China Petroleum Processing and Petrochemical Technology

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 343-351

MACHINE LEARNING APPROACHES TO DETECT DDOS ATTACK IN IOT NETWORK- A COMPREHENSIVE REVIEW

T Ramya

Research Scholar, Anurag Universty, Hyderabad, Telangana,India, 500010

2904ramy@2gmail.com,

Dr. A. Prasantha Rao

Associate Professor, Anurag University, Hyderabad,Telangana,India,500010-

prasanthraoit@cvsr.ac.in,

Abstract

As IoT networks continue to grow, so does the threat of DDoS attacks, which aim to disrupt networks by overwhelming them with traffic. IoT networks are particularly vulnerable due to numerous interconnected devices with limited security measures. Attackers exploit vulnerabilities in IoT devices, forming botnets to launch coordinated attacks. DDoS attacks on IoT networks can have severe outcomes, including service disruptions and data breaches. Preventing and mitigating DDoS attacks requires a multi-layered approach, including strong security practices, firmware updates, and network-level defences. ML algorithms can analyze network traffic patterns and detect anomalies, aiding real-time identification of DDoS attacks. However, ML-based detection systems need labelled training data and continuous monitoring to adapt to evolving attack techniques. Combining ML with other techniques forms a comprehensive DDoS defence strategy. This article gives a review of various methods and techniques proposed by different authors to detect a DDoS attack in IoT environment at a minimum amount of time.

Keywords: DDoS attack, ML Algorithms, IOT Environment

Introduction

As the Internet of Things (IoT) continues to grow, connecting billions of devices worldwide, it also introduces new security challenges. One significant threat is Distributed Denial of Service (DDoS) attacks targeting IoT networks. DDoS attacks main aim is to disrupt or disable the normal functioning of a network, system, or service by devasting it with a flood of traffic from multiple devices.

In IoT networks, DDoS attacks pose unique risks due to the large number of interconnected devices with limited computing resources and often insufficient security measures. These devices, ranging from smart home appliances to industrial sensors, can be compromised and used as part of a botnet—an army of infected devices controlled by malicious actors to carry out coordinated attacks.

The impact of DDoS attacks on IoT networks can be severe, leading to service disruptions, data breaches, and financial losses. Such attacks can target critical infrastructure, e-commerce platforms, or even IoT devices themselves, causing operational disruptions, loss of data integrity, and potential safety risks.

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 343-351

To initiate a DDoS attack in an IoT environment, attackers typically exploit vulnerabilities in IoT devices, such as weak or default passwords, outdated firmware, or insecure communication protocols. Once compromised, these devices can be used to generate massive amounts of traffic directed at a target, overwhelming its resources and rendering it inaccessible.

Preventing and mitigating DDoS attacks in IoT networks require a multi-layered approach. This includes implementing strong security practices for IoT devices, regularly updating firmware to patch vulnerabilities, using secure communication protocols, and deploying network-level defences such as firewalls, intrusion detection systems, and traffic filtering mechanisms.

Furthermore, network administrators can utilize traffic monitoring and anomaly detection strategies to identify and mitigate DDoS attacks in real-time. This may involve monitoring network traffic patterns, analysing flow data, and leveraging machine learning algorithms to detect abnormal traffic behaviour and automatically trigger countermeasures.

Machine learning (ML) algorithms can be employed to identify DDoS attacks in network traffic by leveraging their ability to analyse patterns, classify data, and detect anomalies. ML-based DDoS detection systems can help network administrators detect and react to attacks in real-time.

ML algorithms can enhance DDoS detection capabilities by automating the process and providing real- time insights. However, it is recommended to combine ML-based detection with other techniques, such as traffic analysis, flow-based monitoring, and signature-based detection, to create a comprehensive DDoS defence strategy.

Literature Review

In the [6] paper highlights the significance of SEs in improving the quality of living for users in various contexts such as Smart Campus, Smart Homes, Industry 4.0, and Smart Hospitals. However, the increased number of devices and the heterogeneity of SEs present challenges in terms of network management, planning, and security, particularly with respect to DDoS attacks.

The proposed Smart System for DDoS detection combines Fog and Cloud computing, with the tasks divided between these two architectures to enhance response time and accuracy. The environment follows a four- principle approach: (I) Network monitoring and data collection on network flows in SEs, (II) Feature selection to identify key characteristics for DDoS detection, (III) Traffic division to distinguish network flows from IoT machines andPD, and (IV) ML-based detection by training models using network flow data to identify DDoS attacks.

