Investigation of amplification-based DDoS attacks on IoT devices

SANDRO ILÍDIO COELHO OLIVEIRA[1]
CLAUDIO DOUGLAS GOUVEIA LINHARES[2]
BRUNO AUGUSTO NASSIF TRAVENÇOLO[2]
RODRIGO SANCHES MIANI[2]

UFU - Universidade Federal de Uberlândia
FACOM - Faculdade de Computação
38400-902 - Uberlândia (MG) - Brazil
[1]sandro.icoelhos@gmail.com
[2]claudiodgl,travencolo,miani@ufu.br

Abstract. The purpose of this work is to evaluate the potential of Internet of Things (IoT) devices in conducting Distributed Denial of Service Attacks (DDoS). To this end, we propose a simulated WSN (wireless sensor networks) environment based on nodes running the Constrained Application Protocol (CoAP). Our idea is to extend the results obtained from previous work by evaluating the impact of the DDoS attack according to the following parameters: packet length, number of packets, and the traffic injection rate. Due to the low storage capacity, processing, and performance of the nodes, the whole network had its resources quickly drained during DDoS attack simulations. Our findings suggest that increasing the packet length can have a higher impact on network performance compared to the number of packets or the injection rate.

Keywords: wireless sensor networks, internet of things, cybersecurity, denial of services attacks, simulation

(Received May 19th, 2020 / Accepted June 1st, 2020)

1 Introduction

According to Rayes and Salam [21], the main idea of the Internet of Things paradigm is to act by physically connecting anything to the Internet to monitor and control its functionality. In this way, the ubiquitous presence of these connected devices makes them capable of interacting and cooperating to reach a common purpose [4]. This concept became popular both in academia and the business sector due to the high number of applications for society. However, despite its potential to improve people's quality of life, the Internet of Things brings with it a growing concern with the security and privacy of data [21].

A denial of service (DoS) attack is intended to make resources unavailable to its users by, in most cases, increasing the network traffic to the target device [7]. In a distributed denial-of-service attack (DDoS), the incoming network traffic targeting the victim originates from many sources. In 2016, the most significant DDoS attack recorded until that moment occurred using a malware called Mirai [3]. This malware, infected security cameras, and video recording devices (DVR). Those IoT devices were used to trigger DoS attacks against domain name servers (DNS) hosted at the company DYN, which is responsible for providing network infrastructure services [6].

Wireless Sensor Networks (WSN) are one of the leading technologies used to materialize IoT applications [16]. WSN refers to a group of nodes with sensing, computation, and wireless communications capabilities [1]. An example of a scenario commonly used in WSNs involves monitoring environment variables, such as temperature. For that, several sensor nodes are

spread in an area of interest. Such devices can collect data and transmit it over a wireless network to one or more exit points, known as network coordinating nodes or base-station (BS). Sensor nodes usually have limited processing, storage, and energy resources. Most of them perform only one specific processing function and are powered by non-rechargeable batteries and must be independent, without requiring constant updates and human assistance [9]. Since sensors on a WSN network communicate with each other and with an external node, it is possible that DoS attacks could be launched to cause network resources unavailability and, consequently, harm the performance of applications that are consuming data from sensors [22]. Therefore, evaluating the impact of DoS attacks on WSN networks becomes a relevant research problem as discussed in [17, 5, 11]

The research conducted in [18] implemented scenarios to simulate and evaluate the effects of an amplification DDoS attack on a wireless sensor network (WSN). The scenarios were built so that the WSN has a malicious infiltrated node that sends service discovery requests to all sensors with a spoofed IP address. The results show that such an environment is vulnerable to DDoS attacks.

Using the experimental environment proposed in [18], the goal of our work is to evaluate the impact of DDoS amplification attacks on a WSN network according to i) variations in the number of sensors, ii) packet size that will be reflected in the network and iii) changes in traffic injection rates (higher than 16kbps). The idea is to show that such an attack can be exploited in different ways by the attacker. Another contribution of this work is the application of data visualization techniques to study network nodes' behavior during the simulation.

The rest of the paper is organized as follows. Section 2 presents related work. Section 3 shows the methodology and simulation scenario. Section 4 discusses the experimental results, and Section 5 provides some concluding remarks and future work.

2 Related Work

Furfaro et al. [10] evaluated the effects of DDoS attacks on UDP-based protocols. The authors used the *NeSSi* simulator to test the defense and reaction systems under DDoS amplification and reflection attacks considering the DNS (Domain Name Server) and NTP (Network Time Protocol) protocols. The simulation environment was built using a botnet with 150 zombies attacking three vulnerable serves available bandwidth of 200 Mbits/s. In both attacks, the growth speed is similar, but NTP handled 300% more bandwidth, as the NTP protocol generates more packages the DNS in a ratio of 23:1.

Hengst [12] evaluated the use of IoT devices as reflectors in a DDoS amplification/reflection attack. First, it was identified the twelve most used DDoS attacks, from which it was analyzed which attack can use IoT devices as reflectors. The influence of factors such as device availability, accessibility, usability, and bandwidth in the strength of a DDoS attack was evaluated.

In the paper by Peraković [20], it was analyzed DDoS attacks records from 2013 to 2015. They found that, between the several types of DDoS attacks, the SSDP (Simple Service Discovery Protocol) is the most common protocol. The explanation for this finding is that this protocol is broadly used in IoT devices – it is used for detection of UPnP (Universal Plug and Play) devices, which allows the connection between the devices without user intervention (machine to machine (M2M) communication.

