A Survey on Dos And DDoS Attack In Internet of Things

Enosh Shaoul[1], Prof. Satendra Sonare[2]
[1]Dept of CSE
[2]Professor, Dept of CSE
[1, 2] Gyan Ganga Institute of Technology and Sciences, Jabalpur, Madhya Pradesh, India.

Abstract- *The significant progress in computing and communications devices became a part of people's lives, and a new revolution has emerged called internet things, a modern technology for connecting ordinary devices to the Internet and interacting between them for human comfort, that most methods in the Internet things are used legally. Still, the attackers may use DOS attacks to block the use of devices. However, securing the IoT system from malicious attacks is a very challenging task. Some of the most common malicious attacks are Denial of service (DoS), and Distributed Denial of service (DDoS) attacks, which have been causing major security threats to all networks and specifically to limited resource IoT devices. As security will always be a primary factor for enabling most IoT applications, developing a comprehensive detection method that effectively defends against DDoS attacks and can provide 100% detection for DDoS attacks in IoT is a primary goal for the future of IoT. The development of such a method requires a deep understanding of the methods that have been used thus far in the detection of DDoS attacks in the IoT environment. In our survey, we try to emphasize some of the most recent approaches developed for the detection of DoS and DDoS attacks in IoT networks.*

Keywords- Detection of DoS and DDoS, Internet of Things,

I. INTRODUCTION

The Internet has established itself as a platform that drives economic and technological development in every country in the world. In the information era, the network is seen as a natural destination for offering products and services due to its worldwide reach. The number of new devices connected to the World Wide Web has increased substantially in recent years. High-speed mobile communication helped this phenomenon through smartphones and tablets, joined with the popularization of IoT devices. At this juncture, it is estimated that 50 billion of IoT devices will be connected to the Internet by 2020 [1], with an upward trend in the number of Mobile-to-Mobile (M2M) [2] because of the growing demand for services that operate on IoT networks, especially in the context of smart cities. Besides, the emergence of wearable devices will impact this growth, with the prospect of about 1.1 billion such devices connected to the network by 2022 [2]. While this new environment has undoubtedly introduced advances to online services, it has also brought concerns and new challenges related to the safe operation of the Internet. One of the main issues is related to the weak security of IoT devices, which has facilitated the use of these devices as vectors of cyber attacks, mainly for Denial of Service (DoS) attacks [1]. Distributed Denial of Service (DDoS) attacks using IoT devices has been catching the attention of cybersecurity experts since 2016 [1]. That year, four hundred thousand devices, including cameras and wireless routers, were infected with the Mirai malware and formed a massive botnet that paralyzed the Internet with an orchestrated DDoS attack, breaking the traffic record associated with a single event. More recently, new and more dangerous malware, such as Hajime and IoT Reaper [1], have been identified on the network, indicating an even greater tendency to use IoT technology as a vector for DDoS attacks. Although the academic community and researchers from specialist companies have been working on the topic, there is still no consensus on the solution to the problem of DDoS attacks, especially when the source of the attacks is IoT equipment. In general, although the solutions proposed by the academy are scientifically secure, they do not present practical requirements for deployment on the Internet [3]. In contrast, commercial solutions are not effective in the context of IoT [3], as the attack will eventually lead to resource depletion of corporate network input equipment. Thus, the investigation of DDoS attack detection and mitigation techniques in the context of IoT networks is currently of great interest in the area of network security, whose solutions should significantly impact the availability of Internet services.

In the modern Internet age the use of networking for resources and services has become routine in everyone's daily life. Whether it is accessing one's social media, online banking, using cloud-based applications, or even simply resolving host names through DNS, relying on another company's resources has become the norm. However, when an attacker restricts our access to these resources through a Denial-of-Service attack, it not only affects our daily life, but

affects the business providing the resources. While DoS prevention services exist, the size and frequency of these attacks is increasing every year. This paper addresses the issue of DoS and DDoS attacks, presents examples of major attacks, and presents how the Internet of Things is making these attacks worse.

