

Modeling the impact of jamming attacks in the internet of things

Imane Kerrakchou, Sara Chadli, Yassine Ayachi, Mohammed Saber

Laboratory of Smart Information, Communication and Technologies, National School of Applied Sciences, Mohammed First University, Oujda, Morocco

Article Info

Article history:

Received Aug 21, 2021

Revised Mar 7, 2022

Accepted Mar 21, 2022

Keywords:

Internet of things

Jamming attack

MAC Layer

S-MAC

Wireless sensor network

ABSTRACT

Security is a key requirement in the context of the internet of things (IoT). The IoT is connecting many objects together via wireless and wired connections with the goal of allowing ubiquitous interaction, where all components may communicate with others without constraints. The wireless sensor network is one of the most essential elements of IoT concepts. Because of their unattended and radio-shared nature for communication, security is becoming an important issue. Wireless sensor nodes are susceptible to different types of attacks. Such attacks can be carried out in several various ways. One of the most commonly utilized methods is jamming. However, there are also some other attack types that we need to be aware of, such as tampering, and wormhole. In this paper, we have provided an analysis of the layered IoT architecture. A detailed study of different types of jamming attacks, in a wireless sensor network, is presented. The packet loss rate, and energy consumption. are calculated, and the performance analysis of the wireless sensor network (WSN) system is achieved. The protocol chosen to evaluate the performance of the WSN is the sensor-medium access control (S-MAC) protocol. Different simulations are realized to evaluate the performance of a network attacked by the different types of jamming attacks.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Imane Kerrakchou

Laboratory of Smart Information, Communication and Technologies

National School of Applied Sciences, Mohammed First University

Oujda, Morocco

Email: i.kerrakchou@ump.ac.ma

1. INTRODUCTION

Internet of Things is emerging as a crucial element of the digital transition. The Internet's ability to connect anywhere at any time, making life easier for users, has become very popular over the years. Automating everyday tasks is no longer a dream. The internet of things (IoT) has reached new heights, where a myriad of gadgets and applications are connected successfully to the sensors and the Internet, offering a new generation of relief and communication. The Internet of Things can be connected using many heterogeneous technologies of the network [1], such as the wireless sensor networks (WSNs), the wireless local area networks (WLANs), the radio frequency identification (RFID), and the cellular services (3G, 4G, 5G, and 6G). The wireless sensor network is a type of intelligent wireless network consisting of tens or thousands of sensor nodes capable of detecting, communicating, and calculating in a self-organized way. The sensor nodes collect information through their internal sensors. They perform the information collection task autonomously through wireless, low energy, single-hop, or multi-hop transmission and exchange of data between nodes. The wireless sensor network has a high data acquisition capability and can operate in any

situation, at any time, and in any place that makes it helpful in a number of important domains [2] like national defense and military, medical health, traffic management, and environmental monitoring. It is also becoming a hot topic in national and international research nowadays. Wireless sensor networks are dispersed in nature and sensor nodes have resource constraints and are deployed remotely. They are susceptible to many attacks, which causes security issues in data transmission [3]. The jamming attack is one of the most common attacks, which targets the perception layer. It disrupts the communication between sensor nodes and causes them to unfairly consume the resources of the canal, causing serious damage.

The medium access control (MAC) layer is a part of the perception layer that still has an important role in the transmission of data because it has control over the allocation of the resources of the wireless channel. Optimizing MAC protocols is one of the main ways to save energy, and increase the lifetime of the network. Among the existing protocols, we can mention the sensor-medium access control (S-MAC) protocol, which is a modified version of the IEEE 802.11 MAC distributed coordination model and will be used later for this work because of its intrinsic flexibility, its scalability, and its advantage in solving the data fluctuation problem. In the paper, Jagriti and Lobiyal [4] we will implement three types of jamming attack, which target the MAC layer, using the S-MAC protocol, to visualize the impact of this attack on the performance of the network. The rest of this paper is structured as follows. Section 2 presents an overview of IoT security, classification of attacks by layer, a definition of the S-MAC protocol, and a summary of some reviews on the jamming attack. Section 3 presents the proposed system, the implementation of the jamming attack, and the results obtained. Section 4 concludes the paper with a summary of the jamming attack.

2. RELATED WORKS

2.1. IoT security

In the IoT, the information that is generated by those omnipresent devices is stored either on the devices themselves (e.g., smartphones, and servers), which is often known as data in repose, or it is transferred through networks like the Internet, which is otherwise known as data in transit. By nature, IoT is open, because devices normally operate in the air and are capable of communicating through public networks. Therefore, in order to secure data in repose and in transit, confidentiality, availability, and integrity, must be assured to guarantee the privacy and the security of the IoT [5]. All security controls, protections, and mechanisms are deployed to achieve one or all of these types of protection. In the following text, we examine in detail the different requirements of security in the IoT.