The papers by Kolias et al. [13] and Angrishi [2] describe a general view between IoT devices and DDoS attacks. While the first lists the main IoT malware associated with botnets creation and suggests several countermeasures, the second focuses on the Mirai malware and its variants. In both papers, the authors reinforce the importance of learning technical means to enforce security best practices in computer networks as well as robust security standards for IoT devices and vendors.

Regarding amplification attacks, references [8] and [24] discuss within the scope of IoT. Gondim et al. [8] develop a Decision-Oriented Tool-Agnostic (DOTA) methodology for performing Active Vulnerability Assessment (AVAs). They use the proposed method to evaluate amplified reflection DDoS attacks against IoT infrastructure and devices using an in-house tool. Vasques and Gondim [24] analyzed the reflector saturation during DDoS attacks using both general-purpose computers and IoT devices as mirrors (a Raspberry Pi, an ADSL home gateway, and an enterprise IP camera). Their results indicate that amplified reflection DDoS attacks are feasible to be performed using IoT devices as reflectors. However, the more limited they are, in terms of computational resources, the earlier they saturate.

Finally, the proposal by Pacheco et al. [18] presents a detailed description of an experimental setup to reproduce DDoS attacks in an IoT environment. The ns-3 simulator is used, and several parameters are tested to evaluate the strength of the attacks. To the best of our knowledge, this is one of the few works that use parameterized simulations to evaluate DDoS in an IoT scenario. Our goal is to extend this idea and analyze different attack features.

3 Methodology

In this section we present the IoT protocol stack adopted in the experiments and the simulation environment.

3.1 IoT protocol stack

The IoT protocol stack that will be used during our simulations can be summarized as follows [19]. Figure 1 illustrates the relationship between each layer.

- CoAP - Constrained Application Protocol (Application): ensures formatting of sent/received messages and also features service discovery resources;
- UDP - User Datagram Protocol (Transport): manages point-to-point communication between applications;
- 6LoWPAN - IPv6 over Low power Wireless Personal Area Networks (Network): provides an adaptation of IPv6 to IEEE 802.15.4, using header compression methods;
- IEEE 802.15.4 (Medium Access Control and Physical): provides a reliable link between nodes, detecting errors that may occur during transmission/reception at the physical layer. It also transmits the frame through the mediums;

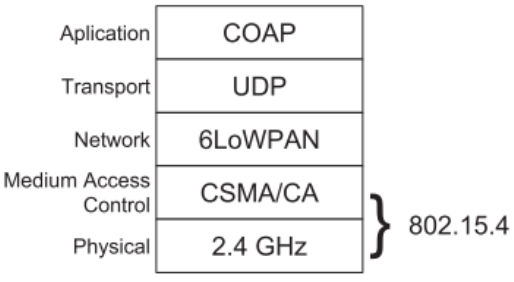

Figure 1: IoT protocol stack. Adapted from [18].

3.2 Test scenarios

The test scenarios are based on a star topology with 1, 3, 5, 50, and 100 nodes, arranged in a mesh with 2 meters of spacing between them. The star topology has become more suitable, as the communication and management of the wireless sensor network take place from the coordinating node. In the simulation environment, shown in Figure 2, the following actors were defined:

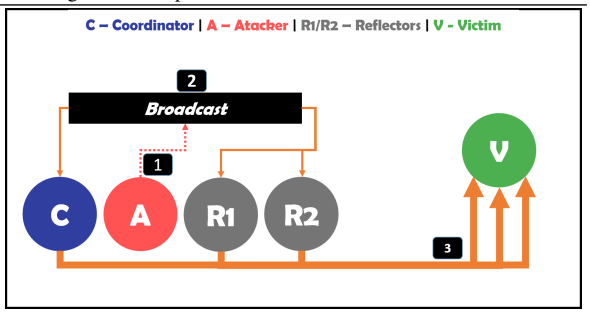

Figure 2: DDoS attack on the WSN network of this work

1. WSN coordinating node (**C**) that is, the one that is responsible for managing and structuring the communication between the other nodes;
2. Attacking node (**A**) that will send broadcast requests with a spoofed source IP address;
3. Auxiliary sensor nodes or reflectors (**R1** and **R2**);
4. Victim of the attack that is outside the WSN. (**V**).

The scenarios were developed to exploit the service discovery function of the CoAP protocol. The network has a malicious infiltrated node that sends service discovery requests to all sensors using the victim's IP as the source address, as can be seen in step number 1 of Figure 2. As a fundamental feature of the CoAP protocol, as soon as a sensor receives a request, it must immediately send a response informing which services it supports. This can be seen in step 2 of Figure 2, in which it shows the reflecting sensors receiving the packages and consequently sending the response to the victim, step 3.

As proposed in [18], the request packet sent by the attacker has the "/.well-known/" URI path prefix, which renders a 20 byte packet size. The response message contains 61 bytes (only one service, temperature sensor), representing a reflection rate of 3.05 for each device that receives the request packet.

