sum of each energy consumption for the four operating states. Combining the calculation of the energy cost and the framework explained above allows to maximize the attack probability with a limited cost c.

IV. Case studies

A. Description of the test-bed

We evaluated our framework with two different types of attack: a passive eavesdropping attack and an active jamming attack. The results were obtained from a test-bed composed of two legitimate nodes and an attacker, as represented in Fig. 2.

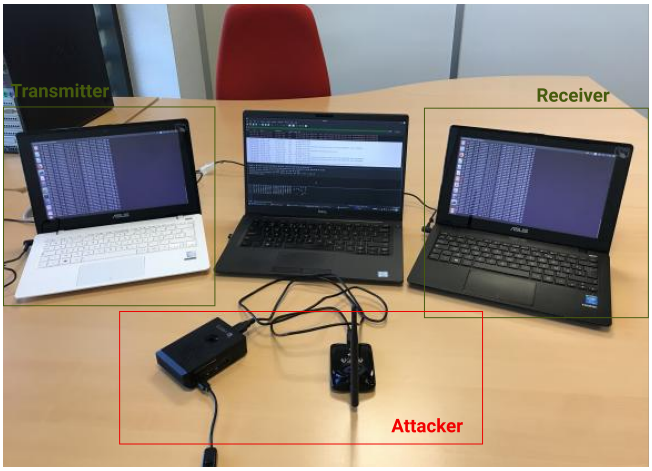


Fig. 2: Test-bed implementation.

The framework is implemented in a Raspberry-Pi equipped with an *Alfa AWUS036h* device. We have chosen this type of instrument to directly modify the MAC layer parameters. Indeed, this device provides a Realtek RTL8187L including the wireless chip `ath9k`. Their driver and firmware are open-source and it is easily extensible, while including the different states of energy consumption. Therefore, each state has a different energy consumption [15]. The transmitter and the receiver are two identical laptops with the same type of network card. These two nodes communicate with the IEEE 802.11 protocol and an access point allows these two nodes to stay connected to each other. As the distance between the elements of the network plays an important role in the transmission time of a packet, this element remains fixed throughout the simulation. In addition, for this type of experiment, we set the distance between all network elements at 1 meter to have a 100% transmission success rate without attack, thus avoiding the evaluation of false positives afterward. Moreover, as the transmission time also depends on the size of the packets, we vary this parameter during the simulation. The transmitter sends packets of random size between 50 and 1400 bytes. The duration of the two experiments below is fixed at 4 minutes.

B. Passive attack: Eavesdropping attack

First of all, we implemented this framework for passive attack (eavesdropping). The goal for the attacker is to record the maximum of packets without intervening on the network. Therefore, the attacker must be in R_x mode while the transmitter is in T_x mode. Based on the framework described above, the attacker can measure its temporal probability of being in each state in order to maximize the attack's success while minimizing the energy cost.

The framework is based on a compromise between the energy spent by the attacker and its efficiency. After several experiments by varying the energy cost c and maximizing the success probability, we found that the optimal solution is reached with an energy cost equal to 0.5. Indeed, with $c = 0.5$, the probability that the attack will be a success is 76%. By decreasing the energy cost, for example to 0.38, the maximum success for the attack is 60%. We conclude that 76% is the maximum that we can achieve with the specific characteristics of the network card used in our experiments. For other values, the conditions are not satisfied to solve the problem of minimization. Based on the Markov Chain theory, the smart attack computes the probability of each state according to the associated cost. Therefore the values obtained for each state are $PR_x = 0.49$, $PT_x = 0.0025$, $P_{SLEEP} = 0.49$ and $P_{IDLE} = 0.01$. In order to compare those results with the smart attack, we also implemented a classic eavesdropping attack on the test-bed. The first criterion that we evaluated is the frugality of the attack. As mentioned previously, the total energy consumption is the sum of the energy consumption for each state depending on the percentage of time. Fig. 3 shows the energy consumption from the attacker's point of view after four minutes of activity. We can notice that the smart attack consumes two times less energy than the basic eavesdropping attack. Indeed, the energy consumption for the eavesdropping attack is 81.6 Joules against 39.98 Joules for the smart attack.

