Toward Modeling of Flooding Attacks Targeting Massive IoT Networks

José Ribeiro(✉), Valdemar Monteiro, and Jonathan Gonzalez

Evotel Informática S.A, Monforte de Lemos, Spain
{jose,valdemar,jgonzalez}@evotel-info.com

Abstract. During the current deployment of 5G networks, the researchers and engineers are now focus on the development of the 6G networks. The vision of the new 6G era is to offer a much wider range of applications compared to 5G by interconnecting billions of IoT devices that can also build upcoming IoE ecosystems. Definitely, the unprecedented growth of 6G IoT devices along with the massive emergence of connections in the future 6G communication platform will increase the security vulnerabilities for the massive IoT networks, leading to a wide spectrum of known and unknown security threats. Therefore, there is an urgent need for developing novel security solutions for massive IoT networks, taking into consideration their resource-constrained limitations. In particular, considerable research efforts have recently been put into the design and development of light-weight Anomaly-based Intrusion Detection Systems (AIDSs). However, they cannot be widely applied in practice as they suffer from high false-positive rate, and thus more robust AIDSs are required to be developed. Toward this direction, in the EU-funded Marie Sklodowska-Curie REACT project, we developed attack behavior models which are important for analyzing and getting a comprehensive understanding of the behavior of attacks over time to predict their behavior and extract design specifications for more robust AIDSs. The focus of this work is on models for flooding attacks against massive IoT networks.

Keywords: Massive IoT Networks · Attack Modeling · Anomaly-Based Intrusion Detection

1 Introduction

During the current deployment of 5G networks, researchers and engineers are now focusing on the development of the next generation of mobile networks (6G), which is expected to be commercialized by 2030. The vision of the new 6G era is to offer a much wider range of applications compared to 5G by interconnecting billions of IoT devices, such as extended reality devices, wearable displays, drones, and autonomous vehicles [1], which can also build upcoming IoE ecosystems. Definitely, the unprecedented growth of 6G-enabled IoT devices along with the massive emergence of connections in the future 6G communication platform will increase the security vulnerabilities for the massive IoT networks, leading to a wide spectrum of known and unknown security threats [2].

T. Pereira et al. (Eds.): IoECon 2024, LNICST 607, pp. 55–64, 2025.
https://doi.org/10.1007/978-3-031-84426-3_5

At the same time, attackers are becoming more sophisticated and powerful to carry out new types of attacks against the massive IoT networks. Therefore, there is an urgent need for developing novel security solutions for massive IoT networks, taking always into consideration their resource-constrained limitations, before they gain the trust of all involved stakeholders and reach their full potential in the 6G era, bringing significant benefits to both citizens and businesses [3]. Intrusion detection that already constitutes a popular defense technology for traditional IP networks is currently foreseen by industry and research community as a promising security solution that can also play a significant role in protecting IoT networks as long as novel Intrusion Detection Systems (IDSs) tailored to the resource-constrained characteristics of IoT networks have been developed. In particular, considerable research efforts have recently been put into the design and development of lightweight Anomaly-based Intrusion Detection Systems (AIDSs), leveraging Machine Learning (ML) techniques (e.g., SVMs) because of their ability to detect new, previously unknown attacks (e.g., zero-day attacks) in IoT networks [4, 5]. However, although AIDSs are attractive conceptually, they cannot be widely applied in practice as they suffer from high false-positive rate due to the fact that they may classify unseen (i.e., not included in the training dataset) benign instances as malicious, and thus more robust AIDSs are required to be developed. Toward this direction, in the EU-funded Marie Sklodowska-Curie REACT project, we developed attack behavior models which are important for analyzing and getting a comprehensive understanding of the behavior of attacks over time in order to predict their behavior and extract design specifications for more robust AIDSs. The focus of this work is on models for flooding attacks against massive IoT networks, as they are considering as a common threat for massive IoT networks [6–8]. The developed models are based on simulated data related to the generated network traffic of simulation scenarios in Cooja simulator [9] where massive IoT networks are under flooding attacks. The generated network traffic is captured from the properly configured Cooja tool "Radio messages".

