A Survey on Layered approach to securing IoT against DoS/DDoS attacks using machine learning techniques

Atanu Kumar Dey
Dept. Computer Science and Engineering
University Of Chittagong
Chattogram, Bangladesh
atanudey.csecu@gmail.com

***Abstract*—Internet of Things (IoT) is one of the continuously growing networking fields in this technological era which is based on a wireless network connecting billions of smart devices and people. With this growing, security threat on this technology is also increasing, as a result, we are experiencing cyber-attack like Mirai affecting a large infrastructure of the internet. In recent times some of the most common malicious attacks were of this type which is, in general, known as Denial of service (DoS), and Distributed Denial of Service (DDoS) attacks. Because of the limited resource of IoT devices, securing them from malicious attacks is a very challenging task. Due to the complexity and complexity of DDoS attacks these days, conventional threshold-based detection methods are no longer valid and reliable while the development of artificial intelligence (AI) in recent years has led to the use of Machine Learning models to improve DDoS attack detection. Despite all odds researchers, are studying new processes to develop effective detection and mitigation methods to secure IoT against DDoS attacks. To develop this kind of method, a deep understanding of the existing methods that have been used in the detection of DDoS attacks in the IoT environment is necessary. This survey highlights some of the latest Machine Learning (ML) techniques developed to detect DDoS attacks on different layer of IoT architecture, their advantages, and disadvantages, Comparisons between the performance of selected methods are also provided.**

Keywords— Internet of Things (IoT), Denial of Service (DoS),Distributed Denial of Service (DDoS) attack, Machine learning (ML), DDoS detection, DDoS mitigation.

I. Introduction

Internet of Things (IoT) is a platform with a wide range of devices including, smartphones, computers, cameras, wearable devices, micro-sensor-based monitoring systems, smart home appliances, etc. Internet of Things (IoT) have become a prevalent system in which people, processes, data, and things connect to the Internet and each other. According to Cisco annual internet report, globally, M2M connections will grow to 14.7 billion by 2023. There will be 1.8 M2M connections for each member of the global population by 2023 [1].With the expansion of IoT into different domains and areas, it can be used to support decision-making and improve the quality of our lives. These areas include communications, health care, industry, military and operational applications, power generation and distribution, transportation, surveillance, sustainable agriculture, and emergency response to natural and man-made disasters. [2], [3]. But a growing security issue and malicious attack like Denial of Service (DoS) and Distributed Denial of Service(DDoS), one of the most highlighted and most important attacks of today's cyberworld making adaption of those system challenging. With simple but extremely powerful attack mechanisms, DDoS introduces an immense threat to current Internet community.

Typically, in a DDoS attack, the attacker floods the targeted network with large spam requests that try to exceed the server hosting capacity and block the process of standard requests from legitimate users. A DDoS can be classified as a Bandwidth depletion attack and Resource depletion attack [4]. In the first one attacker tries to consume all the network's bandwidths using an attacking army while the resource depletion attack is intended to deprive the user of his memory, CPU, and socket. Due to lack of necessary security protocol, low computational power non-legacy IoT devices becomes an easy target to create botnet for a DDoS attack and the world has been repeatedly shown that IoT devices are vulnerable to being used as a platform to perform DDoS attacks, e.g. the Mirai botnet on KerbsOnSecurity in 2016 [5] and other recent IoT botnets like Reaper [6]. In a DDoS attack due to its distributed nature, it becomes difficult to track the source from the incoming traffic flood [7].

Many existing research has used Machine learning techniques for different classification and detection process in different domain. And many of them has shown optimistic results for detecting illegal network traffic indicating DoS or DDoS attack in different layer of IoT infrastructure. This study has tried to review some of those work.