II. RELATED WORK

2.1 Background: The Internet has established itself as a platform that drives economic and technological development in every country in the world. In the information era, the network is seen as a natural destination for offering products and services due to its worldwide reach. The number of new devices connected to the World Wide Web has increased substantially in recent years. High-speed mobile communication helped this phenomenon through smartphones and tablets, joined with the popularization of IoT devices. At this juncture, it is estimated that 50 billion of IoT devices will be connected to the Internet by 2020 [4], with an upward trend in the number of Mobile-to-Mobile (M2M) [5] because of the growing demand for services that operate on IoT networks, especially in the context of smart cities. Besides, the emergence of wearable devices will impact this growth, with the prospect of about 1.1 billion such devices connected to the network by 2022 [5]. While this new environment has undoubtedly introduced advances to online services, it has also brought concerns and new challenges related to the safe operation of the Internet. One of the main issues is related to the weak security of IoT devices, which has facilitated the use of these devices as vectors of cyber attacks, mainly for Denial of Service (DoS) attacks [4].

Distributed Denial of Service (DDoS) attacks using IoT devices has been catching the attention of cybersecurity experts since 2016 [4]. That year, four hundred thousand devices, including cameras and wireless routers, were infected with the Mirai malware and formed a massive botnet that paralyzed the Internet with an orchestrated DDoS attack, breaking the traffic record associated with a single event. More recently, new and more dangerous malware, such as Hajime and IoT Reaper [4], have been identified on the network, indicating an even greater tendency to use IoT technology as a vector for DDoS attacks. Although the academic community and researchers from specialist companies have been working on the topic, there is still no consensus on the solution to the problem of DDoS attacks, especially when the source of the attacks is IoT equipment. In general, although the solutions proposed by the academy are scientifically secure, they do not present practical requirements for deployment on the Internet [6]. In contrast, commercial solutions are not effective in the context of IoT [6], as the attack will eventually lead to resource depletion of corporate network input equipment. Thus, the investigation of DDoS attack detection and mitigation techniques in the context of IoT networks is currently of great interest in the area of network security, whose solutions should significantly impact the availability of Internet services. Machine learning (ML) is quickly expanding in many fields, such as science, technology, marketing, education, healthcare, and many other fields. Recent anomaly detection research has shown the promise of machine learning for recognizing malicious Internet traffic [7]. Machine learning technique in cybersecurity is helpful by recommending the proper decision for analysis and even doing the proper action automatically. However, little effort has been made to valuate ML models with features geared explicitly towards IoT device networks or IoT attack traffic.

Recent works with the focus on securing against distributed denial of service attacks in the context of IoT networks is presented in this section, detailing different detection and mitigation techniques to place this work proposal in the state-of-the-art. The work proposed by Yin et al. [8] provides a framework called SD-IoT (Software-Defined - Internet of Things) and an attack detection algorithm that analyzes the similarity of input packet rate vectors in SD-IoT switch ports border. The proposed system calculates the similarity ($\rho x,y$) of the analyzed vector and compares it to a threshold value (ηU). If $\eta U \leq \rho x,y \leq 1$, SD-IoT switch will be under DDoS attack. The experiments were performed using the Mininet emulation tool [9]. However, the authors place devices only as targets for DDoS attacks, not as potential infected agents and originators of the attacks.

On the other hand, the work by Doshi et al. [10] presented a behavioral analysis of IoT network variables such as bandwidth, packet interval, protocols, packet size, and destination address. Also, the authors performed an analysis of several machine learning algorithms and validated the dataset generated by the authors. They ran tests with five algorithms: KNN (K-Nearest Neighbors), LSVM (Support Vector Machine with the linear kernel), DT (Decision Tree), RF (Random Forest), NN (Neural Network). In [11], it was used fog computing in the SDN environment to detect DDoS attacks from IoT devices. The authors proposed the Edge-Centric Software-Defined IoT Defense (ECESID), using SDN switches to defend DDoS attacks and enforcing traffic control rules near the source of the attack. The authors use a combination of two attack detection algorithms: Threshold Random Walk with Credit-Based Rate Limiting (TRW-CB) and Rate Limiting (RL). The authors used Mininet to emulate IoT networks and connecting devices, using the Mirai malware to infect IoT devices, analyzing the behavior of