Following the Introduction, the rest of the paper is organized as follows. Section 2 is focused on the simulation of massive IoT network scenarios. In particular, Sect. 2 discusses a scenario of massive IoT network without attack, and three scenarios where the massive IoT network is under User Datagram Protocol (UDP) flooding attack. In Sect. 3, flooding attack behavioral models, based on Machine Learning algorithms, are discussed. Finally, the paper is concluded in Sect. 4.

2 Simulation of Massive IoT Network Scenarios

2.1 Network Topology of Massive IoT Network Without Attack – Benign Scenario

The network topology of the simulated massive IoT network scenario in Cooja simulator environment consists of one UDP-server (the green mote) and 500 UDP-senders (the yellow motes), as shown in Fig. 1. The mote type used for the simulations is the type of sky with Contiki operating system. The server is located in the center, while the UDP-senders are placed in circles around the server. The UDP-senders are configured to send a UDP packet every 125s in order to avoid packet loss at the server side based on the number of the UDP-senders (500 yellow motes). The senders stop sending packets

around 5 min before the termination of the simulation to assure that all packets will have been delivered before the termination of simulation. Otherwise, the packets sent close to the termination period will never be received and thus, they will be counted as packet loss.

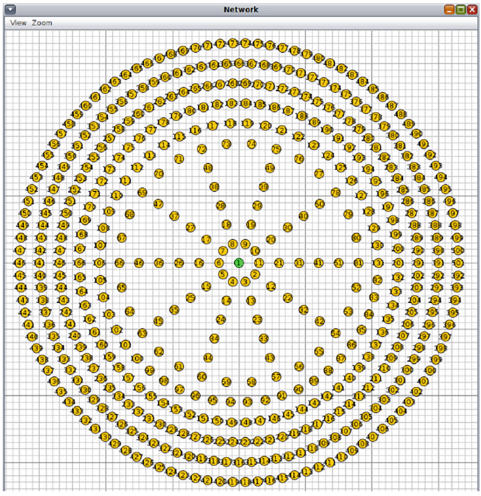

Fig. 1. Benign Scenario Topology in Cooja Simulator. (Color figure online)

2.2 Network Topology of Massive IoT Network Under UDP Flooding Attack – Malicious Scenarios

UDP flooding is a threat that can significantly affect the whole IoT network. This type of attack functions as a DoS attack, rendering the targeted entity incapable of effectively processing incoming requests. The target device continuously receives illegitimate requests from the attacker, leading to the depletion of its resources. The UDP attack is easy to perform, demanding minimal effort from the attacker, who exploits this simplicity to launch substantial volumes of UDP packets upon the target. In response, the target device tries to find solutions for the proper handling of these packets.

However, encountering failure, it issues an ICMP packet. While it keeps returning the ICMP packets, its capacity to effectively respond even to genuine requests sent by neighboring entities is being reduced. To create a UDP flooding attack, we modified one UDP-sender to launch a flooding process after 600 s so as to send a large amount of UDP packets per second (10 pkts/sec), and thus deplete the UDP-server's resources. We created three different scenarios to study the behavior of the network under UDP flooding attack. In each scenario, the attacker is located in a different place in the network. In particular, we have:

Malicious Scenario 1

Mote, m2, is the attacker and has a direct connection to the UDP server, without any relying mote in the middle, as shown in Fig. 2.