II. Background

Three-layer architecture is considered as an essential IoT architecture. As name stands, it basically consists of three layers: perception layer, network layer, and application layer [9]. During a DDoS attack attacker may exploit in one or multiple layers. To prevent an attack successfully a system should have a multi-layer protection system. Researchers have

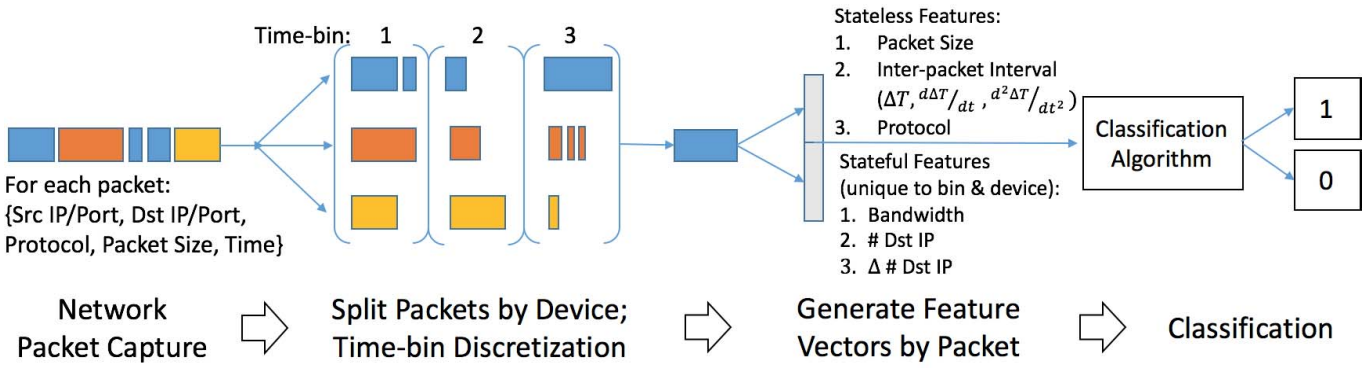

Fig. 1. Approach1 Pipeline [8]

suggested different protection and detection frameworks that can be applied in a single or multiple layers of an architecture.

In this study some of the existing approaches to prevent DDoS attacks in different layer have been reviewed. Those approaches mainly use different features of IoT combining with machine learning for detection and prevention purpose. Approach1: Uses IoT specific network characteristics at the edge of IoT network where physical devices connects with server using network middleboxes. [8], Approach2: Detects source of anomaly in IoT networks consisting of WSNs. [10], Approach3: A honeypot based approach in IoT network layer. [11], Approach4: SDN based network architecture [12]. Approach5: Multi agent intrusion detection system using Naive Bias classification technique in IoT perception layer [13].

A. Approach1 Review

In this study, R. Doshi et al. [8], developed a supervised machine learning-based anomaly detection pipeline shown in Fig.1 to detect local IoT device sources of DDoS attacks in-home gateway routers or other network middleboxes like routers, network switches, firewalls. This pipeline consists of four phases that perform 1. Traffic capture 2. Packet grouping by device and time 3. Feature extraction, 4. Binary classification using well-known ML classifiers like KNN, LSVM, DT, and Random Forest. And a four-layer fully-connected NN. As a binary classifier, it classifies the data as normal traffic or attack traffic.

The pipeline is flow-based and protocol-agnostic. The features were designed in a way that can be collected from specific behaviors of the IoT network and its flow characteristics like inter-packet intervals, protocol, and packet length. For feature, extraction authors have used two classes stateless and state-full. The stateless feature is derived from flow-independent characters of single packets. As a stateful feature, average network bandwidth, individual destination IP address, and its changes in time are used. Authors have found stateless features perform better than stateful features from the Gini impurity score which indicates that real-time anomaly detection of IoT attack traffic could be practical as the stateless features are lightweight and derived from network-flow characteristics where's adding stateful features with it improves accuracy.

For training and testing of classifiers, authors have generated training and testing datasets consisting of normal and attack traffic by simulating a local network of IoT devices. For the implementation of the ML classifiers, they have used Scikit-learn Python's library and Keras library (for NN). These classifiers identify non-legal traffic with an accuracy rate ranging between 0.991 and 0.999. The authors found that K-nearest neighbors produce the best detection when random forest and neural network classifier also performs well.

B. Approach2 Review

In this work, Aysa et al. [10] proposed the framework of Fig.2 for detecting infected devices by DDoS attack from a Wireless Sensor Network (WSN) using machine learning and data mining algorithms such as LSVM, Decision tree, and Neural Network. The authors also mentioned the use of standard datasets considered as big data from two of the most common IoT botnet attacks BASHLITE and Mirai for training the machine learning models. The framework is further divided into four phases, 1. data preparation, 2. data preprocessing, 3. learning and training over the normal and abnormal dataset, 4.testing and evaluations.