3.3 Comparison with previous work

Table 1 presents the characteristics of the work proposed in [18] and our work. Concerning the differences, the size of the request packet had its value doubled so that the behavior of the network with a larger amount of data could be analyzed. The injection rate varied between 1.92, 2.8, 24, 32, and 64 Kbps (12/13/150/200 packets per second), taking into account the results obtained by the authors of [18]. It is important to note that the number of packets per second (PPS) sent by the attacker defines the traffic injection rate. Therefore, a rate

of 0.16 kbps is equivalent to 1 request packet per second transmitted to all intermediate sensors. Finally, to simulate smaller networks, tests were performed with one and three sensors only, since the minimum amount used in the previous work was five sensors.

The proposal of new parameters was necessary to verify a hypothesis suggested in [18] that, although viable, the CoAP reflection attack requires a high number of IoT networks to be effective.

Regarding the measures used to evaluate the network performance, two new metrics were proposed: i) rate of reflected packets and ii) packets sent. The first one measures the percentage of packets that are reflected by the intermediate nodes. Since every packet sent by the attacker should have a reply by the intermediate nodes, we would expect that during normal conditions, this rate would be 1: 1. However, an intermediate node might not be able to reply to every request sent by an attacker during an attack. In other words, this metric captures the performance of the intermediate nodes during an attack. The second metric is straightforward and accounts for the number of packets sent by each node.

4 Results

The simulations were implemented using the ns-3 and executed for 60 seconds. The results were divided into two parts: the first shows the simulations carried out with one, three and five sensors (subsections: 4.1, 4.2 and 4.3, respectively), where we will present the number of packets sent by each node, the rate of reflected packets and the average amplification of packets. The second part of the results, in the subsection 4.4, presents the results achieved with the aid of *DyNetVis* visualization software in the simulations with 50 and 100 sensors, by which we changed the number of packets per second, the injection rate and the request packet size. Section 5 highlights the discussions about the results achieved.

The experiments were divided according to the number of reflector sensors in each scenario. It is relevant to say that the coordinating node was also included in the analysis. If the subsection mentions “3 sensors” (subsection 4.2, for instance), the posterior distribution of nodes must be taken into account for that scenario: one attacking node, three reflecting nodes and one coordinator.

4.1 1 Sensor

Figure 3 represents the number of packets that each sensor sent to the network; the attacker is responsible for sending the requisition packets in *broadcast* and the

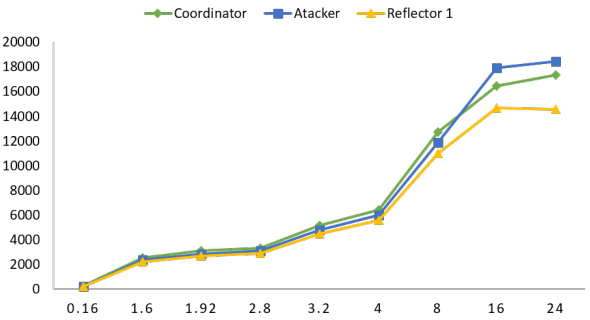

Figure 3: Number of packets sent by each node (1 Sensor)

responses sent to the victim. Figure 3 shows that the network’s behavior remains similar when the attacker’s injection rate varies between 0.16 Kbps and 8 Kbps. However, after 16 Kbps, the number of packets sent by the coordinator and reflector number 1 decreases, indicating saturation of both sensors.

Figure 4 represents, on average, how much the network was able to reflect from the packets sent by the attacker. As noted, simulating with one sensor (in addition to the coordinator and attacker), the network behaves well up to 4 Kbps, reflecting more than 100% of the received packets. However, after 8 Kbps, the reflectors start having problems answering the attacker’s requests, and the packet loss starts (around 20%, that is, the network has issues but is still functional). From the attacker’s point of view, this may be the beginning of unavailability in the network elements, characterizing the DoS attack. As discussed in [18], the network disruption should be possible with a more significant number of nodes. In the following sections, this possibility will be explored appropriately.

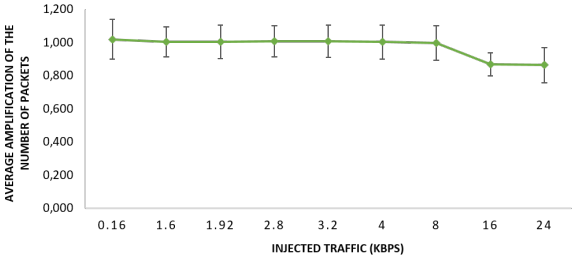

Figure 4: Rate of reflected packets (1 Sensor)

Figure 5 was generated to improve the visualization of the amount of data sent to the network by the attacker. It also shows how much of this data was amplified and sent to the victim. It is possible to see that in the previous scenario of the experiment (24 Kbps), the amplification rate is around 4.75. However, with lower in-

Table 1: Differences between the simulations elaborated by [18] and our work

Attribute	Pacheco et al. [18]	This work
Request packet size	20 Bytes	20 / 40 Bytes
Traffic injection rate	0.16 / 1.6 / 3.2 / 4.0 / 8.0 / 16.0 Kbps	0.16 / 1.6 / 1.92 / 2.8 / 3.2 / 4 / 8 / 16 / 24 / 32 / 64 Kbps
PPS sent	1 / 10 / 20 / 25 / 50 / 100	1 / 10 / 12 / 13 / 20 / 25 / 50 / 100 / 150 / 200
Number of sensors	5 / 25 / 50 / 75 / 100	1 / 3 / 5 / 50 / 100
Metric	Amplification rate Total traffic generated Average traffic generated for each node	Amplification rate Total traffic generated Rate of reflected packets Packets sent
Type of atack	DDoS by amplification and reflection	
Topology	Star	
Duration of the simulation	60 seconds	
Protocols stack	CoAP / UDP / 6LowPAN / IEEE 802.15.4	
Type of sensors	Coordinator / attacker / victim	
Implemented service	Temperature	

jected traffic rates, the amplification rate is higher than that; for example, for 3.2 Kbps, we have an amplification rate of 5.54.