- Confidentiality: the confidentiality of data guarantees that only permitted entities can access the data and stop unauthorized entities from invading it [6].
- Availability: it guarantees the survival of IoT systems to approved parties where required during attacks. It also guarantees that it is capable of delivering a minimum quality of services in the case of failures or power loss.
- Authorization: it guarantees that only users and permitted devices have access to resources or network services.
- Integrity: data may be manipulated or changed by the attacker, during processing and storage on the devices. Therefore, it is important to ensure that data is precise, coherent, and secure throughout its entire life cycle [7].
- Privacy: An individual user's identity must be protected by the secured IoT system to preserve privacy.
- Authentication: it requires an IoT system to guarantee the identity of the peer it is communicating with. (E.g. The recipient checks whether or not the data received came from the correct source).
- Non-repudiation: it involves the ownership of data by guaranteeing that no one could deny their authenticity. That is to say, it is not possible for the sender to deny the data he has sent and for the recipient to deny the data he has got.

2.2. Attacks on IoT

The system of IoT, due to its dynamic and distributed nature, provides weak channels of communication that are utilized by malicious objects to open and exploit novel threats concerning the tracking, surveillance, and reporting of the actions of users. The increase in the number of devices of the IoT in our community had presented a variety of security attacks that must be addressed. There are three principal attack types based on the basic architecture of the IoT system: physical, network, and application attacks. This section gives a brief description of each layer and the different types of attacks that threaten each layer. The different attacks against the security of IoT systems are summarized in Figure 1.

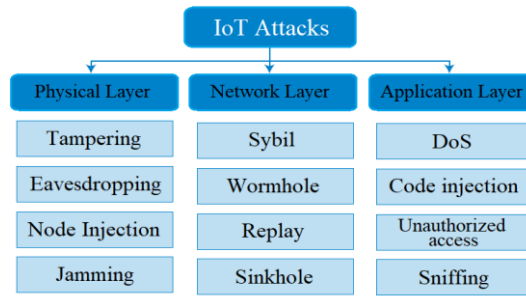


Figure 1. Layered classification of IoT attacks

2.2.1. Physical layer attacks

The physical layer processes data collected from conditions and physical events. This data collection is done using the sensors and the actuators that detect changes in the environment and make the measurements. This layer typically handles data collection and processing using different technologies such as WSN, RFID, global positioning system (GPS), and RFID sensor network (RSN). Among the most known attacks on the physical layer [8], we find the following:

- Tampering attack: The attacker can physically access the sensors. He will utilize this method to obtain sensible data, like encryption and decryption codes.
- Eavesdropping attack: In this type of attack, the eavesdropper captures the data transferred to the IoT node from the base station and utilizes it for further attacks. It could be prevented by keeping the IoT node isolated or by utilizing algorithmic cryptography to prevent these attacks [9].
- Fake node injection: A new false node is introduced and is assigned to change the original information and share the incorrect data [10].
- Jamming attack: This is a type of attack that affects the radio frequencies used by nodes in a WSN to communicate. A jamming source can be effective enough to affect the entire system. In fact, an attacker could potentially disrupt the correspondence in the entire system even with the less efficient jamming sources by intentionally carrying the jamming sources [11].

2.2.2. Network layer attacks

The network layer is linked to the provision of access to the network access. The collected data from the physical layer is transferred to the specific system to be processed by this layer. The network layer uses modern technologies and access protocols such as LoWPAN/IPV4/IPV6. Through this layer, objects can connect to other objects, which are the primary aspect of the system of IoT for intelligent event management. After the physical layer, this layer is susceptible to security attacks [12], including:

- Sybil attack: In this attack, the malicious nodes can establish alternate identities in order to fool other nodes. In this situation, the goal of the attacker, with no physical nodes, is to control different areas of the system [13].
- Wormhole attack: This attack occurs when nodes find out information on their neighbors. In this attack, malicious nodes make a tunnel by which they can communicate. The malicious nodes give the wrong impression to the system that the malicious route is the shortest route to the destination. Therefore, most nodes utilize this route and the attacker only observes it [14].
- Replay attack: With this attack, the resource of the sensor is consumed by the repeated retransmission of the data. This attack could be prevented by implementing a timestamp and secure management of the session keys.
- Sinkhole attack: The attacker publishes false routing information in order to attack network traffic. It causes other attacks such as dropping or altering routing information, and selective transfer [15].