For training data authors has used three standard sets of benign normal and malicious data downloaded from UCI. This data was prepared by using information from Wi-Fi-associated IoT camera gadgets. Then command & control server and scan server is used to scan vulnerabilities and load attacks. By analyzing BASHLITE and Mirai attacks normal and attack data was collected at different time intervals in CSV format [14]. For getting more finer and normalized data min-max scaling technique is used and the negative impact of marginal values is reduced. Then 40 key features were selected for the training of machine learning models using the Pearson coefficient technique from 115 highlights which was selected by utilizing network protocol, IP address, MAC address, and communication channels. Open-source WEKA software is used to train machine learning algorithms such as Decision Tree (J-48), Linear SVM, Neural Network (Backpropagation), Random Forest on the dataset. Comparing those implementa-

tions authors have found that the merge between random forest and decision tree achieved high accuracy to detect attacks. The accuracy or true positive values of different models ranges between 89.7% to 99.7% depending on model and datasets where LSVM was producing less accuracy comparatively which reflects the nonlinearity of data.

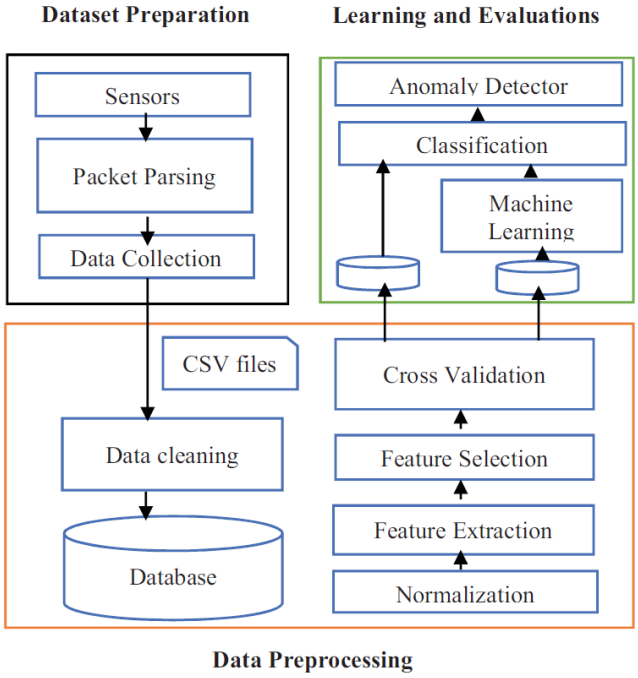

Fig. 2. Approach2 Framework [10]

C. Approach3 Review

A honeypot-based approach which uses machine learning techniques for detecting DDoS attack malware was proposed by Vishwakarma & Jain [11] in this study. Where data generated by the IoT honeypot is used to train machine learning dynamically. The advantage of using honeypot over datasets to train the model by unknown variants of malware families that wasn't possible using limited known data. To sustain this advantage, authors have mentioned the uses of unsupervised learning over supervised learning also may remove any human intervention if needed. While concentrating over detecting malware this work was also studied the identifying of the unknown malware families responsible for Zero-Day DDoS attacks using clustering feature of unsupervised learning.

The framework begins to work when an attacker tries to exploit the exiting vulnerability presented in IoT virtual honeypot. Then the data collected by the honeypot as log files which includes information like malware families, their variants, type of targeted devices, C&C servers IP address, port number are transformed into tabular data with minimum possible memory and is used to train the machine learning model. For the implementation of machine learning model authors have mention the process proposed by R. Doshi et al. which is described in Approach 1. Authors have proposed to implement the framework using IoT honeypot inspired by the ThingPot [15] over every IoT device in a network and router level implementation of machine learning classifier.

D. Approach4 Review

In this work, Bakker et al. [12] studied the achievement of using machine learning for detecting DDoS with the assistance of Software-Defined Networking (SDN), which is a new technology that aims to improve network management by centralizing network information and control. For implementing ML algorithms, NMETA2 was used and ML models were evaluated on a physical network testbed to show their efficiency especially in removing infected network traffic accurately during a DDoS attack. Where existing ML-based DDoS intrusion detection system (IDS) focuses on identifying legitimate traffic, and sometimes misclassifying nonlegitimate traffic, causing un-intentional degradation of performance for normal network traffic. Besides that, there could be a lot of data loss that may cause poor performance of the ML classifier.