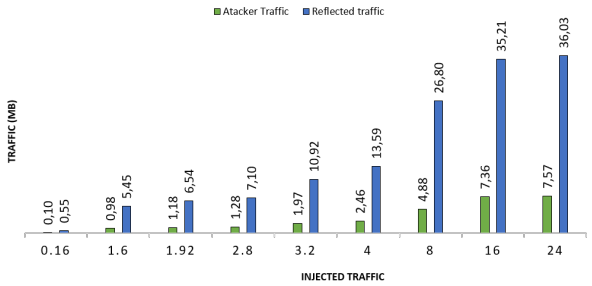

Figure 5: Injected and amplified traffic (1 Sensor)

4.2 3 Sensors

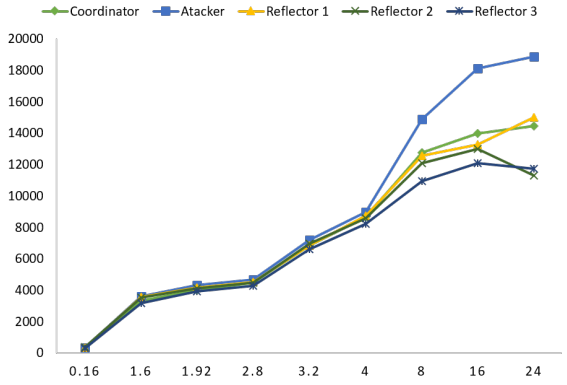

Figure 6: Number of packets sent by each node (3 Sensors)

It is observed in Figure 6 that the behavior of the nodes remains steady when the attacker's injection rate varies between 0.16 Kbps and 8 Kbps. However, after 8 Kbps, the number of packets sent by the coordinator and the reflector sensors decreases, indicating saturation. Compared with the scenario with only one reflector, it is possible to see that the number of sensors directly impacted the network's performance during the attack. In other words, there is an indication that the efficiency of reflectors is related not only to the attacker injection rate but also to the number of reflectors in a network.

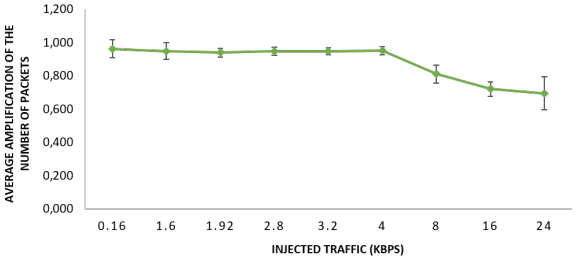

Figure 7: Rate of reflected packets (3 Sensors)

Figure 7 shows that the network can reflect about 95% of the packets it receives until the attacker's throughput rate reaches 4 Kbps. After 8 Kbps, the reflectors are unable to process all the receiving packets, and the network gradually loses resources, reaching around 30% of the packet loss in the scenario with the injection rate at 24 Kbps.

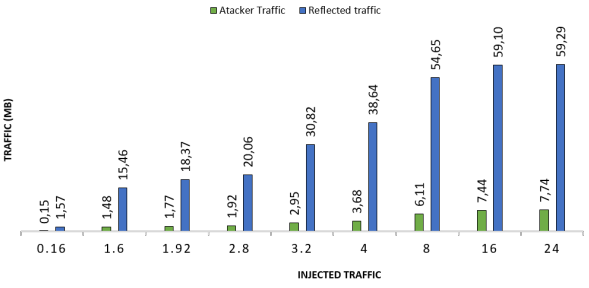

Figure 8: Injected and amplified traffic (3 Sensors)

Figure 8 shows that in the previous scenario of the

experiment (24 Kbps), the difference between the traffic generated by the attacker and the reflected traffic shows an amplification rate of 7.66, that is, a value 2.89 times higher than the previous experiment (1 sensor). It is also noticeable that the amount of data the attacker sent to the network remains almost unchanged in the injection rates of 16 and 24 Kbps in both simulations. This behavior, where traffic levels indicate stagnation, can be used to adjust network parameters to mitigate attacks against sensors.

4.3 5 Sensors

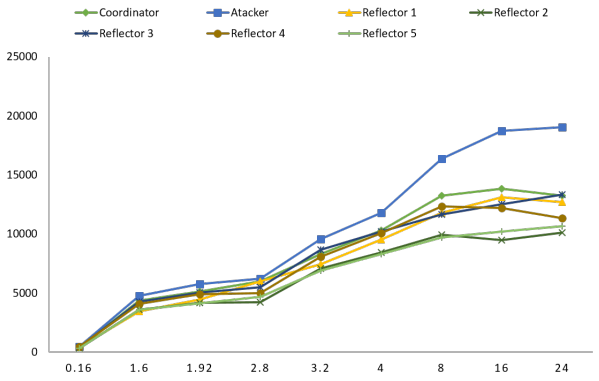

Figure 9: Number of packets sent by each node (5 Sensores)

Figure 9 shows that there were variations in all flow levels of the network during the simulation. Reflectors 2 and 5 had more difficulty in reflecting the attacker's packets since, in a total of 19,071 packets sent by the attacker, they managed to reflect only 10,126 and 10,653, respectively. Reflector 4 and the coordinator obtained high levels of reflection from the packages. However, the performance of nodes in the reflection of packets drops dramatically in simulations where the traffic injection rate is higher than 4Kbps. That is, the difference between the number of packets sent by the attacker and the number of packets reflected by the sensors is inversely proportional to the increase in the traffic injection rate.