2.2.3. Application layer attacks

The application layer includes the applicable section of the entire system, which aims to deliver the service requested from a specified user. This layer uses different protocols, which generally comprise constrained application protocol (CoAP), message queue telemetry transport (MQTT) [16]. The use of these protocols allows the user to be provided with the requested service in an efficient manner. There are various types of attacks that occur at the application layer, such as:

- DoS attack: In this layer, the attacker denies the availability of the application or service for the user through the transmission of a large number of requests. A high level of authentication is required to prevent this type of attack [17].
- Malicious code injection: With this attack, malicious code is injected into the software application and affected the services delivered by the network [18].
- Unauthorized access: In this attack, an unauthorized attacker breaks into the network and blocks authentic users from accessing the system. In addition, the attacker will also remove sensible information and damage the infrastructure of the IoT completely.
- Sniffing attack: Attackers can use different tools of sniffing to survey the traffic flow of the network. Using traffic surveillance, the attackers can also obtain confidential and sensitive information on the users and the network. Using this information, other attacks are also possible on the network [19].

2.3. S-MAC protocol

The perception layer, specifically the MAC layer, has an essential role to play in the proper functioning of the network. One of the fundamental functions of the MAC is to prevent collisions, so nodes located in the same interference zone do not send at the same moment. The two principal functions performed at the medium access layer are the control of when to transmit and when to listen for the packet.

Many different MAC protocols have been developed for wireless sensor networks, including S-MAC, T-MAC, and B-MAC. The S-MAC protocol is a well-known protocol in WSNs [20]. It was designed to meet the energy saving requirement of WSNs. The S-MAC frame T_F is divided into two parts (see Figure 2). A listening period T_L and a sleeping period T_S i.e. $T_F = T_L + T_S$. The listening period allows communication between sensor nodes and other nodes to send and receive control packets T_C . During the sleep period, the nodes turn off their radios to consume less energy. The first part of the listening period (T_{sync}) is the synchronization by transmitting SYNC packets i.e. $T_L = T_{sync} + T_C$. Each node keeps a schedule table that stocks all the schedules (listen and sleep period) of its neighbors and then uses it to send data during the T_D period.

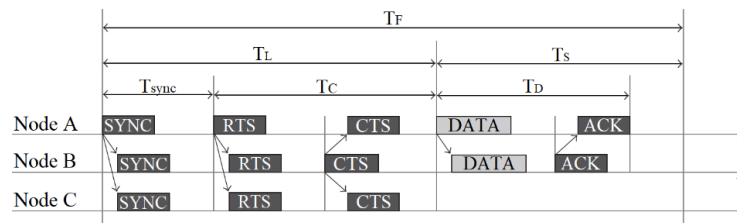


Figure 2. Frame for S-MAC protocol

Once a node begins working, it will listen during a specific period of time. During this period, if it does not receive any schedules from its neighbors, it chooses its proper schedule and begins to follow it. Immediately afterward, the node will broadcast the SYNC packet to notify the schedule. If during this time, the node received a schedule from a neighbor node, it would set its schedule in the same way.

Before the node transmits data to its neighbor in order to organize the data exchange, it sends the request to send (RTS) packet and then waits for the answer from the neighbor. If its neighbor was ready to receive, it transmitted a CTS packet and data transfer could begin immediately. Nodes that aren't participating in any data transfer, switch to sleep state to conserve energy. Once the data transmission is complete, an ACK is sent by the receiver to indicate that the transfer is successfully completed (see Figure 3). It is necessary for each node to maintain its Table of schedules after a set number of the scheduled synchronizations. As a result, each node must listen for a long period of time to discover neighbors that may have a different schedule. This leads to packet overhead and is the drawback of the protocol S-MAC.

2.4. Surveys on IoT

The vast advancement and the commercialization of IoT have brought to light many vulnerabilities in the security of the system IoT. To delve into this topic and provide a detailed overview for researchers, a few studies have been reported that we will review here. In one of these studies, Mosenia and Jha [21] the seven-layer model of CISCO, where they mainly focused on the IoT layer at the edge. In the paper, Yank *et al.* [22], the authors highlighted the problems of security for a four layer of IoT architecture. On another hand, in the paper, Frustaci *et al.* [23] demonstrated the attacks against the system IoT in three layers, which are the application, the transportation, and the perception layers. Then they highlighted crucial security vulnerabilities in the communication and networking protocols utilized in these layers. Similarly, in the

paper, Ayotunde *et al.* [24], provided a taxonomy categorizing the security threats according to the architecture, application, communication, and data. They also demonstrated the security vulnerabilities in various applications like the smart environment, and healthcare. In contrast, in the paper, Khan and Salah [25], discussed security threats in relation to the architecture of IoT deployment.