The experiments conducted using real-time IoT network traffic with DDoS attacks demonstrate the effectiveness of the proposed system. The system achieves a high accuracy rate of 99% when appropriate features are identified, while also minimizing data exchange capacity and detection time.

The contributions of this article include the design of a system that integrates cloud and fog computing, ahomework on the impact of feature selection on DDoS detection accuracy and data exchange volume, a traffic segmentation approach applicable to various management tasks in SEs, and experiments using real-time network traffic datasets with DDoS attacks.

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 343-351

In paper [7] the authors presents a stateful SDN (Software-Defined Networking) security solution for real-time IoT (Internet of Things) network data, focusing on the detection and removing of DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks. The proposed solution utilizes entropy as the detection technique, which offers improvements such as high sensitivity, low false positive rate, simplicity in entropy calculation, and no need for additional network devices.

Traditionally, SDN leverages Open Flow as an abstract of the data plane, where flow tables on switches are responsible for forwarding stateless packets according to rules defined by the controller. However, this approach can lead to signalling overhead and increased latency. To overcome this limitation, the paper introduces a stateful approach in SDN by incorporating some stateful logic in switches, allowing for more efficient handling of network traffic. This paper demonstrates that entropy-based mechanisms can be implementing effectively with real-time IoT traffic in stateful SDN architectures.

The experiments conducted in the paper involve three different scenarios using real data traffic from two datasets: "BigFlows" and "Bot-IoT". The "Bot-IoT" dataset is particularly suitable for network forensic analytics in IoT as it incorporates both legitimate IoT network traffic and traffic associated with DoS and DDoS attacks. The experimental scenarios involve various network topologies, including more complex ones, to assess the performance and effectiveness of the proposed solution in realistic settings.

The important points of the work can be potted as follows:

- Development of an entropy-based solution that operates effectively in a stateful SDN architecture, enabling both detection and mitigation of DoS and DDoS attacks.
- Use of real IoT traffic in the experimental scenarios, enhancing the realism and relevance of the results compared to studies using artificial traffic or non-IoT network traffic.

In conclusion, the paper presents an innovative stateful SDN security solution for detecting and mitigating DoS and DDoS attacks in real IoT traffic. The use of entropy-based mechanisms in conjunction with a stateful SDN architecture contributes to a more efficient and comprehensive defense against these security threats. The experiments conducted with real-time IoT traffic and complex network topologies validate the effectiveness of the proposed solution.

In paper[15] the authors introduces a novel detection and mitigation technique for IoT-based DDoS attacks, with a primary focus on stealthy attacks which exhibit a low data rate increase per machine(as low as 10%). These attacks are challenging to detect and can bypass most existing methodologies . The proposed method utilizes a statistical anomaly detection algorithm called Online Discrepancy Test (ODIT), which offers several advantages, including minimal interruption of regular service, scalability to large systems, independence from presumed baseline and attack patterns, and quick and accurate detection and mitigation due to its sequential nature.

The key insights of the paper are as follows:

1. Proposal of a novel detection and mitigation technique: The paper presents a new technique specifically designed to address stealthy DDoS attacks in IoT environments. The proposed

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 343-351

technique leverages the ODIT algorithm, which offers sequential detection and mitigation capabilities.

2. Analysis of time and space complexity: The time and space complexity of the proposed technique are analysed, providing insights into the computational requirements and resource utilization.

3. Asymptotic optimality: The paper demonstrates the asymptotic optimality of the proposed detector in the minimal sense as the size of the training data increases. This analysis ensures that the technique performs well even as the dataset size increases.

4. Solution for dynamic scenarios: The paper addresses dynamic scenarios where the number of devices in the network replaces over time. The proposed technique is adaptable to such scenarios, allowing for effective detection and mitigation in evolving IoT networks.

5. Comprehensive performance evaluation: The effectiveness of the proposed technique is evaluated through a comprehensive performance evaluation. This evaluation includes a testbed implementation, the use of the N-BaIoT dataset (a popular dataset for IoT network analysis), and simulations. The results of the evaluation provide insights into the detection accuracy, mitigation effectiveness, and overall performance of the proposed technique.

In summary, the paper presents a novel detection and mitigation technique for IoT-based DDoS attacks, focusing on stealthy attacks with low data rate increases per machine. The proposed technique, based on the ODIT algorithm, offers several advantages and addresses the challenges posed by these types of attacks. The paper provides a thorough analysis of the technique's time and space complexity, proves its asymptotic optimality, offers a solution for dynamic scenarios, and presents a comprehensive performance evaluation using real-world datasets and simulations.