To address such issues the authors have used ML techniques to detect DDoS attacks in online network settings and demonstrated how statistical could be employed in an SDN environment for detecting DDoS attacks. In this study author's goal was to use the existing ML models in an SDN environment without creating a new approach. For this, they have selected seven methods: Quadratic Discriminant Analysis (QDA), Linear Discriminant Analysis (LDA), Support Vector Machine (SVM), Naive Bayes, k-nearest neighbors (KNN), Random Forest and Decision Tree. From these classifiers, they have selected three classifiers and integrated them with nemeta2 in an offline environment. Then the methods were integrated with the features of network traffic, which includes two statistical properties of network traffic flows, 1) connection duration, and 2) quantity of data sent in one direction. And finally assessed on a physical network testbed by repeating a scenario of a DDoS attack. Selected network characteristics can be utilized to describe both normal and adverse behavior during a DDoS attack. A DDoS attack results in a large number of packets/data being sent over during a smaller amount of time compared to normal network traffic.

E. Approach5 Review

In this work, Mehmood et al. [13] proposed a Naive Bayes Classifier-Multi-agent Intrusion Detection System (NBC-MAIDS) which uses a machine learning-based classification algorithm to detect and prevent DDoS attacks on IoT platforms. The detection system implements the Naïve Bayes algorithm with the help of agents spreading through the nodes of the IoT ecosystem. These agents collect information using sensors indicating their position in the physical layer of IoT architecture. These agents independently gather data and communicate with other agents of the network and work as a whole system to perform any deployed task. Depending on the task these agents are mobile or stationary in a platform. In characteristics, each agent has its intelligence and is capable of

communicating with others also cooperative and rational. The detection system includes four types of agents 1. Collector agent, 2. System monitoring agent, 3. Actuator agent, 4. Communication agent. These agents monitor the nature of the traffic and the management of nodes. Multi-agents are deployed to audit the network traffic, classify if the incoming packet is an attack packet or not, drop the attack packet and manage the traffic database, and communicate with other agents to monitor the detection results and inquire about further information.

This is a three-phase model. In the first phase system processes some domain knowledge, attack graphs using WEKA based selection mechanism and collects the data for the classification algorithm. In the second phase data from the first phase is analyzed by the distributed agents throughout the network with the help of a predefined algorithm and an inference analyzer. Afterward, the data is classified for detecting malicious traffic. Then the attack can be prevented by reporting the status to the control system or network administrator.

III. Analysis

In Approach 1 [8] the study shows a good performance of the classifiers using the specific behaviors of IoT network. Also, the application of machine learning at the edge infrastructure of the IoT network layer for securing it against DDoS using low-dimensional features and simple algorithms which use low computational power.

But for limiting computational overhead authors make some assumptions about the nature of the attack while mimicking the attack traffic. Such as using a large number of packet-sized packets and TCP protocol instead of UDP, which may affect performance in real-life applications, where attack traffic can be constructed as normal traffic. The authors assume that the network includes a wireless device, which can monitor, store and block any network traffic that exceeds its path. The authors also speculate that the period of the DoS attack time is 90 seconds. We recognize that if any of these assumptions are not met, then this pipeline may not work.

By analyzing the work of Approach 2 [10] we can conclude author's major intention was to implement different supervised machine learning classification using different DDoS attack datasets and make a comprehensive analysis of them. While having so many similarities with the previous approach this study has worked with big data and the framework designed with consideration of low specification of IoT makes a new direction for any future work.

In recent time most of the industrial grade DDoS protection system uses honeypot approach because of its efficiency of simulating sudo infected environment resulting a false attack success report to attacker. But this system is costly as it need a big infrastructure with current technology [4]. Approach 3 [11] work suggest us a fusion of machine learning with it which may make the technology cost effective and produce a better detection and mitigation system. In this work at the beginning authors have preferred the use unsupervised machine learning in their study but after studying the work of R. Doshi et al. it doesn't reflect so as the last-mentioned work doesn't include any unsupervised learning.