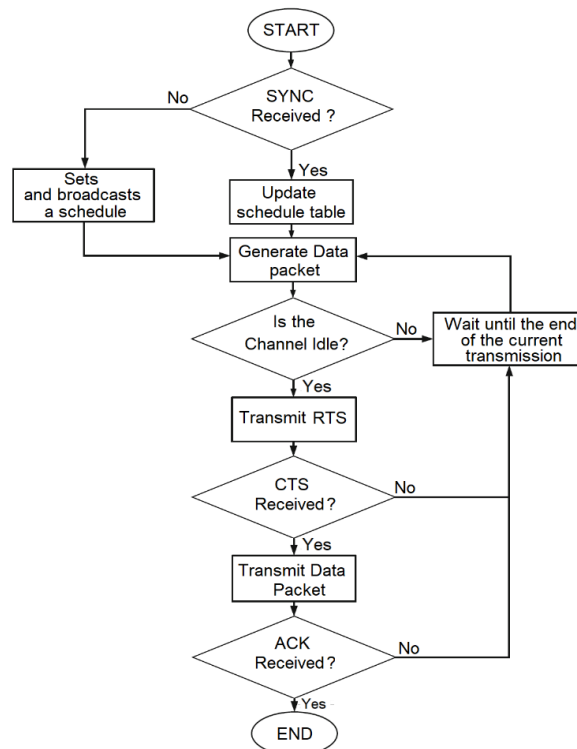


Figure 3. Diagram of S-MAC protocol

3. IMPLEMENTATION OF JAMMING ATTACK ON S-MAC PROTOCOL

3.1. Proposed system

In this paper, we simulate three types of jamming attacks that target the base station. The idea is to visualize the effects of these attacks on the performance of the WSN and determine which attack is the most impactful. Our system consists of a group of nodes and a base station. The nodes are randomly distributed in the network and communicate directly with the base station using single hop communication. The role of the base station is to collect and process packets sent to it by the nodes in the network in a centralized model.

The attack can be launched on any node of the network. However, in our case, we have chosen to target the base station. In the first type of jamming attack, we suppose that the attacker does not know the protocol used in the network. So, once the malicious node is implemented in the system, the attack is launched. The attacker generates large DATA packets, and then transmits them continuously to the base station, saturating the transmission channel. In the second and third types of jamming attack, it is supposed that the attacker knows the protocol used in the network which is, in our case, the S-MAC protocol. The malicious node analyzes the behavior of the network to determine the protocol used, and then it synchronizes with all the nodes to determine the period of activity and the period of inactivity of the network. Finally, the attacker triggers the attack with a high number of large packets by disrupting the transmission channel. For the second type of attack, RTS control packets are used to launch the attack, while for the third type, DATA packets are used. The Figure 4 shows the activity modeling of the jamming attack.

3.2. Simulation setup

The implementation of the three types of jamming attacks is performed using the OMNeT++ simulator which is designed to model and study wireless network protocols. We considered the simulation parameters as shown in Table 1. In this simulation experiment, two scenarios are created that share the same attributes during the simulation, except that the first scenario (see Figure 5) represents a WSN without attack, no attack is implemented in the network. We talk about the normal case.

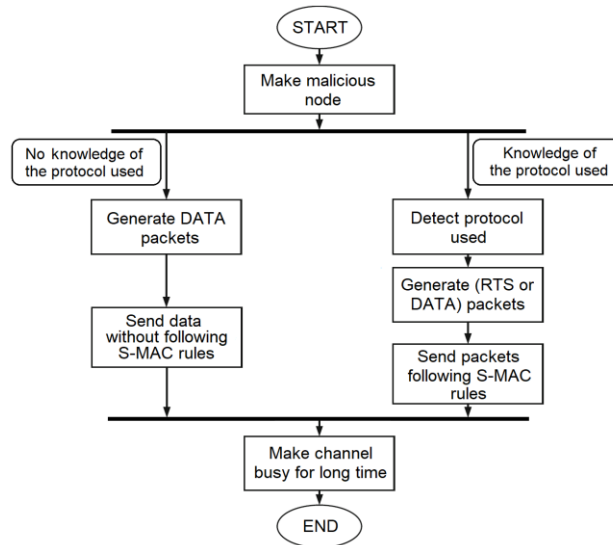


Figure 4. Activity modeling of jamming attack

Table 1. Simulation parameters

Parameters	Values
Simulation Time (s)	700
Simulation Area (m)	80x80
Sink	1
No. of Nodes	29
Mobility Model	No Mobility
Topology	Star
Transmit Power (mW)	36.3
Packet Rate (pps)	4
Data Packet Size (bytes)	100
End Time	End of simulation
Protocol	S-MAC
SYNC Packets Size (bytes)	11
RTS Packets Size (bytes)	13
Contention Period (ms)	10
Frame Time (ms)	610