In paper [10] work proposes an integrated detection mechanism called Smart Detection-IoT (SD-IoT) system to detect DDoS attacks in IoT network environments. The system architecture focuses on early detection of DDoS attacks at the source network. The proposed approach utilizes a sensor installed on the IoT network access point to classify online traffic using a Machine Learning (ML)-methodology strategy. The system is designed to be compatible with existing Internet infrastructure without requiring software or hardware upgrades, making it feasible for deployment. User data privacy is ensured throughout the system's operation as data fields are not accessed.

The important insights of this study are:

1. Modelling and validation of an online detection system: The study presents the modelling, coding, and validation of an online detection system specifically designed for DDoS attacks in IoT network scenarios. The system, SD-IoT, classifies online random samples of IoT network traffic as either DoS attacks or regular traffic while maintaining information privacy.

2. Exploration of network traffic properties: The study explores the properties of network traffic in the IoT network scenario and creates a new signature database based on the findings. This database aids in the detection of DDoS attacks.

3. Practical online processing: The study presents a practical strategy for processing and validating raw network traffic data in real-time. The proposed system is embedded in a wireless

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 343-351

AP and integrated into an SDN controller. It employs a signature-based machine learning algorithm to identify DDoS attacks. Network traffic samples collected by an OpenFlow switch are forwarded to the detection system for analysis.

4. Evaluation of classification algorithms: The study evaluates three classification algorithms - Logistic Regression (LR), Random Forest (RF), and Extreme Gradient Boost (XGB) - in the core of the detection system. The performance of these algorithms in detecting DDoS attack patterns is assessed.

[12] Research paper proposes an architecture for capturing and mitigating DoS/DDoS attacks in the context of the Internet of Things (IoT). The main contributions of the paper include the design and implementation of an architecture with two main components: DoS/DDoS detection and DoS/DDoS mitigation. The mitigation countermeasures are based on the detection decisions made by the system.

Unlike previous works that focused on distinguishing between normal traffic and attack traffic, the proposed detection approach takes into consideration the perspective of a cyber security analyst. It aims to identify subcategories of DoS/DDoS attacks and determine the corresponding mitigation countermeasures at a fine-grained level. The paper identifies six subcategories of attacks by combining two attack categories (DDoS and DoS) with three types of packets (TCP, UDP, and HTTP).

The proposed detection classification approach combines the concept of Looking-Back with basic classifiers to achieve accurate results. Based on the detection outcomes, specific mitigation countermeasures are applied. In the case of a DoS attack, specific traffic (HTTP, TCP, or UDP) from a particular IP address is denied, while allowing the rest of the traffic. For DDoS attacks, rate-limiting is applied to specific traffic (HTTP, TCP, or UDP), while allowing the remaining traffic.The evaluation demonstrates promising results, with the Looking- Back-enabled Random Forest achieving an accuracy of 99.81%.

In research paper [19] the authors proposes a customized framework called SD-IoT (Software-Defined Internet of Things) for providing security services in IoT networks, specifically focusing on the detection of DDoS attacks. The framework is divided into three layers: the application layer, control layer, and infrastructure layer.

The application layer includes the C-DAD (Counter-based DDoS Attack Detection) application, which is responsible for detecting DDoS attacks in the SD-IoT network. The C-DAD architecture consists of different sub- modules, each containing counters with threshold values. The counter values are evaluated, and if they exceed the threshold, a trigger is generated for the flow analyser to determine the network's compromised or normal status. The paper presents various experiments with different variables and algorithms, providing detailed analysis and results in tabular and graph format.

In conventional systems, Intrusion Detection Systems (IDS) are implemented at the end level of the Internet, but they are insufficient to handle the security requirements of IoT networks. The proposed framework addresses this issue by offering a software-defined IoT security environment.

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 343-351

The three main insights of this work are as follows:

1) SDNWISE-based customized framework: The framework enhances SDNWISE with additional security services, allowing the dynamic addition of security features without changing the network infrastructure. It includes an IoT controller as a gateway between the IoT network and SDNWISE controller, along with SOPFS (Sensor Open Flow Switch) for communication between IoT nodes and the SDNWISE controller via the IoT controller.