Approach 4 [12] work illustrates how statistical classification could be deployed using SDN for detecting DDoS attacks. However, for implementation purposes, while selecting a statistical classifier to classify traffic authors, have suggested taking careful consideration to get the smallest possible packet processing overhead. By offering a centralized control plane, versatility within network management, security, and quality service SDN made itself an attractive platform for detecting DDoS attacks. Though in approach shows a high Detection Rate but it also indicates a possibility of misclassification. While in this work despite the low Detection rate the mean false-positive rate was between 0.3% and 3%.

The work also indicates SVM has the least significant impact on the data processing, while the processing time of Random Forest suggests it is less considerable for practical implementation. An active DPAE and SVM classifier combined system provided the best DDoS detection accuracy in this study.These results suggested that statistical classification approaches can be used to decrease the number of misclassified normal traffic.

In the last approach due to the distributed nature of Multi Agent System (MAS) the total computational load of the system is distributed among the different nodes of the network which makes this process easily employable in the low specs IoT devices, which also may reduce system cost as it would need additional infrastructure for protection purpose. Authors also compared NBC-MAIDS with the Bio-inspired Reputation, Trust Model (BRTM) WSN and Distributed Reputation-based Beacon Trust System (DRBT) model. Results showed that NBC-MAIDS outperformed other models in attack detection rate. The NBC-MAIDS strengthens other intrusion detection systems in detection accuracy using machine learning-based solutions by implementing multiple agents for accurate DDoS attack detection.

Table I shows a brief overview of features that is used to train machine learning models in those approaches. Except Approach3 all other approaches use similar type of feature. From section II we can see Approach 1 emphasizes on IoT specific features while also considering characteristics from network layer such as protocol, inter-packet intervals, and packet length. Approach 2 utilized some statistical features along with network specific features like weight, mean, and variance between two network streams. As Approach 3 used honeypot for collecting data, it includes various type of attack and malware specific data. Approach 4 utilized network traffic flows features which describe two statistical properties of traffic: the amount of information sent in one direction and the duration of a connection.

Table II shows accuracy comparison between four approaches but for Approach 3 authors didn't provide any evaluation data. From the table we can see all of ML algorithms has similar type of accuracy while KNN and NN algorithms performs best suggesting Neural Network can be used for the

TABLE I
FEATURE SELECTION OF DIFFERENT APPROACHES

Approach1	**Approach2**	**Approach3**	**Approach4**
• Packet Size • Inter-packet Interval • Protocol • Bandwidth • IP Destination Address Cardinality and Novelty • Variance of two stream	• Recent traffic from packet's host(IP) • Recent traffic to the packet's destination host • Time-frame • The weight of the stream • Variance of two stream • Mean of two stream	• Malware families • Malware variants • Type of targeted devices • C&C server IP address • Port Number	• Number of bytes sent by source • Number of bytes sent by destination • Number of packets sent by source • Duration of a bidirectional flow (secs) • Source Bytes per Packet • Destination Bytes per Packet

TABLE II
ACCURACY OF CLASSIFIERS IN DIFFERENT APPROACHES

Classifier	*Approach 1*	*Approach 2*	*Approach 3*	*Approach 4*
LSVM	.991	.897	-	-
SVM	-	.892 to .994	-	.934
KNN	.999	-	-	.925
DT	.999	.995 to .997	-	-
RF	.999	.997	-	.923
NN	.999	.984 to .996	-	-

TABLE III
DATA USED IN APPROACHES

	Datasets	**Data size**
Approach1	Generated from a Local network simulation setup	491,855 packets
Approach2	Philips Baby Monitor From Mirai and BASHLITE	70240 benign
	Provision Security Camera Data From Mirai and BASHLITE attack	62124 benign
	Simple Home Security Camera Data From Mirai and BASHLITE attack	19, 528 benign
Approach3	-	-
Approach4	Information Security Centre of Excellence (ISCX) at the University of New Brunswick (UNB)	571,698 samples

deployment of those approaches.