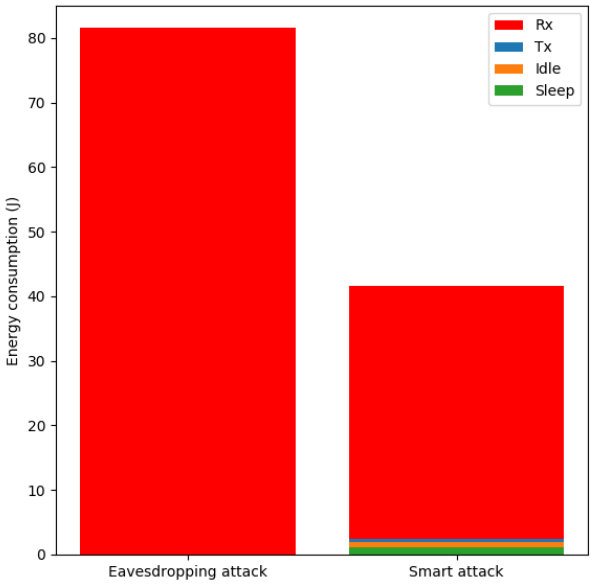


Fig. 3: Comparison of energy consumption between eavesdropping and smart attacks.

The second point evaluated is the impact of the attack. The effectiveness of passive attack can correspond to the ratio of total packets recorded to the total of packets sent. The basic eavesdropping attacks record the packets broadcasted

on the network, which here corresponds to 200 packets. Thereby, this type of attack is 100% effective. The smart attack listens on average 176 packets for an attack of the same duration. Consequently, if we merge this point with the energy expenditure, the smart attack has a success rate of 88% but consumes 50% less energy than the basic attack.

Although this is a passive attack that does not influence network performance, this type of attack can be extremely useful. Indeed, it can be the basis of several other attacks such as the traffic fingerprint attack. The latter is based on analyzing the data in order to recognize a pattern from the packets. With this attack, a malicious person can identify with a high probability several private information such as the habits of a user. Furthermore, with the advent of Machine Learning-based attacks, there is an increasing need for attackers to recover as much data as possible in a short period of time. At the same time, security systems increasingly rely on ML solutions and the need for data is also a significant issue in this area. Consequently, this framework can be of significant help in saving energy without reducing performance from an attacker or defense perspective.

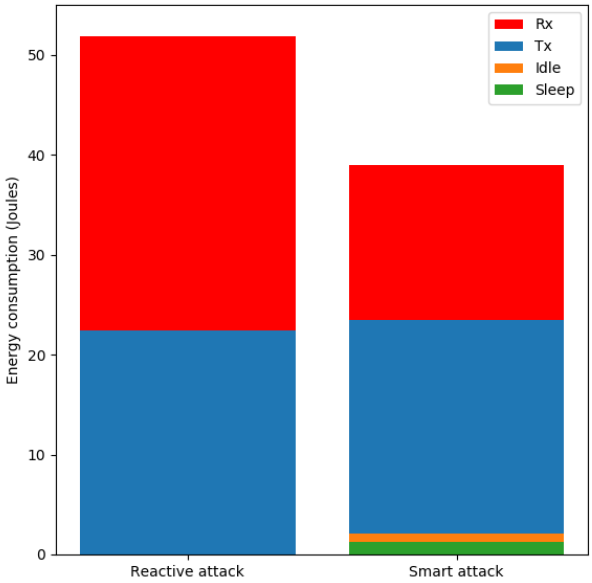


Fig. 4: Comparison of energy consumption between reactive and smart attack.

C. Active attack: Jamming attack

Previously, we demonstrated the performance of the framework used during a passive attack. In this section, we employ it to enhance an active attack: a reactive jamming attack. The aim of this type of attack consists of intentionally interfering with the communication medium to corrupt a transmission (a packet). Consequently, the attacker is by default in listening mode (R_x) and when the communication is present on the medium, it switches to transmission mode (T_x) in order to jam the latter.