Figure 10 shows that the network drops about 15% to 20% of the packets with traffic injection rates between 0.16 Kbps and 4 Kbps. From 8 Kbps, the levels drop gradually, so that at the end of the simulation, only 62% of the received packets are being reflected. The results obtained with five sensors showed significant differences compared to the results achieved with one and three sensors in all metrics presented, especially in the one exposed by Figure 10, where changes in the amplification rate from the first injection traffic levels are noticeable.

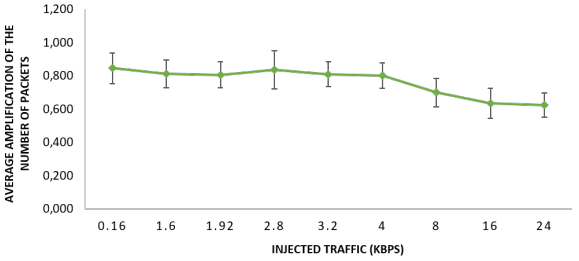

Figure 10: Rate of reflected packets (5 Sensors)

Figure 11 indicates that there was no significant difference between the values of the highest traffic injection rates, as the network at that point was already saturated with the number of received packets. The best result is found with a traffic injection rate of 2.8 Kbps, reaching an amplification rate of 13.84.

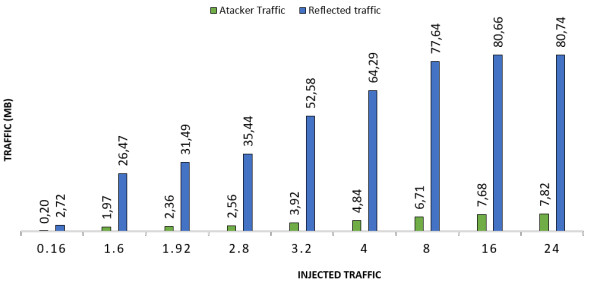

Figure 11: Injected and amplified traffic (5 Sensors)

4.4 50 and 100 sensors

Figure 12 and Figure 14 represents the total traffic amplification rate and the relation between the traffic sent by the attacker and the traffic reflected by the other sensors in simulations using 50 sensors. Moreover, the Figure 13 and Figure 15 presents an visual analysis using the software Dynamic Network Visualization – *DyNetVis*, developed by [15], and freely available at `www.dynetvis.com`. In all analyses, the traffic injection rate was equal to *64 Kbps, and the request package size was changed from 20 to 40 bytes.

Figure 12 demonstrates that the traffic amplification rate did not succeed in these cases since the maximum result expected was 155.55, corresponding to 3.05 times for a total of 51 sensors. When considering a traffic injection rate as 16 Kbps, the result is 88% worst than the expected. Even duplicating the attacker's flow rate, the network has shown more congestion, presenting a result approximately 89 times smaller than the total expected.

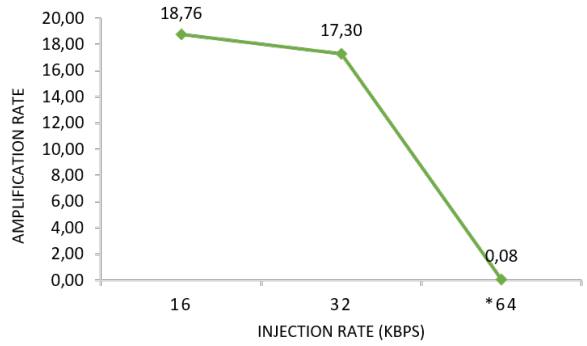

Figure 12: Total amplification of the simulations with 50 sensors.

In the last simulation, only 0.05% of the packages received by the network were reflected to the victim, showing complete exhaustion of the protocols responsible for the communication of the sensors. In absolute numbers, the total traffic in scenarios with 16 and 32 Kbps should be between 311 and 622.2 MB, respectively, and for 64 Kbps, the victim should be receiving 1.24 GB in total. However, as demonstrated in Figure 14, the traffic obtained with the simulations was far below the expected, with the total maximum reflected traffic equal to 44.21 MB.

To better understand the pattern of the attacks, we applied to the data, some information visualization techniques using the software DyNetVis [15]. This software provides different layouts to observe the structure and temporal patterns of networks using the nodes connections. A recommended technique to see temporal behaviors is the Massive Sequence View – MSV, since has been used with success in different scenarios [15][14],[23],[25]. The MSV layout position the nodes vertically and the timestamps horizontally, growing from the left to the right.

In addition to MSV, we used a simple line graph to visualize the evolution of connections along the time [15]. The number of connected sensors is represented vertically, and the time is represented horizontally. It is important to notice that the IEEE 802.15.4 protocol implements the concept of CSMA/CA. Then, during the simulations, there should not be two or more nodes communicating simultaneously with the same destiny. However, this pattern occurs in layouts constructed using DyNetVis. The reason is that the networks were aggregated before visualization (i.e., the temporal resolution was modified, gathering some timestamps), to produce a better layout.