Each of ML classifiers has its own pros and cons: the construction nature of DT requires large storage, computational complexity for DT is high for large data, DT is still considered as a transparent method, simple, and easy to use. SVM knew of its generalization capability and appropriateness for data with a small number of sample points but a large number of feature attributes, SVM has some difficulties in interpreting its models. KNN is effective and popular for intrusion detection, however, using KNN classifier is challenging and time-consuming. RF is robust to overfitting but may be impractical in real-time specifically in applications where the required training dataset is big [8]. In the reviewed approaches these ML classifiers collaborative with other technologies to serve the purpose of DDoS attack detection for IoT networks. ML is a good choice for classifying non-legal network traffic in IoT since it can work with the unexpected and unstable behavior IoT and without the need for human intervention which is practical for IoT applications. ML techniques still have some challenges when used for IoT due to the computational and resource constraints and the large datasets needed for training [16], [17].

Table III shows different type of data sets used in approaches with their source and sizes.

IV. CONCLUSION

Primary goal of this survey was to review studies related to DDoS attack protection using Machine learning in different layer of IoT architecture. During the survey a common finding was most of the study focused on building a protection in network layer either it is in edge of the network where IoT devices connects with larger operating network through some intermediate devices or in server level. But by the acquired knowledge during this survey there is barely any studies that suggests a full protection architecture that includes all layer of IoT architecture. But fundamentally a DDoS attack on IoT starts by creating a botnet from malware infected IoT devices proceeding to servers through each middle layer. And there need more study to develop a solution that will protect the system at any layer.

REFERENCES

[1] "Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper." [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[2] M. Anirudh, S. A. Thileeban, and D. J. Nallathambi, "Use of honeypots for mitigating dos attacks targeted on iot networks," in *2017 International conference on computer, communication and signal processing (ICCCSP)*. IEEE, 2017, pp. 1–4.

[3] A. Zappone, M. Di Renzo, and M. Debbah, "Wireless networks design in the era of deep learning: Model-based, ai-based, or both?" *IEEE Transactions on Communications*, vol. 67, no. 10, pp. 7331–7376, 2019.

[4] M. M. Salim, S. Rathore, and J. H. Park, "Distributed denial of service attacks and its defenses in iot: a survey," *The Journal of Supercomputing*, vol. 76, no. 7, pp. 5320–5363, 2020.

[5] "IoT Botnet To Blame for Big DDoS Attack," Oct. 2016. [Online]. Available: https://www.sdxcentral.com/articles/news/iot-botnet-blame-big-ddos-attack/2016/10/

[6] L. Urquhart and D. McAuley, "Avoiding the internet of insecure industrial things," *Computer law & security review*, vol. 34, no. 3, pp. 450–466, 2018.

[7] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[8] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," in *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018, pp. 29–35.

[9] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, "Iot architecture challenges and issues: Lack of standardization," in *2016 Future technologies conference (FTC)*. IEEE, 2016, pp. 731–738.

[10] M. H. Aysa, A. A. Ibrahim, and A. H. Mohammed, "Iot ddos attack detection using machine learning," in *2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*. IEEE, 2020, pp. 1–7.

[11] R. Vishwakarma and A. K. Jain, "A honeypot with machine learning based detection framework for defending iot based botnet ddos attacks," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2019, pp. 1019–1024.

[12] J. N. Bakker, B. Ng, and W. K. Seah, "Can machine learning techniques be effectively used in real networks against ddos attacks?" in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2018, pp. 1–6.

[13] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. Malik, "Nbc-maids: Naïve bayesian classification technique in multi-agent system-enriched ids for securing iot against ddos attacks," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 5156–5170, 2018.

[14] A. H. Mohammed, A. M. Shantaf, and M. Khalaf, "The probe into reflection mobile radio propagation," in *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. IEEE, 2020, pp. 1–4.

[15] M. Wang, J. Santillan, and F. Kuipers, "Thingpot: an interactive internet-of-things honeypot," *arXiv preprint arXiv:1807.04114*, 2018.

[16] M. Mamdouh, M. A. Elrukhsi, and A. Khattab, "Securing the internet of things and wireless sensor networks via machine learning: A survey," in *2018 International Conference on Computer and Applications (ICCA)*. IEEE, 2018, pp. 215–218.

[17] K. Wehbi, L. Hong, T. Al-salah, and A. A. Bhutta, "A survey on machine learning based detection on ddos attacks for iot systems," in *2019 SoutheastCon*. IEEE, 2019, pp. 1–6.