infected devices, and mitigating attacks. At that work, the detection of infected devices occurs at the stage where these devices attempt to infect other healthy devices. This strategy can present a deficiency in the detection process, where infected devices are hibernating while waiting for the attack to take place or while performing DDoS attacks. In work presented by Hasan [12], a set of attack data and regular traffic in the literature was used. They also engineered the existing data, separating and clearing the variables. After this step, tests were performed with different machine learning algorithms, such as Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF) and Artificial Neural Network (ANN). The analysis was performed offline, that is, no detection or mitigation system was implemented, and only statistical metrics were obtained regarding the classification of the existing dataset. Another approach [13] presented a DDoS attack detection system using a network entropy analysis. The entropy variation of the destination IP address is measured using the Shannon equation. In the case of DDoS attacks, the entropy values fall compared to the values obtained in a network with regular traffic. Tests were performed by the authors using an SDN environment in Raspberry PI, with a POX controller to mitigate connections detected as an attack. In their work, false alarm rates, detection, and accuracy were not shown, and there are no comparisons with datasets present in the literature. In [14], the authors proposed a DDoS attack detection and mitigation system that integrates an Intrusion Detection System (IDS) into the client-side SDN architecture for home or organizational network scenarios. The system operates through loop control between three essential architectural components: the network, the IDS, and the controller. IDS analyze all exchanged traffic on the network, detecting ongoing DDoS attacks. The controller, when notified by IDS, transfers to the network devices some new flow rules to restore regular operation as quickly as possible. The authors use Snort as a detection solution, mirroring all port traffic, and deeply inspecting incoming packets. This type of approach proved to be efficient in the tests performed; however, by performing deep inspection, the solution becomes vulnerable in volumetric attacks.

2.2 Existing Comparison:

Security problems have become increasingly important with the spread of IoT devices. The Software-Defined Networking (SDN) paradigm provides a way to control IoT devices securely. For the IoT paradigm, we have suggested a general system for detecting and mitigating Distributed Denial-of-Service (DDoS) attacks using an SDN. The proposed architecture [15] consists of a pool of controllers comprising SDN controllers, IoT gateway-integrated. Also, we have offered an IoT DDoS attack detection and mitigation algorithm attached to the proposed SDN IoT platform. Finally, the proposed algorithm shows the experimental results that have improved performance and the proposed architecture adapts to heterogeneous and fragile devices to enhance IoT security.

To ensure that the information system can provide services for users normally, it is important to detect the occurrence of DDoS attacks quickly and accurately. Therefore, this research proposes [16] a system based on packet continuity to detect DDoS attacks. On average, it only takes a few milliseconds to collect a certain number of consecutive packets, and then DDoS attacks can be detected. Experimental results show that the accuracy of detecting DDoS attacks based on packet continuity is higher than 99.9% and the system response time is about 5 milliseconds.

One of the serious threats to IoT systems is known as denial of service (DoS) attack, which usually target broker services on that system. Several researches have been performed to overcome this DoS attack. However, the results appear to be ineffective. It can be seen that the accuracy of the DoS detection systems are still low. This study [17] aims to provide a solution to the above problems by proposing an Intrusion Detection System based on Artificial Intelligence (AI, AdaBoost) for IoT system. The method used in this study is supervised learning which measures the accuracy of predictions in detecting DoS on IoT network data. The experiments have been carried out on 130223 DoS attack data and 130284 normal data. The detection accuracy of the DoS detection is 95.84 % and the F1-Score is 95.72 %. Recall and precision have achieved 93.28% and 98.29%, respectively.

A Distributed Denial of Service (DDoS) attack is a lethal threat to web-based services and applications. These attacks can cripple down these services in no time and deny legitimate users from using these services. The problem has further prevailed with the massive usage of unsecured Internet of Things (IoT) devices across the Internet. Moreover, many existing rule-based detection systems are easily vulnerable to attacks. In this paper [18], we performed a comparative analysis of Machine Learning (ML) algorithms to detect and classify DDoS attacks. As part of the work, various machine learning algorithms such as Naïve Bayes, J48, Random Forest and ZeroR ML classifiers are compared. Principal Component Analysis (PCA) method has been used to select the optimal number of features. WEKA tool has been used to implement ML algorithms.

WSN is the prominent subpart of IoT. The routing protocol for low power and lossy networks (RPL) is the safest

alternative for WSN and it is mostly used at the network layer. DOS attacks are the most serious attacks that have arisen in all levels of the IoT. In this study [19], we determined the effectiveness of a selective forward attack which is a network layer DoS attack and on the basis of energy consumption and received packets by the nodes identifies the attacker location.