To easily identify each simulation, an acronym was defined for each setup using the following rules:

- P - Request packet in bytes;
- S - Sensors;
- T - Traffic injection rate in Kbps;
- For Example, *50S16T20P* represents a simulation of 50 sensors with 16 Kbps of traffic injection rate and request packet size of 20 bytes.

The line graph obtained in the simulation *50S16T20P*, as shown in Figure 13, demonstrates that there is no apparent trend or pattern regarding the number of connected sensors over time. However, we were able to note that there is a connection in every timestamp since every vertical line is above the horizontal line.

The MSV layout, as the line graph, shows the nodes' connection pattern throughout time and helps in the visual analysis of the communication among sensor pairs. In this visualization, each sensor is represented by a circle. If there is a connection between nodes, the edge (straight line positioned vertically) that connects both sensors is highlighted in a specific color. Table 2 describes the meaning of colors used in the MSV layout.

Table 2: Color legend for the MSV layout.

Node	Edge	Color
Coordinator	Coordinator ->Victim	Red
Sensors	Sensor ->Victim	Blue
Victim	Sensor ->Coordinator	Green

Figure 15 shows the MSV for the simulation *100S16T20P*. There is similar behavior to the Figure 13. It is possible to notice that several timestamps have the same amount of nodes communicating with the victim. However, the difference from the *50S16T20P* simulation is that when using 100 sensors, there are some moments that the communication between the nodes is interrupted (the line graph reaches zero), indicating some network resource depletion. In this scenario, where there is no communication between the nodes, the MSV layout shows blank spaces in the layout in the same timestamps where the line graph has zero connections. These patterns are also present in the visualization for the simulations of *50S16T20P* and *50S32T20P*.

Finally, an interesting result was obtained when the request packet has been doubled to 40 bytes. Figure 16 demonstrate the simulation of *50S64T40P*, with some different patterns from the previous analysis (Figure 13 and Figure 15) as:

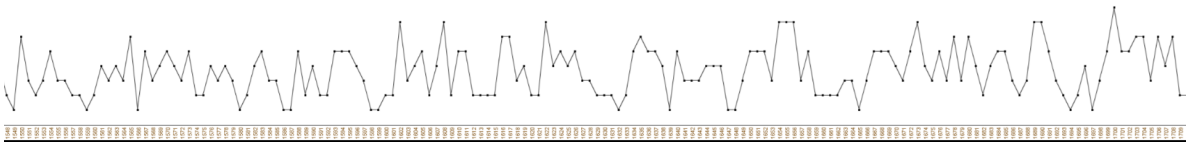

Figure 13: Line graph of the simulation with 50 sensors, 16 Kbps and request packet of 20 Bytes.

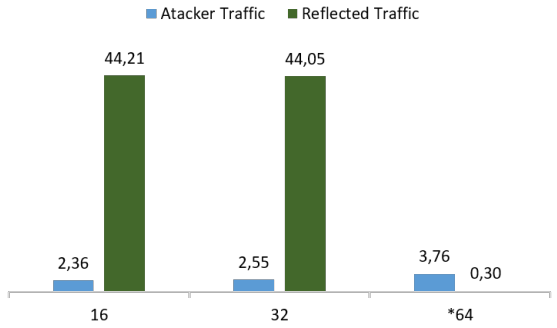

Figure 14: Traffic generated by the attacker and traffic amplified by the reflectors (50 Sensors).

- The presence of a few simultaneous connections between the nodes can be observed in the MSV layout by the increase of blank spaces and represented by the same repeated pattern in the line graph;
- Absence of high peaks in the same line graph, indicating low communication activity;
- High amount of gaps among different timestamps, demonstrating the depletion of network resources due to the lack of communication between the sensors.

5 Concluding remarks

In this work, we analyzed the potential of IoT devices in effecting DDoS attacks. Based on the work conducted by [18], we performed different experiments, examined them using various metrics, and employed a visualization technique to show the risks of DoS attacks in IoT environments. However, to obtain an effective attack, it is necessary a good understanding of the capacity of the IoT devices, the available services, the implemented protocols, and other properties. We have shown that for an amplification-based DoS attack in a WSN scenario, the following parameters should be considered: the number of sensors, traffic injection rate, and also the attackers' packet size.

The results can be analyzed based on two points of view: i) the attacker's view (traffic injection and packet size sent to the network) and ii) network behavior (rate of reflected packets). A first observation is that, from the attacker's point of view, an increase in the traffic injection rate does not necessarily imply an increase in the traffic amplification rate. For simpler scenarios, with 1, 3, and 5 sensors, this increase is noticeable up to a certain traffic injection rate, as illustrated by Figures 5, 8 and 11. However, in more complex scenarios, an increase in the data rate sent to the network does not mean that the attacker will succeed in conducting an amplification-based DoS attack. Figure 12 illustrates this situation.

A significant result was obtained when the request packet had is default size doubled to 40 bytes using a scenario with 50 sensors and an injection rate of 64 Kbps. The analysis was visually explored using the software *DyNetVis* [15]. In this environment, it was observed that the network was not able to process the high number of data requests from the attacker.