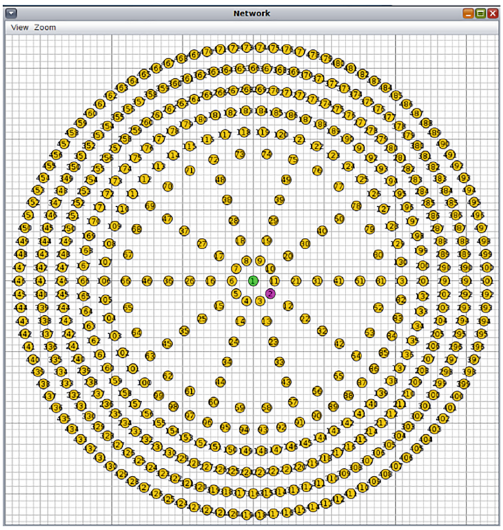

Fig. 2. Malicious Scenario 1: Direct connection between the attacker, m2, and the UDP server.

Malicious Scenario 2
Mote, m86, is the attacker and is placed in the middle of the network, as shown in Fig. 3.

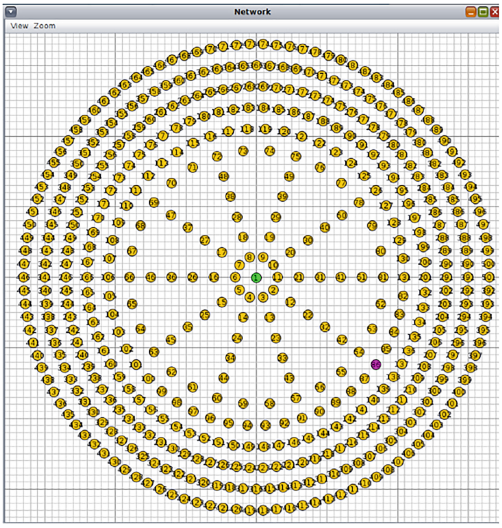

Fig. 3. Malicious Scenario 2: The attacker, m86, is placed in the middle of the network.

Malicious Scenario 3
Mote, m88, is the attacker and is placed in the ring where the neighbors can connect to server through different paths, as shown in Fig. 4.

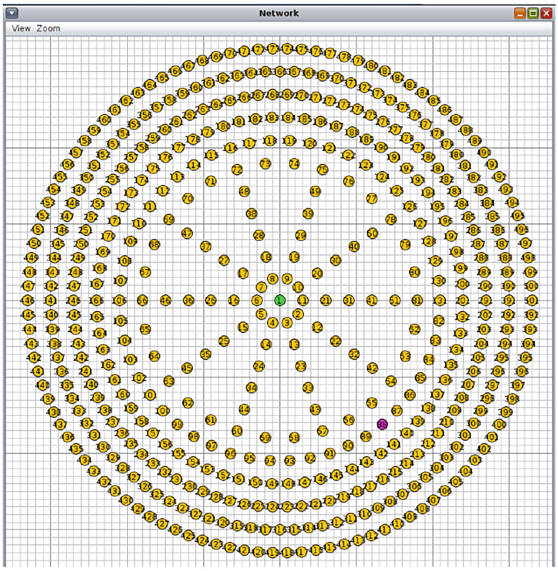

Fig. 4. Malicious Scenario 3: The attacker, m88, is placed in the ring where the neighbors can connect to server through different paths.

From the above 4 scenarios (i.e., 1 benign and 3 malicious), we collected the UDP packets sent by every mote as well as the received packets by the UDP-server from each mote in the network. Based on the sent packets, received packets, and the packet loss, we created a dataset, saved in a CSV file, for each scenario.

3 Flooding Attack Behavioral Models

We used the Python language and the Scikit-Learn library [10] to develop the appropriate Python script to perform the training and testing of the following Machine Learning (ML) algorithms used for modeling and prediction: Logistic Regression (LR), K-Neighbors Classifier (KNN), Classification And Regression Trees (CART), Gaussian Naïve Bayes (NB), and Support Vector Machine (SVM). The Python script trains and tests 5 models based on the above 5 ML algorithms for all 4 scenarios (i.e., 1 benign and 3 malicious).