In this case for the attack to succeed, the attacker must be in transmit mode (T_x) at the same time as the transmitter. As with the passive attack, the attacker computes the probability of each state in order to maximize the success of the attack while minimizing its energy consumption. If we base ourselves on the same energy cost as the passive attack, the maximal cost of the energy consumption is fixed to 0.5. In this situation, the values of the probabilities for each state is: $PR_x = 0.005$, $PT_x = 0.74$, $P_{SLEEP} = 0.25$ and $P_{IDLE} = 0.01$.

In the same way, as for the passive attack, we have evaluated the energy consumption of the attacker. As demonstrated in Fig. 4, the energy consumption for the smart attack is lower than for the reactive attack. Indeed, the basic reactive attack consumes 51.85 Joules against 39 Joules for the smart attack.

In order to evaluate the effectiveness of the attack, we calculated the Packet Error Rate (PER), which is the number of packets received with error divided by the total number of packets received. In this situation, the reactive attack has an average PER of 9.5% versus 20% for the smart attack. Indeed, the effectiveness of a reactive jamming attack depends essentially on the size of the transmitted packets. Therefore, in the case of small packet size, the reactive attack does not have time to jam the packet. The attacker identifies the packet and moves in transmission mode. Yet, during this change, the packet is already transmitted and the jammer sends a signal on an unoccupied channel. Consequently, the reactive jammer is not efficient to corrupt small packets. Smart jammer problematically determines when the packet will be in transit. This way there are more chances of jamming a packet even if it is small in size. An active attack is more likely to be detected because it directly disrupts the behavior of its victim. This is why we have also compared our attack and the basic reactive attack against a detection mechanism. A statistical detection method was implemented in the test-bed. On the basis of a network, we can determine the average of the packet delivery ratio (PDR) and hence define a detection threshold. PDR is equal to the ratio of the total number of successfully received packets to the total number of sent packets. Hence, if the PDR decreases below the detection threshold, an attack is identified. In this experiment, we defined a detection threshold at 70%. The smart attack is detected 5.67 seconds later compared to a reactive attack.

We have shown that the use of the framework can improve the performance of a jamming attack while reducing its energy consumption. However, this use case can be very useful from a defense perspective. Indeed, jamming attacks can be used against illegal communications such as surveillance of protected areas by a drone. In this situation, having a defense jammer that consumes less power while having high performance can be beneficial. We tested our framework with a jamming attack but it can be applied to other types of active attacks that need to intercept a packet in transit. For example, the black-hole attack of intercepting a packet and dropping it could be improved with this type of framework.

V. Conclusion and future work

This article explains the main advantages of using advanced processes in creating attacks such as Game theory, Markov Chain theory, and ML algorithms. Indeed, these new approaches can allow the attacks to satisfy the various criteria of an intelligent attack. The threat landscape is evolving, it is urgent to study these new attacks in order to better circumvent them. In this direction, we have implemented a framework that can adapt to several types of attacks in a real test-bed. This framework based on a Markov Chain theory aims to improve the efficiency of the attack while minimizing its energy consumption. In this article, we have proven its effectiveness with two types of attacks: passive and active. Our approach halves the energy expenditure of an eavesdropping attack while having a similar success rate. Moreover, for the smart jamming attack, we have demonstrated that this latter allows jamming more packets while having a low power consumption compared to a basic reactive jamming attack. Indeed, its energy consumption is reduced by 24% and its impact on the network increased by 10.5%. In this paper, we experiment our new model with the 802.11 protocol. However, the derived framework is general and can be applied to different wireless protocols which include the four operating states.

In future works, we plan to implement this Markov Chain theory in a reinforcement learning algorithm. One of the objectives will be to make the process more autonomous by choosing the characteristics of the framework such as the maximum energy cost. In addition, it might be interesting to assess the impact of this smart attack over a large network.

References

[1] Cisco, "Internet-of-things cisco," 2016 [Online], last accessed 15 November 2021. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf

[2] N. Namvar, W. Saad, N. Bahadori, and B. Kelley, "Jamming in the internet of things: A game-theoretic perspective," in *2016 IEEE Global Communications Conference (GLOBECOM)*, 2016, pp. 1–6.

[3] M. H. R. Khouzani and S. Sarkar, "Maximum damage battery depletion attack in mobile sensor networks," *IEEE Transactions on Automatic Control*, vol. 56, no. 10, pp. 2358–2368, 2011.