The second scenario (see Figure 6) represents a WSN under attack by a malicious node. The three types of attacks, explained in section 3.1, are simulated in this scenario under three different conditions:

- WSN with the attack by data packet (DATA), without knowledge of the protocol used in the system (DATA Attack NoKP).
- WSN with the attack by control packet (RTS), with knowledge of the protocol used in the system (RTS Attack KP).
- WSN with the attack by data packet (DATA), with knowledge of the protocol used in the system (DATA Attack KP).

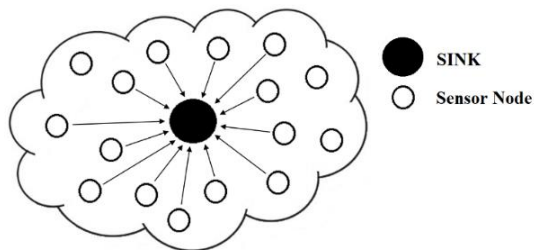


Figure 5. Scenario 1–normal case

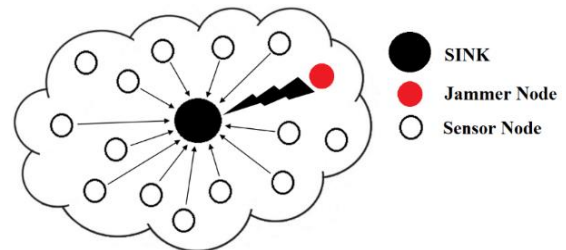


Figure 6. Scenario 2–WSN with jamming attack

This scenario contains a single jammer that injects unauthorized traffic into the network and affects the WSN, which has no specific detection or prevention mechanism against jamming attacks. We used a high data rate, and transmission power that is too high in order to represent the jamming attack. The jammer specifications are shown in detail in Table 2. The main objective of simulating Scenario 1 (normal case) is to identify the state of the network under normal conditions, which will later allow us to compare and differentiate the impact and severity of the three types of jamming attacks on the network.

Table 2. Simulation parameters for jammer node

Parameters	Values
No. of Jammers	1
Trajectory	Fixed
Transmit Power (mW)	57.2
Packet Rate (pps)	60
Protocol	S-MAC
SYNC Packets Size (bytes)	11
RTS Packets Size (bytes)	210
Data Packets Size (bytes)	210
Frame Time (ms)	610
Contention Period (ms)	10
End Time (s)	End of simulation

3.3. Analysis of the results

In order to evaluate the performance of the WSN and analyze the impact of the jamming attack, we need to measure the network performance. The simulation results, for performance measures, such as packet loss rate, the lifetime of the network, and energy consumption, have been illustrated in the following figures. Figure 7 represents the number of data packets sent by all the nodes of the network and the number of data packets received by the base station for the two scenarios. For the first scenario, which represents the normal case, we notice that the number of packets sent is approximately equal to the number of packets received by the sink. Therefore, the network works correctly. For the second scenario, which represents the three types of jamming attack, we notice that the number of packets sent and received is lower compared to the first scenario. The decrease in the number of packets sent by the nodes in the network is due to the continuous sending of a high data rate by the malicious node, which increased the traffic and made the transmission channel busy. This prevented the nodes from sending all their packets to sink.

We can also see that in the case of the attack with knowledge of the protocol used (RTS Attack KP, DATA Attack KP), the number of packets sent is much lower than in the case of no knowledge of the protocol used (DATA Attack NoKP). The knowledge of the protocol used in the network allows the attacker to synchronize with all the nodes and share their wake-up times, thus allowing him to know the right time to launch the attack and, ultimately, have a huge impact on the transmission of packets in the entire system.