We have used the metrics of accuracy, precision, recall, and F1-score to evaluate our models. The definition of each metric is given below:

- *Accuracy:* demonstrates the overall success of the model based on the following equation:

$$\frac{True\ Positive + True\ Negative}{True\ Positive + True\ Negative + False\ Positive + False\ Negative} \quad (1)$$

- *Precision:* demonstrates the overall effectiveness of the model based on the following equation:

$$\frac{True\ Positive}{True\ Positive + False\ Positive} \quad (2)$$

- *Recall:* demonstrates the overall success of the model based on the following formula:

$$\frac{True\ Positive}{True\ Positive + False\ Negative} \tag{3}$$

- *F1-score:* takes into consideration the precision and recall metrics and is calculated by the following formula:

$$\frac{2 \times (Recall \times Precision)}{Recall + Precision} \tag{4}$$

Regarding Accuracy, the following results were obtained as shown in Table 1.

Table 1. Accuracy.

Model	Accuracy			
	Benign Scenario	Malicious Scenario 1 – m2	Malicious Scenario 2 – m86	Malicious Scenario 3 – m88
LR	0.97	0.67	0.89	0.9
KNN	0.99	0.99	1.0	0.97
CART	1.0	0.99	1.0	1.0
NB	0.94	0.99	1.0	1.0
SVM	1.0	0.99	1.0	0.97

Regarding Precision, the following results were obtained as shown in Table 2.

Table 2. Precision.

Model	Precision			
	Benign Scenario	Malicious Scenario 1 – m2	Malicious Scenario 2 – m86	Malicious Scenario 3 – m88
LR	0.97	0.5	0.82	0.83
KNN	0.99	0.98	1.0	0.97
CART	1.0	0.99	1.0	1.0
NB	0.89	0.99	1.0	1.0
SVM	1.0	0.99	1.0	0.97

Regarding Recall, the following results were obtained as shown in Table 3.

Table 3. Recall.

Model	Recall			
	Benign Scenario	Malicious Scenario 1 – m2	Malicious Scenario 2 – m86	Malicious Scenario 3 – m88
LR	0.97	0.67	0.89	0.9
KNN	0.99	0.99	1.0	0.97
CART	1.0	0.99	1.0	1.0
NB	0.94	0.99	1.0	1.0
SVM	1.0	0.99	1.0	0.97

Regarding F1-score, the following results were obtained as shown in Table 4.

Table 4. F1-score.

Model	F1-score			
	Benign Scenario	Malicious Scenario 1 – m2	Malicious Scenario 2 – m86	Malicious Scenario 3 – m88
LR	0.97	0.57	0.85	0.86
KNN	0.99	0.99	1.0	0.97
CART	1.0	0.99	1.0	1.0
NB	0.92	0.99	1.0	1.0
SVM	1.0	0.99	1.0	0.97

Furthermore, we calculated the prediction of the packet loss for the first 100 motes, which are closer to the server, for all 5 models. The corresponding Box Plots for packet loss prediction for each scenario are shown below in Figs. 5, 6, 7, and 8.

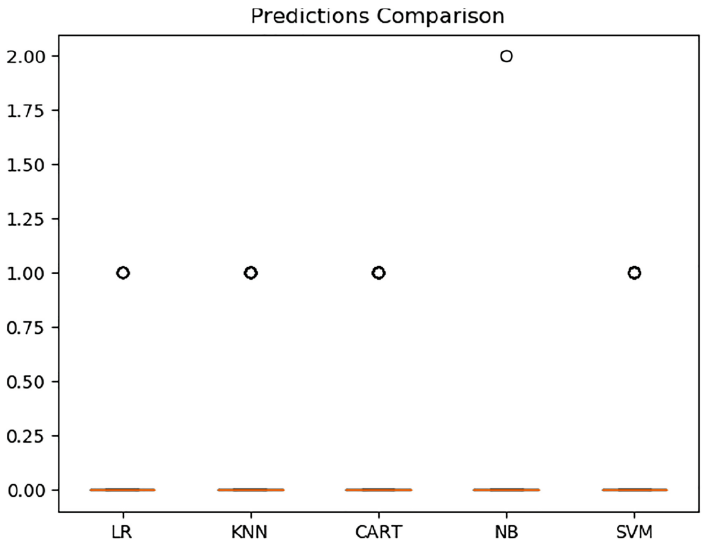

Fig. 5. Packet Loss Prediction Box Plot – Benign Scenario.