[4] E. Bout, V. Loscri, and A. Gallais, "How machine learning changes the nature of cyberattacks on iot networks: A survey," *Communications Surveys and Tutorials, IEEE Communications Society*, 2021.

[5] Tensorflow, "Main page of tensorflow framework," 2021 [Online], last accessed 15 November 2021. [Online]. Available: https://www.tensorflow.org

[6] OpenAiGym, "Main page of openai-gym framework," 2021 [Online], last accessed 05 January 2021. [Online]. Available: https://gym.openai.com/

[7] J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, and H. Haddadi, "Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach," in *Proceedings of the Internet Measurement Conference*, 2019, pp. 267–279.

[8] A. Acar, H. Fereidooni, T. Abera, A. K. Sikder, M. Miettinen, H. Aksu, M. Conti, A.-R. Sadeghi, and S. Uluagac, "Peek-a-boo: I see your smart home activities, even encrypted!" in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020, pp. 207–218.

[9] R. Trimananda, J. Varmarken, A. Markopoulou, and B. Demsky, "Ping-pong: Packet-level signatures for smart home device events," *arXiv preprint arXiv:1907.11797*, 2019.

[10] S. Amuru, C. Tekin, M. van der Schaar, and R. M. Buehrer, "Jamming bandits—a novel learning method for optimal jamming," *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 2792–2808, 2015.

[11] S. Ahmadian, H. Malki, and Z. Han, "Cyber attacks on smart energy grids using generative adverserial networks," in *2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. IEEE, 2018, pp. 942–946.

[12] D. Wu, B. Fang, J. Wang, Q. Liu, and X. Cui, "Evading machine learning botnet detection models via deep reinforcement learning," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6.

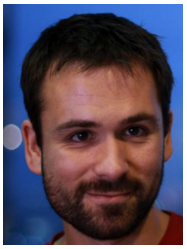
[13] L. Galluccio, G. Morabito, and S. Palazzo, "Analytical evaluation of a tradeoff between energy efficiency and responsiveness of neighbor discovery in self-organizing ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 7, pp. 1167–1182, 2004.

[14] V. Loscri, "An analytical evaluation of a tradeoff between power efficiency and scheduling updating responsiveness in a tdma paradigm," in *The Fourth International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness & Workshops*, 2007, pp. 1–7.

[15] A. Communications. Single-chip 2x2 mimo mac/bb/radio with pci express interface for 802.11n 2.4 and 5 ghz wlans. [Online]. Available: https://datasheetspdf.com/datasheet/AR9280.html

Emilie Bout received her B.Sc degree and her M.Sc degree in computing sciences from the University Polytechnic des Hauts de France in 2017 and 2019. She is currently working toward a Ph.D in Inria Lille researching Networking and Cybersecurity partially granted by the DGA (General Armament Direction). Her main research interests focus on the creation of "smart" denial-of services attacks in wireless networks and their countermeasures.

Valeria Loscrì is a permanent researcher of the FUN Team at Inria Lille–Nord Europe since Oct. 2013. From Dec. 2006 to Sept. 2013, she was Research Fellow in the TITAN Lab of the University of Calabria, Italy. She received her MSc and PhD degrees in Computer Science in 2003 and 2007, respectively, from the University of Calabria and her HDR in 2018 from Université de Lille. Her research interests focus on emerging technologies for new communication paradigms such as VLC and Tera-Hertz bandwidth and cooperation and coexistence of wireless heterogeneous devices. Since 2019, she is Scientific International Delegate for Inria Lille.



Antoine Gallais is a Full Professor at INSA Hauts-de-France (Université Polytechnique Hauts-de-France), Valenciennes, France. He received M.Sc. (2004) and PhD (2007) degrees in computer science from the University of Lille, France, and was an associate professor at the University of Strasbourg, France, from 2008 to 2019. His main research interests lie in wireless ad hoc and mesh networks, actuator and sensor networks, Industrial Internet of Things, activity scheduling, routing and MAC protocols, mobile networks, fault-tolerance, cybersecurity and performance evaluation. Biography text here.