2) Counter-based DDoS Attack Detection (C-DAD) application: This application is built on top of the proposed framework and utilizes counter-based methods such as Packet Counter, Payload Counter, and Traffic Workload Counter to identify malicious traffic and detect DDoS attacks in the SD-IoT network. The algorithm is designed to be efficient for zero-day attacks and does not rely on attack signatures or machine learning models.

3) Evaluation and results: The C-DAD algorithm is thoroughly tested and analyzed through separate experiments with different parameters.

Overall, this research work presents a customized SD-IoT framework and a counter-based detection algorithm for efficiently detecting DDoS attacks in IoT networks. The proposed solution offers flexibility, dynamic security services, and promising results in detecting DDoS attacks, enhancing the security of IoT systems.

Conclusion:

DDoS attacks on IoT networks pose significant risks due to the huge number of interconnected nodes and limited security measures. Preventing and mitigating these attacks require a multi-layered approach that includes implementing strong security practices, regular firmware updates, and network-level defences. Additionally, employing traffic monitoring and ML-based anomaly detection techniques can aid in real-time identification and response to DDoS attacks. ML algorithms offer the ability to analyze patterns and indentify anomalies in network traffic, enhancing DDoS detection capabilities.This provides a larger scope of research in this domain,

Future Scope:

The rapid growth of IoT networks and the increasing sophistication of DDoS attacks necessitate continuous research and development of robust security measures. Future efforts can focus on:1)Developing advanced ML algorithms that can adapt to evolving attack techniques and detect emerging DDoS attack patterns.2)Enhancing the accuracy of ML-based DDoS detection systems by incorporating more diverse and comprehensive training datasets.3) Exploring the integration of ML with other detection techniques, such as behavioural analysis and threat intelligence, to strengthen the overall defence against DDoS attacks.

References

1. Abdulkareem, K.H., Mohammed, M.A., Gunasekaran, S.S., Al-Mhiqani, M.N., Mutlag, A.A., Mostafa, S.A., Ali, N.S., Ibrahim, D.A.: A review of fog computing and machine learning: Concepts, applications, challenges, and open issues. IEEE Access 7, 123–140 (2019).

2. Molina Zarca, A.; Bernabe, J.B.; Trapero, R.; Rivera, D.; Villalobos, J.; Skarmeta, A.; Bianchi, S.;Zafeiropoulos, A.; Gouvas, P. Security Management Architecture for NFV/SDN-

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 343-351

Aware IoT Systems.IEEE Internet Things J. 2019, 6, 8005–8020. doi:10.1109/JIOT.2019.2904123.

3. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. IEEE Internet Things J. 2019, 6, 8182–8201.

4. Blanco, B.; Fajardo, J.O.; Giannoulakis, I.; Kafetzakis, E.; Peng, S.; Pérez-Romero, J.; Trajkovska

;Khodashenas, P.S.; Goratti, L.; Paolino, M.; others. Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN. Comput. Stand. Interfaces 2017, 54, 216–228.

5. Yousaf, F.Z.; Bredel, M.; Schaller, S.; Schneider, F. NFV and SDN—Key Technology Enablers for 5G Networks. IEEE J. Sel. Areas Commun. 2017, 35, 2468–2478. doi:10.1109/JSAC.2017.2760418.

6. Costa, Wanderson& Portela, Ariel & Gomes, Rafael. (2021). Features-Aware DDoS Detection in Heterogeneous Smart Environments based on Fog and Cloud Computing. International Journal of Communication Networks and Information Security (IJCNIS). 13. 10.54039/ijcnis.v13i3.5080.

7. Galeano-Brajones J, Carmona-Murillo J, Valenzuela-Valdés JF, Luna-Valero F. Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach. Sensors. 2020; 20(3):816. https://doi.org/10.3390/s20030816.

8. Cisco Visual Networking Index: Forecast and Trends (2017–2022). Available online: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual networking-index- vni/white-paper-c11-741490.html

9. Ericsson. Ericsson Mobility Report.Available online: https://www.ericsson.com/4acd7e/assets/local/mobilityreport/documents/2019/emr-november-2019.pdf (accessed on 15 December 2019).

10. F. A. Fernandes Silveira, F. Lima-Filho, F. S. Dantas Silva, A. de Medeiros Brito Junior and L. F. Silveira, "Smart Detection-IoT: A DDoS Sensor System for Internet of Things," 2020 International Conference on Systems, Signals and Image Processing (IWSSIP), Niteroi, Brazil, 2020, pp. 343-348, doi: 10.1109/IWSSIP48289.2020.9145265.