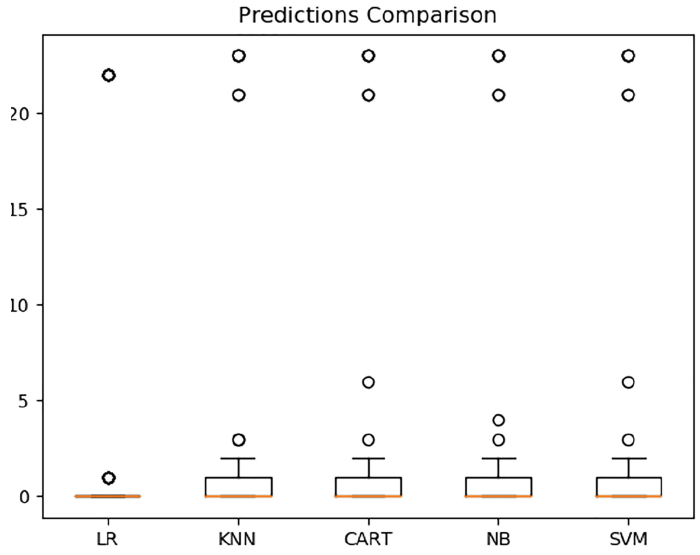

Fig. 6. Packet Loss Prediction Box Plot – Malicious Scenario 1 – m2.

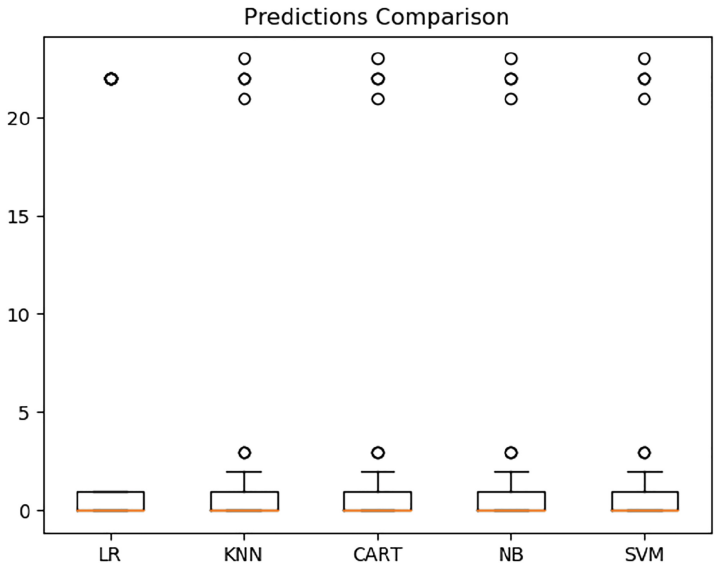

Fig. 7. Packet Loss Prediction Box Plot – Malicious Scenario 2 – m86.