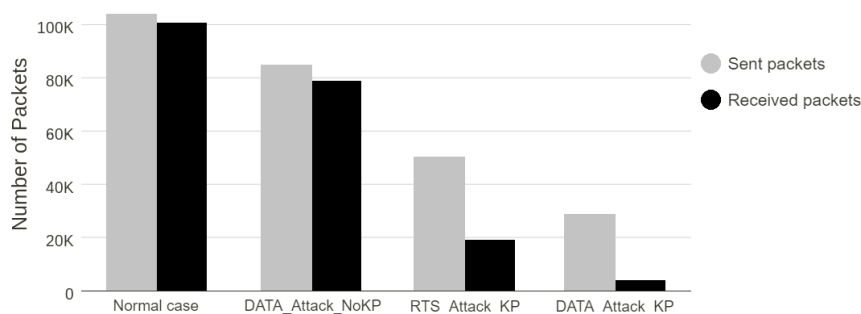


Figure 7. Number of packets sent and received

For the number of packets received, we notice that the base station does not correctly receive the packets sent to it by the nodes in the network, because the number of packets received is lower than the number of packets sent. This is mainly due to the high traffic in the transmission channel generated by the attacker, which prevented the legitimate nodes from transmitting their packets to the sink. In addition, the malicious node made the base station busy by receiving and processing fake packets that were transmitted to it, which subsequently interrupted the normal operation of the packet reception process in the system. Figure 8 shows the packet loss rate, as in (1), by each node for the three cases:

$$PacketsLossRate = 1 - \frac{packetsReceived[node]}{packetsSent} \tag{1}$$

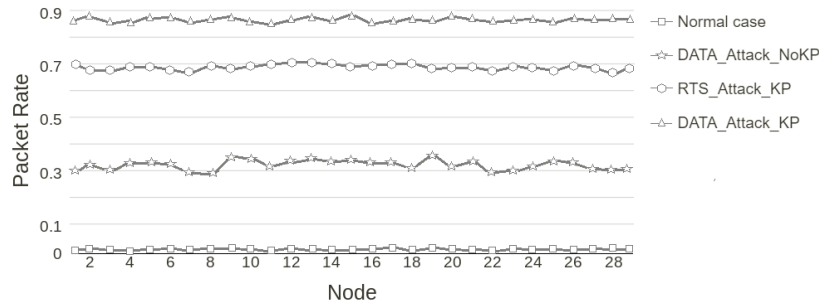


Figure 8. Packet loss rate per node

Figure 9 represents the energy consumption of the network by each node (2). For the first scenario, we can see that energy consumption is normal. So the system is working properly. As the moment the jamming attack is launched in the system, the energy consumption increases.

$$EnergyConsumption = initialEnergy - remainingEnergy \tag{2}$$

The reason for the high energy consumption of the base station (Node 0) in the case of no knowledge of the protocol used (DATA Attack NoKP), is the reception of traffic generated by the malicious node. On the other hand, in the case of knowledge of the protocol used (RTS Attack KP, DATA Attack KP) the energy consumption of the base station (Node 0) is much higher because of the reception and processing of false packets. The knowledge of the protocol allows the attacker to behave as a legitimate node, which allows him to deceive the base station, and the latter ends by processing these false packets. In addition to this, the high traffic generated by the attacker forces other nodes in the network to send more packets than expected since a communication failure is generally followed by several more attempts. With every new attempt, the nodes consume more energy.

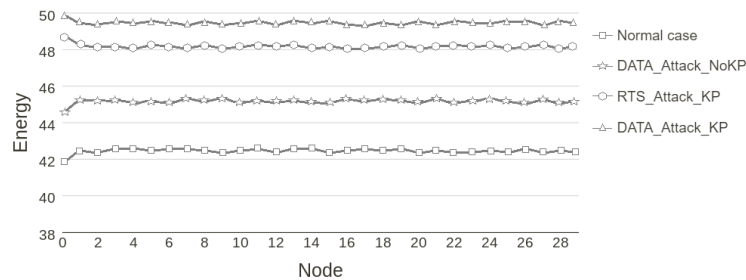


Figure 9. Energy consumption per node (J)

Energy is a term that is often used in synchrony with network lifetime. The Network lifetime is the period during which a wireless sensor network is fully operational. So this means that maximum energy consumption results in a minimum network lifetime. Figure 10 shows the estimated lifetime of the network. For the attacked network, we can find that the network lifetime is much shorter compared to the normal case. This is due to the jamming attack, which increased the traffic, thus wasting energy and eventually decreasing the lifetime of the network.

From the simulation results, we can see that all three types of jamming attacks (DATA Attack NoKP, RTS Attack KP, DATA Attack KP) affect the network performance. On the other hand, an attack by data packet, with knowledge of the protocol used in the system (DATA Attack KP) is much more effective than the other two types, because it affects the base station and all the nodes of the system in a very significant way and degrades the performance of the network, causing the system to stop working quickly.