11. F. Sales, D. L. Filho, F. A. F. Silveira, A. D. Medeiros, B. Junior, G. Vargas-solar, and L. F. Silveira, “Smart Detection : An Online Approach for DoS / DDoS Attack Detection Using Machine Learning,”Security and Communication Networks, vol. 2019, p. 15, 2019.

12. Alaeddine Mihoub, Ouissem Ben Fredj, Omar Cheikhrouhou, Abdelouahid Derhab, Moez Krichen,Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques,Computers& Electrical Engineering,Volume 98,2022,107716,ISSN 0045-7906,https://doi.org/10.1016/j.compeleceng.2022.107716.

13. 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. 66641-66, 2018.

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 343-351

14. P. Manso, J. Moura and C. Serrão, "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. Doshi, Y. Yilmaz and S. Uludag, "Timely Detection and Mitigation of Stealthy DDoS Attacks Via IoT Networks," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 5, pp. 2164-2176, 1 Sept.-Oct. 2021, doi: 10.1109/TDSC.2021.3049942.

16. Lei Xue, Xiaobo Ma, Xiapu Luo, Edmond WW Chan, Tony TN Miu,andGuofei Gu. Linkscope: Toward detecting target link flooding attacks.IEEE Transactions on Information Forensics and Security, 13(10):2423–2438, 2018.

17. Keval Doshi, Mahsa Mozaffari, and Yasin Yilmaz. Rapid: Real-timeanomaly-based preventive intrusion detection. In Proceedings of the ACM Workshop on Wireless Security and Machine Learning, pages 49– 54, 2019.

18. Khaleel Mershad, Omar Cheikhrouhou, Leila Ismail, Proof of accumulated trust: A new consensus protocol for the security of the IoV, Vehicular Communications, Volume 32, 2021,100392,ISSN 2214- 2096, https://doi.org/10.1016/j.vehcom.2021.100392.

19. J. Bhayo, S. Hameed and S. A. Shah, "An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)," in IEEE Access, vol. 8, pp. 221612-221631, 2020, doi: 10.1109/ACCESS.2020.3043082.

20. N. Kumar, N. Mittal, P. Thakur and R. Srivastava, "Analysis of different detection and mitigation algorithm of ddos attack in software-defined Internet of Things framework: A review" in Recent Trends and Advances in Artificial Intelligence and Internet of Things, Cham, Switzerland:Springer, pp. 597-607, 2020.

21. N. M. Abdelazim, S. F. Fahmy, M. A. Sobh and A. M. B. Eldin, "A hybrid entropy-based DoS attacks detection system for software defined networks (SDN): A proposed trust mechanism", Egyptian Informat. J., May 2020.

22. H. Mostafaei and M. Menth, "Software-defined wireless sensor networks: A survey", J. Netw. Comput. Appl., vol. 119, pp. 42-56, Oct. 2018.

23. X. Luo, Q. Yan, M. Wang and W. Huang, "Using MTD and SDN-based honeypots to defend DDoS attacks in IoT", Proc. Comput. Commun. IoT Appl. (ComComAp), pp. 392-395, Oct. 2019.

24. H. Mustapha and A. M. Alghamdi, "DDoS attacks on the Internet of Things and their prevention methods", Proc. 2nd Int. Conf. Future Netw. Distrib. Syst. (ICFNDS), pp. 4, 2018.

25. A. B. Dehkordi, M. Soltanaghaei and F. Z. Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN", J. Supercomput., pp. 1-33, Jun. 2020.

26. R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz and J. González, "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN", Future Gener. Comput. Syst., vol. 111, pp. 763-779, Oct. 2020.

27. SDN-Wise the Stateful Software Defined Networking Solution for the Internet of Things, Mar. 2020, [online] Available: https://sdnwiselab.github.io/.

Catalyst Research Volume 23, Issue 2, August 2023 Pp. 343-351

28. F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine learning in iot security: Current solutions and future challenges", IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686-1721, 2020.

29. Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto and K. Sakurai, "Machine learning-based iot-botnet attack detection with sequential architecture", Sensors, vol. 20, no. 16, 2020, [online] Available: https://www.mdpi.com/1424-8220/20/16/4372.

30. Understanding support vector machine(svm) algorithm from examples (along with code), [online] Available: https://www.analyticsvidhya.com/blog/2017/09/understaing-support-vector-machine-example- code/.