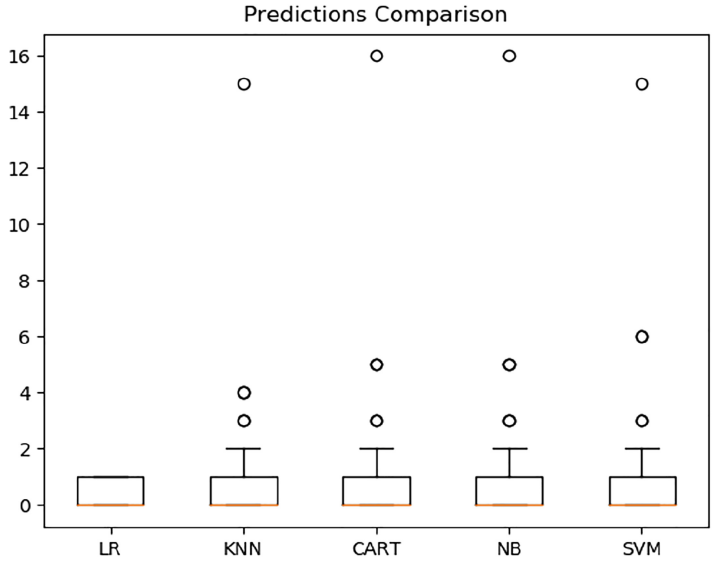

Fig. 8. Packet Loss Prediction Box Plot – Malicious Scenario 3 – m88.

Based on the above Box Plots for all scenarios, it can be seen the increase of the packet loss for the malicious scenarios compared to the benign scenario that can facilitate the prediction of potential flooding attack in the massive IoT network. However, in order to get better results, the size of the dataset that we used for the current work should be

extended in terms of the number of features (e.g., duty cycle of each mote). This will lead to more precise attack behavior models for more comprehensive understanding of the behavior of the flooding attacks over time and better prediction of their behavior.

4 Conclusion and Future Work

In this work, we presented attack behavior models of flooding attacks, developed in the EU-funded Marie Sklodowska-Curie REACT project, against massive IoT networks. These models, based on Machine Learning algorithms, are important for analyzing and getting a comprehensive understanding of the behavior of the flooding attacks over time in order to predict their behavior and extract design specifications for more robust AIDSs. Based on the performance evaluation of the developed models, it was concluded that the number of features of the dataset that we used for the current work should be increased with new features such as the duty cycle of each mote. As future work, we plan to enhance our existing dataset with additional features and use the new dataset for developing models with increased performance that will allow the extraction of design specifications for more robust AIDSs.

Acknowledgments. This research work was funded by the European Union's Horizon Europe research and innovation programme under the Marie Sklodowska-Curie grant agreement No 101069053 (REACT project).

References

1. Guo, F., et al.: Enabling massive IoT toward 6G: a comprehensive survey. IEEE IoT J. **8**(15), 11891–11915 (2021)
2. Porambage, P., et al.: The roadmap to 6G security and privacy. IEEE Open J. Commun. Soc. **2**, 1094–1122 (2021)
3. Lin, J., et al.: A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE IoT J **4**(5), 1125–1142 (2017)
4. Esra, A., Almaiah, M.A., Aljughaiman, A.: Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms. Sensors **24**(2), 713 (2024). https://doi.org/10.3390/s24020713
5. Bhavsar, M., Roy, K., Kelly, J., et al.: Anomaly-based intrusion detection system for IoT application. Discov. Internet Things **3**, 5 (2023). https://doi.org/10.1007/s43926-023-00034-5
6. Javanmardi, S., Ghahramani, M., Shojafar, M., Alazab, M., Caruso, A.M.: M-RL: a mobility and impersonation-aware IDS for DDoS UDP flooding attacks in IoT-Fog networks. Comput. Secur. **140**, 103778 (2024). https://doi.org/10.1016/j.cose.2024.103778. ISSN 0167-4048
7. Lee, S.-H., Shiue, Y.-L., Cheng, C.-H., Li, Y.-H., Huang, Y.-F.: Detection and prevention of DDoS attacks on the IoT. Appl. Sci. **12**(23), 12407 (2022). https://doi.org/10.3390/app122312407
8. Kumari, P., Jain, A.K.: A comprehensive study of DDoS attacks over IoT network and their countermeasures. Comput. Secur. **127**, 103096 (2023). https://doi.org/10.1016/j.cose.2023.103096. ISSN 0167-4048
9. Osterlind, F., et al.: Cross-level sensor network simulation with Cooja. In: Proceedings of the 31st IEEE Conference on Local Computer Networks, Tampa, FL, USA (2006)
10. Pedregosa, F., et al.: Scikit-learn: machine learning in python. J. Mach. Learn. Res. **12**(85), 2825–2830 (2011)