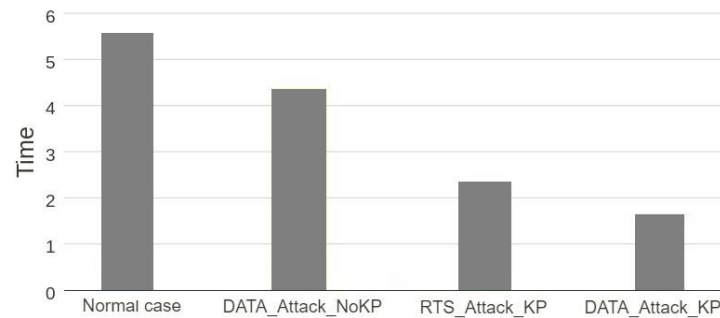


Figure 10. Estimated network lifetime (days)

4. CONCLUSION

In this paper, we have performed an extensive study on the different types of jamming attacks that target the IoT: Attack by data packets without knowledge of the protocol used, attack by control packets (RTS) with knowledge of the protocol used, and attack by data packets with knowledge of the protocol used. First, we have described the context of IoT security and a detailed taxonomy of the different security objectives. Then, we have detailed the different attacks that threaten connected objects and classify them according to the layers that define the IoT system architecture. Also, we have described in detail the functioning of the S-MAC protocol. Finally, we have provided a description of the proposed system and analyzed the results obtained according to the three types of jamming attacks simulated. The parameters used to analyze the efficacy of the system are the packet loss rate, energy consumption, the number of packets delivered, and the network lifetime. The final discussion showed that the attack by data packet, with knowledge of the protocol used in the network, is the most dangerous type of attack that can be applied to the system because of the very high energy consumption of the nodes, which decreases their lifetime, and finally destroys the system quickly. In future work, we will try to develop and implement a mechanism to secure the networks against the attack of Jamming by data packets with knowledge of the protocol used, in order to increase the lifetime of the system, and ensure proper reception of the packets.




REFERENCES

- [1] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in Internet of Things," *Future Generation Computer Systems*, vol. 100, pp. 144–164, Nov. 2019, doi: 10.1016/j.future.2019.04.038.
- [2] Z. Huanan, X. Suping, and W. Jiannan, "Security and application of wireless sensor network," *Procedia Computer Science*, vol. 183, pp. 486–492, 2021, doi: 10.1016/j.procs.2021.02.088.
- [3] S. G. Hymelin Rose and T. Jayasree, "Detection of jamming attack using timestamp for WSN," *Ad Hoc Networks*, vol. 91, p. 101874, Aug. 2019, doi: 10.1016/j.adhoc.2019.101874.
- [4] Jagriti and D. K. Lobiyal, "Energy consumption reduction in S-MAC protocol for wireless sensor network," *Procedia Computer Science*, vol. 143, pp. 757–764, 2018, doi: 10.1016/j.procs.2018.10.428.
- [5] R. Yugha and S. Chithra, "A survey on technologies and security protocols: Reference for future generation IoT," *Journal of Network and Computer Applications*, vol. 169, p. 102763, Nov. 2020, doi: 10.1016/j.jnca.2020.102763.
- [6] I. Kerrachou, S. Chadli, M. Emharraf, and M. Saber, "Analysis jamming attack against the protocol S-MAC in IoT networks," in *Lecture Notes in Networks and Systems*, vol. 211 LNNS, Springer International Publishing, 2021, pp. 311–321.
- [7] I. Kerrachou, S. Chadli, A. Kharbach, and M. Saber, "Simulation and analysis of jamming attack in IoT networks," in *Lecture Notes in Networks and Systems*, vol. 211 LNNS, Springer International Publishing, 2021, pp. 323–333.
- [8] K. Aarika, M. Bouhla, R. AitAbdelouahid, S. Elfilali, and E. Benlahmar, "Perception layer security in the internet of things," *Procedia Computer Science*, vol. 175, pp. 591–596, 2020, doi: 10.1016/j.procs.2020.07.085.
- [9] R. K. Jha, Puja, H. Kour, M. Kumar, and S. Jain, "Layer based security in narrow band internet of things (NB-IoT)," *Computer Networks*, vol. 185, p. 107592, Feb. 2021, doi: 10.1016/j.comnet.2020.107592.
- [10] V. Malik and S. Singh, "Evolutionary computing environments: implementing security risks management and benchmarking," *Procedia Computer Science*, vol. 167, pp. 1171–1180, 2020, doi: 10.1016/j.procs.2020.03.430.
- [11] S. Vadlamani, B. Eksioğlu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," *International Journal of Production Economics*, vol. 172, pp. 76–94, Feb. 2016, doi: 10.1016/j.ijpe.2015.11.008.
- [12] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, p. 102481, Jan. 2020, doi: 10.1016/j.jnca.2019.102481.
- [13] S. M. Tahsien, H. Karimpour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *Journal of Network and Computer Applications*, vol. 161, p. 102630, Jul. 2020, doi: 10.1016/j.jnca.2020.102630.
- [14] V. Ekong and U. Ekong, "a Survey of security vulnerabilities in wireless sensor networks," *Nigerian Journal of Technology*, vol. 35, no. 2, p. 392, Apr. 2016, doi: 10.4314/njt.v35i2.21.
- [15] B. Mihajlov and M. Bogdanoski, "Analysis of the WSN MAC protocols under jamming DoS attack," *International Journal of Network Security*, vol. 16, no. 4, pp. 304–312, 2014.
- [16] M. A. A. da Cruz, J. J. P. C. Rodrigues, P. Lorenz, P. Solic, J. Al-Muhtadi, and V. H. C. Albuquerque, "A proposal for bridging application layer protocols to HTTP on IoT solutions," *Future Generation Computer Systems*, vol. 97, pp. 145–152, Aug. 2019, doi: 10.1016/j.future.2019.02.009.