Future work includes analyzing the performance of the sensor regarding their distance from the attacker. Our initial findings suggest that the sensors near the attacker have shown better performance than those "physically" far from the attacker. Another experiment includes the analysis of attacks using several coordinated networks, attacking only one victim. We also intend to explore the impact of different metrics, such as battery consumption, memory, and processing during an attack.

References

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. Wireless sensor networks: a survey. *Computer networks*, 38(4):393–422, 2002.

[2] Angrishi, K. Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets. *arXiv preprint arXiv:1702.03681*, 2017.

[3] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., et al. Understanding the mirai botnet. In *26th {USENIX} Security Symposium ({USENIX} Security 17)*, pages 1093–1110, 2017.

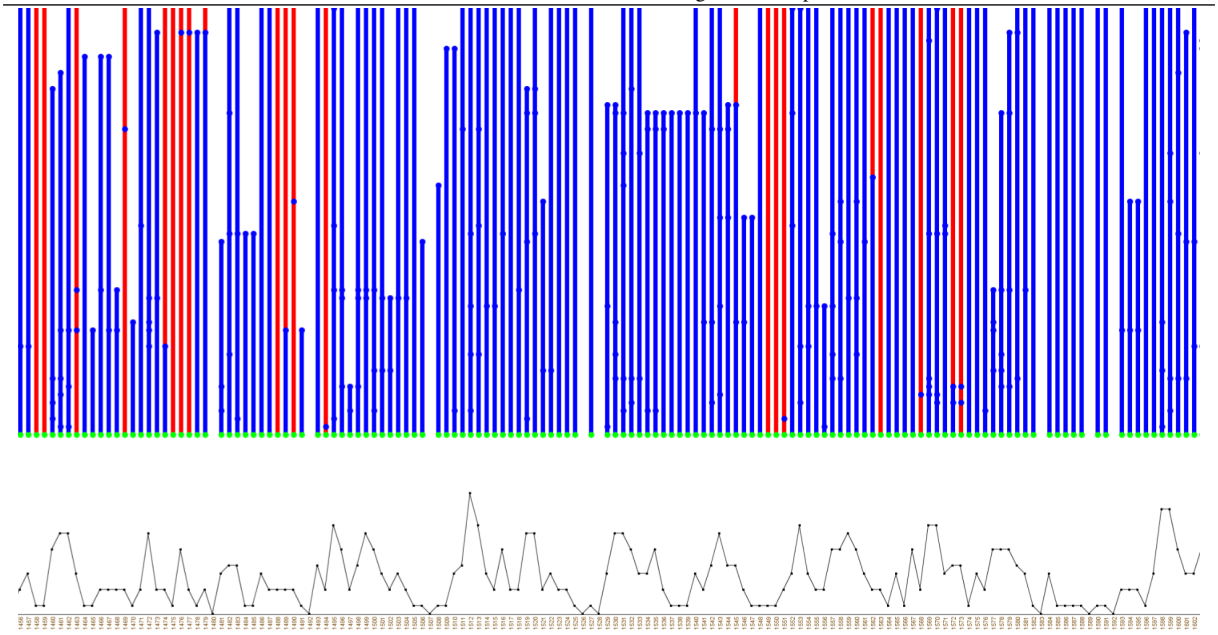

Figure 15: Part of the visualization for the simulation with 100 sensors, 16 Kbps and request packet of 20 Bytes.

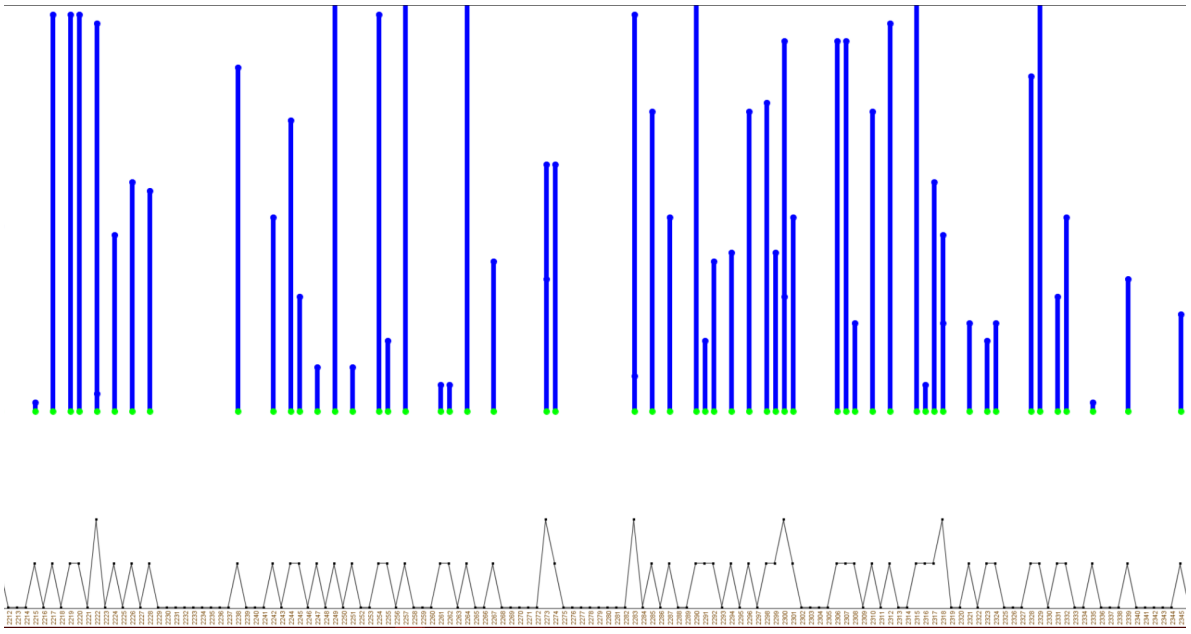

Figure 16: Part of the visualization for the simulation with 50 sensors, 64 Kbps and request packet of 40 Bytes.