With help of software and system configuration threats are detected. Which can lead to possible vulnerability and we also wrote attack script which performs an attack on the system to detect if the attack can be done on the system by using software tool configuration error identified. The proposed system [20] identify the vulnerability of the architecture leads to Brute force attack and with the help of attacks script are able to find out if there are any open ports which could be used to exploit the system and also perform Dos & DDos attack to check if the system is vulnerable for it along with it we also check if the data stored in the IoT device is encrypted or not. Once the scan is complete a detailed report is sent to the user Email.

One of the most common cyber-attacks on such systems is Denial of Service (DOS)/Distributed Denial of Service (DDOS) attacks that threaten the availability of IOT services to users. Such a threat along with the challenges posed to secure IOT systems, encouraged researchers to investigate and implement DOS/DDOS detection models based on Machine Learning (ML) algorithms. This paper [21] aims to provide a review of some of the proposed ML models by researchers for detecting DOS/DDOS attacks where the focus of review is on the deployment methodology of the ML model, the detection methodology, the datasets used for training and testing the models, and performance.

The paper [22] aims to provide a summary with a reference to the Internet of Things (IoT) of the distributed denial of service (DDoS). The network research community has known about the denial of service (DoS), which is intended to stop legitimate users from accessing a particular network tool since the early 1980s. The aim of the paper is to define DDoS scope, classifications and opportunities for assailants who use IoT to conduct such operations and to use IoT in healthcare. The research approach is to analyze DDoS, IoT and the use of IoT literature in the health sector. The study found that DDOS attacks on IoT-specific devices have become a very easy phenomenon because network attacks are much simpler due to limited security protocols. IOT distribution companies have made limited efforts to enable security of these devices and protecting the data, thus making them susceptible to vulnerabilities. Due to weak security layers, the confidentiality, authenticity and integrity of private data collected by IoT devices are threatened by attackers. The current research identified the gap and importance for further research to provide a mechanism for detection and prevention of DDOS attack in the application layer of IoT healthcare devices in India. Considering the major challenges in IOTs in defending against external attacks and hacking, it is important that they have inherent frameworks warding off such attacks.

With the advancement of wired and wireless communication technologies, the Internet of Things (IoT) devices are also increasing. Hackers exploit a massive amount of IoT devices, which lack security protection for specific purposes. Distributed denial of service (DDoS) attack is an enhanced denial of service (DoS) attack and is one of these hacked devices' common usages. This paper [23] proposes a time-stamped bi-directional gated recurrent unit (GRU) model to detect DDoS attacks. Compared with previous work, our method maintains higher accuracy and lower training time. Generally, in most DDoS attack schemes, the accuracy is still high.

III. CONCLUSION

This paper presented the survey on some of the existing work for DoS and DDoS attacks in IoT networks. Detection-IoT system, a solution that uses machine learning to classify IoT network traffic and detect denial of service attacks by only analyzing the IoT traffic packets of network traffic samples, thus not compromising data privacy. The intention is to detect the attack as close as possible to the threat, allowing actions to be taken as quickly as possible to mitigate them.

REFERENCES

[1] N. Vlajic and D. Zhou, “IoT as a Land of Opportunity for DDoS Hackers,” Computer, vol. 51, no. 7, pp. 26–34, 2018.

[2] E. Summary, “Cisco public Cisco Visual Networking Index: Global Mobile Data Traffic The Cisco® Visual Networking Index (VNI) Global Mobile Data,” pp. 2017–2022, 2019.

[3] Y. Cao, Y. Gao, R. Tan, Q. Han, and Z. Liu, “Understanding Internet DDoS Mitigation from Academic and Industrial Perspectives,” IEEE Access, vol. 6, pp. 66 641–66 648, 2018.

[4] N. Vlajic and D. Zhou, “IoT as a Land of Opportunity for DDoS Hackers,” Computer, vol. 51, no. 7, pp. 26–34, 2018.

[5] E. Summary, “Cisco public Cisco Visual Networking Index: Global Mobile Data Traffic The Cisco® Visual Networking Index (VNI) Global Mobile Data,” pp. 2017–2022, 2019.