- [17] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 1, pp. 367–380, Jan. 2009, doi: 10.1109/TVT.2008.921621.
- [18] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
- [19] S. Anand and A. Sharma, "Assessment of security threats on IoT based applications," *Materials Today: Proceedings*, Oct. 2020, doi: 10.1016/j.matpr.2020.09.350.
- [20] Y. Rao, C. Deng, J. Su, Y. Qiao, J. Zhu, and R. chuan Wang, "Setting strategy of delay-optimization-oriented SMAC contention window size," *PLoS ONE*, vol. 12, no. 7, p. e0181506, Jul. 2017, doi: 10.1371/journal.pone.0181506.
- [21] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, Oct. 2017, doi: 10.1109/TETC.2016.2606384.
- [22] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.
- [23] M. Frustaci, P. Pace, G. Aloï, and G. Fortino, "Evaluating critical security issues of the IoT world: present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018, doi: 10.1109/JIOT.2017.2767291.
- [24] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: a survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, Jun. 2017, doi: 10.1016/j.jnca.2017.04.002.
- [25] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

BIOGRAPHIES OF AUTHORS






Imane Kerrakchou    graduated as an engineer in electronic systems, computer science and networks from the National School of Applied Sciences at Mohammed First University, Oujda, Morocco in 2017. She is currently a PhD student in Computer Science in the Department of Electronics, Computer Science and Telecommunications at the National School of Applied Sciences, Mohammed First University, Oujda, Morocco. Her research areas are IoT security, attack modeling, and machine learning models of cybersecurity. She can be contacted at email: i.kerrakchou@ump.ac.ma.






Sara Chadli    graduated as a network and telecommunication engineer from National School of Applied Sciences, Oujda, Morocco, in 2012. She received here Ph.D. in telecommunication and electronics engineering from Mohammed first University in 2016. she is currently an assistance professor in the Department of physiqes of Mohammed first University. Her research interests include Mobile AD Hoc networks (MANET), Network Security, modeling and control of advanced electrical power systems, design, application of power electronics and Telecommunications Engineering. She can be contacted at email: chad.saraa@gmail.com.



Yassine Ayachi    is a graduate PhD specialized in cybersecurity, with engineer diploma of networks and systems from National Schoul of Applied Sciences 2007 at University Mohammed First Oujda (Morocco). His researches fields are in cybersecurity especially intrusion decetion, attack modelling and cybersecurity machine learning models. He is also a cybersecurity and ISO-27000 compliance consultant and delivery manager at Novelis Morocco. He can be contacted at email: y.ayachi@ump.ac.ma.



Mohammed Saber    is currently an associate professor in the Department of Electronics, Computer Science and Telecommunications at National School of Applied Sciences at Mohammed First University, Oujda, Morocco (2013). He received a PhD in Computer Science at Faculty of Sciences, Oujda, Morocco, in July 2012, an enginner degree in Network and Telecommunication at National School of Applied Sciences, in July 2004, and Licence degree in Electronics at Faculty of Sciences, in July 2002, all from Mohammed First University, Oujda. He is currently director of Smart Information, Communication & Technologies Laboratory (SmartICT Lab). His interests include Network Security (Intrusion Detection System, Evaluation of security components, Security IoT), AI, Robotics, Embedded Systems. He can be contacted at email: m.saber@ump.ac.ma.