[4] Atzori, L., Iera, A., and Morabito, G. The Internet of Things: A survey. *Proceedings of the 1st International Conference on E-Business Intelligence (ICEBI2010)*, 54(15):358–366, 2010.

[5] Balaji, S. and Sasilatha, T. Detection of denial of service attacks by domination graph application in wireless sensor networks. *Cluster Computing*, 22(6):15121–15126, 2019.

[6] Cao, C., Guan, L., Liu, P., Gao, N., Lin, J., and Xiang, J. Hey, you, keep away from my device: remotely implanting a virus expeller to defeat mirai on iot devices. *arXiv preprint arXiv:1706.05779*, 2017.

[7] Carl, G., Kesidis, G., Brooks, R. R., and Rai, S. Denial-of-service attack-detection techniques. *IEEE Internet computing*, 10(1):82–89, 2006.

[8] Costa Gondim, J. J., de Oliveira Albuquerque, R., Clayton Alves Nascimento, A., García Villalba, L. J., and Kim, T.-H. A methodological approach for assessing amplified reflection distributed denial of service on the internet of things. *Sensors*, 16(11):1855, 2016.

[9] Delicato, F. C. Middleware baseado em serviços para redes de sensores sem fio. *PhD Thesis, Federal University of Rio de Janeiro, Brazil*, 2005.

[10] Furfaro, A., Malena, G., Molina, L., and Parise, A. A Simulation Model for the Analysis of DDoS Amplification Attacks. *Proceedings - UKSim-AMSS 17th International Conference on Computer Modelling and Simulation, UKSim 2015*, pages 267–272, 2016.

[11] Ghildiyal, S., Mishra, A. K., Gupta, A., and Garg, N. Analysis of denial of service (dos) attacks in wireless sensor networks. *IJRET: International Journal of Research in Engineering and Technology*, 3:2319–1163, 2014.

[12] Hengst, K. DDoS through the Internet of Things. *25th twente student conference on IT*, 2016.

[13] Kolias, C., Kambourakis, G., Stavrou, A., and Voas, J. Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84, 2017.

[14] Linhares, C. D., Ponciano, J. R., Pereira, F. S., Rocha, L. E., Paiva, J. G. S., and Travençolo, B. A. A scalable node ordering strategy based on community structure for enhanced temporal network visualization. *Computers and Graphics*, 84:185 – 198, 2019.

[15] Linhares, C. D. G., Travençolo, B. A. N., Paiva, J. G. S., and Rocha, L. E. C. DyNetVis: A System for Visualization of Dynamic Networks. *Proceedings of the Symposium on Applied Computing*, pages 187–194, 2017.

[16] Mainetti, L., Patrono, L., and Vilei, A. Evolution of wireless sensor networks towards the internet of things: A survey. In *SoftCOM 2011, 19th international conference on software, telecommunications and computer networks*, pages 1–6. IEEE, 2011.

[17] Osanaiye, O. A., Alfa, A. S., and Hancke, G. P. Denial of service defence for resource availability in wireless sensor networks. *IEEE Access*, 6:6975–7004, 2018.

[18] Pacheco, L. A. B., Gondim, J. J., Barreto, P. A. S., and Alchieri, E. Evaluation of distributed denial of service threat in the internet of things. In *2016 IEEE 15th International Symposium on Network Computing and Applications (NCA)*, pages 89–92. IEEE, 2016.

[19] Palattella, M. R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L. A., Boggia, G., and Dohler, M. Standardized Protocol Stack For The Internet Of (Important) Things. *IEEE Commun. Surveys Tuts.*, 15(3):1389–1406, 2012.

[20] Peraković, D., Periša, M., and Cvitić, I. Analysis of the IoT impact on volume of DDoS attacks. *33rd Symposium on New Technologies in Postal and Telecommunication Traffic (PosTel 2015)*, (December):295–304, 2015.

[21] Rayes, A. and Salam, S. Internet of things-from hype to reality: The road to digitization. *Internet of Things From Hype to Reality: The Road to Digitization*, 32(8):1–328, 2016.

[22] Raymond, D. R. and Midkiff, S. F. Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*, 7(1):74–81, 2008.

[23] van den Elzen, S., Holten, D., Blaas, J., and van Wijk, J. J. Reordering massive sequence views: Enabling temporal and structural analysis of dynamic networks. In *2013 IEEE Pacific Visualization Symposium (PacificVis)*, pages 33–40, Feb 2013.

[24] Vasques, A. T. and Gondim, J. J. Amplified reflection ddos attacks over iot mirrors: A saturation analysis. In *2019 Workshop on Communication Networks and Power Systems (WCNPS)*, pages 1–6. IEEE, 2019.

[25] Zhao, Y., She, Y., Chen, W., Lu, Y., Xia, J., Chen, W., Liu, J., and Zhou, F. Eod edge sampling for visualizing dynamic network via massive sequence view. *IEEE Access*, 6:53006–53018, 2018.