[6] Y. Cao, Y. Gao, R. Tan, Q. Han, and Z. Liu, "Understanding Internet DDoS Mitigation from Academic and Industrial Perspectives," IEEE Access, vol. 6, pp. 66 641–66 648, 2018.

[7] V. Chandola, A. BANERJEE, and V. KUMAR, "Survey of Anomaly Detection," ACM Computing Survey (CSUR), vol. 41, no. 3, pp. 1–72, 2009.

[8] D. Yin, L. Zhang, and K. Yang, "A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework," IEEE Access, vol. 6, no. Mcc, pp. 24 694–24 705, 2018.

[9] R. L. S. De Oliveira, C. M. Schweitzer, A. A. Shinoda, and L. R. Prete, "Using Mininet for emulation and prototyping Software-Defined Networks," in 2014 IEEE Colombian Conference on Communications and Computing, COLCOM 2014 - Conference Proceedings, 2014.

[10] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer internet of things devices," in Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018, 2018.

[11] M. Ozcelik, N. Chalabianloo, and G. Gur, "Software-Defined Edge Defense Against IoT-Based DDoS," IEEE CIT 2017 - 17th IEEE International Conference on Computer and Information Technology, pp. 308–313, 2017.

[12] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," Internet of Things, vol. 7, p. 100059, 2019.

[13] N. Sambandam, M. Hussein, N. Siddiqi, and C. H. Lung, "Network Security for IoT Using SDN: Timely DDoS Detection," DSC 2018 - 2018 IEEE Conference on Dependable and Secure Computing, no. January, pp. 1–2, 2019.

[14] P. Manso, J. Moura, and C. Serrao, "SDN-based intrusion detection ˜ system for early detection and mitigation of DDoS attacks," Information (Switzerland), vol. 10, no. 3, pp. 1–17, 2019.

[15] K. M. Shayshab Azad, N. Hossain, M. J. Islam, A. Rahman and S. Kabir, "Preventive Determination and Avoidance of DDoS Attack with SDN over the IoT Networks," 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI), 2021, pp. 1-6, doi: 10.1109/ACMI53878.2021.9528133.

[16] H. -C. Chu and C. -Y. Yan, "DDoS Attack Detection with Packet Continuity Based on LSTM Model," 2021 IEEE 3rd Eurasia Conference on IOT, Communication and Engineering (ECICE), 2021, pp. 44-47, doi: 10.1109/ECICE52819.2021.9645650.

[17] S. Rachmadi, S. Mandala and D. Oktaria, "Detection of DoS Attack using AdaBoost Algorithm on IoT System," 2021 International Conference on Data Science and Its Applications (ICoDSA), 2021, pp. 28-33, doi: 10.1109/ICoDSA53588.2021.9617545.

[18] A. Chopra, S. Behal and V. Sharma, "Evaluating Machine Learning Algorithms to Detect and Classify DDoS Attacks in IoT," 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), 2021, pp. 517-521.

[19] S. Sinha and K. G, "Network layer DoS Attack on IoT System and location identification of the attacker," 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), 2021, pp. 22-27, doi: 10.1109/ICIRCA51532.2021.9545071.

[20] H. S. Shreenidhi, S. Prabakar and P. A. Kumar, "Intrution detection system Using IoT device for safety and security," 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021, pp. 340-344, doi: 10.1109/ICCIKE51210.2021.9410730.

[21] M. A. Mahmood and A. M. Zeki, "Securing IOT against DDOS attacks using machine learning," 3rd Smart Cities Symposium (SCS 2020), 2020, pp. 471-476, doi: 10.1049/icp.2021.0905.

[22] M. Khatkar, K. Kumar and B. Kumar, "An overview of distributed denial of service and internet of things in healthcare devices," 2020 Research, Innovation, Knowledge Management and Technology Application for Business Sustainability (INBUSH), 2020, pp. 44-48, doi: 10.1109/INBUSH46973.2020.9392171.

[23] C. -Y. Chen, L. -A. Chen, Y. -Z. Cai and M. -H. Tsai, "RNN-based DDoS Detection in IoT Scenario," 2020 International Computer Symposium (ICS), 2020, pp. 448-453, doi: 10.1109/ICS51289.2020.00094.