Machine Learning Approaches for Detection of DoS Attacks in IoT Networks

Adrian Gruszczynski
Freie Universität Berlin
IoT & Security Seminar Report

***Abstract*—This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***Index Terms*—DDoS, IoT, anomaly detection, machine learning**

I. Introduction

Internet of Things is a group of heterogeneous physical devices running software, often equipped with sensors that exchange data with other devices over the Internet or other communication networks. The networking and computing capabilities are limited due to size, space and energy consumption constraints. It facilitates automation by measuring and recognising events from the near surroundings. There are countless use-cases for IoT in various domains, including consumer electronics, smart cities and healthcare. Nowadays, IoT is an interdisciplinary area of research involving numerous fields such as Machine Learning, Embedded Systems, Networking and Distributed Systems. It facilitates automation, control of the environment and intelligent decision-making that requires low human intervention and thus enjoys wide popularity and adoption. Due to the variety of use-cases and application domains, the IoT ecosystem consists of a substantial number of diverse standards and technologies adapted within the network. Critics emphasise security and privacy concerns as the primary weak spot of IoT. In the upcoming years, the number of connected IoT devices will increase significantly, resulting in higher decentralisation and complexity, causing further fragmentation within the ecosystem. The emergence of a new application layer called Web of Things and the application of modern Machine Learning techniques will open a market for novel services that might adapt to individual human needs.

Thanks to the wide adoption, IoT devices are very close to humans and can affect our well-being and safety. Furthermore, a variety of critical systems and infrastructure depends on these devices. The great interest and predicted future adoption make IoT an active area of research that attracts scientists from outside of computer science and electrical engineering, for instance, social sciences or environmental studies. The enormous number of connected devices poses a significant security threat and provides a vector for potential misuse. In particular, the propagation of insecure IoT devices offers a fertile ground for malicious actors and has resulted in multiple distributed denial of service (DDoS) attacks on critical internet infrastructure. To address this issue, scientists propose various solutions, including Machine Learning techniques. Machine Learning (ML) provides methods for detecting patterns in data and enjoys ever-increasing popularity. Modern applications leverage Machine Learning for translation, speech recognition and computer vision. In the cyber-security field, Machine Learning finds use for fraud, malware and spam detection. With the recent emergence of Deep Learning, strategical reasoning and decision-making of a machine may exceed human performance creating room for novel use-cases. The application of modern Machine and Deep Learning approaches delivers a toolbox for network traffic analysis, intrusion detection and real-time anomaly detection. Thanks to the variety of use-cases and the fragmentation within the IoT ecosystem, a broad implementation of Machine Learning methods for DDoS detection stays challenging. Further limitations such as limited computing resources, energy constraints and complex system architecture call for novel solutions.

The aim of this study is to evaluate several Machine Learning approaches for DDoS detection in the context of practical implementation within the IoT ecosystem. It will highlight various strategies for DDoS detection in IoT systems to explore the current state of the art and explain one method in more detail. The objective is to improve the understanding of DDoS detection in IoT and demonstrate the role of Machine Learning.

II. Related Work

The application of Machine Learning approaches for DDoS detection in IoT is an emerging area of research. Although DDoS detection in IoT and DDoS detection with Machine Learning are both well-researched fields, the body of research on applying Machine Learning approaches for DDoS detection in IoT leaves much to be desired. There is no survey comparing Machine Learning and Deep Learning methods for DDoS detection under IoT constraints. Specifically, the practical aspects of these methods, such as computational complexity, energy consumption, ability to detect unknown attacks and detection performance, are unexplored and will benefit from further examination. The existing surveys focus on general DDoS attacks and defences in IoT or provide a broader perspective on various Machine Learning methods for IoT Security.

A. General DDoS Protection

In the general DDoS protection and prevention field, R. Vishwakarma and A. K. Jain present a comprehensive survey of DDoS attacks and DDoS defence techniques for IoT. They introduce the layered IoT architecture and demonstrate the security issues of IoT networks. They propose an extensive taxonomy of IoT-specific DDoS attack types and defence techniques. Furthermore, they compare the pros and cons of each method and discuss open research questions and limitations. Zargar et al., in their survey, propose a taxonomy of DDoS attacks and classify the existing countermeasures for different use-cases. They emphasise the role of IoT in the expansion of DDoS attacks.

B. Machine learning for DDoS protection

In the domain of DDoS detection using Machine Learning methods, Saied et al. apply Artificial Neural Networks (ANNs) to detect and prevent known and unknown DDoS attacks. They leverage network characteristic data to detect TCP, UDP and ICMP DDoS attacks. They obtain training data by reproducing the network environment under DDoS conditions. The classification accuracy was superior to existing approaches, particularly for detecting unknown DDoS attacks. Ming-Yang Su uses a weighted k-nearest neighbour classifier for real-time DDoS detection. He proposes a genetic algorithm for feature selection and weighting and evaluates his classifier using several well-known DDoS attacks. He obtains 97.42% detection accuracy for known types of DDoS attacks and 78% for the unknown.

C. Machine learning for IoT Security

In the Machine Learning for IoT Security field, Cvitic et al. propose a conceptual model for DDoS detection in IoT networks based on traffic characteristics. They argue that IoT-generated traffic is distinguishable from human-generated network traffic. They assign IoT traffic to three categories: periodic updates, event-driven and payload exchange. Based on the proposed model, DDoS attacks are an anomaly to the legitimate IoT traffic for a given device type. The authors suggest Boosting Machine Learning method for network traffic anomaly detection. Lopez-Martin et al. use flow statistics-based information from the packet header (bytes transmitted, packet interval times, TCP window size, etc.) to develop a network traffic classifier. They use a dataset of over 250 thousand network flow data points collected from over 100 different services. Their classifier combines a Recurrent Neural Network and a Convolutional Neural Network. Their best models classify the service (HTTP, Telnet, YouTube, Google, etc.) with 96.23% accuracy. Furthermore, they emphasise the importance of flow data features for classification accuracy. Sivanathan et al. show over 99% accuracy in classifying IoT devices based on patterns in their network activity. They collected network traffic data of 28 IoT devices such as cameras, lights and sensors for over six months. They present insights into the data using statistical features, propose a state-of-the-art performance multi-stage Machine Learning classifier and discuss trade-offs of their solution for real-time use. Al-Garadi et al. present a survey on Deep Learning methods for IoT Security. They introduce layers of the IoT system and picture various IoT-specific attack surfaces and threats. They review and discuss several Machine Learning and Deep Learning methods for IoT security in the context of the advantages, shortcomings and opportunities. Furthermore, they provide a comprehensive overview of studies applying Machine Learning and Deep Learning methods on different IoT layers (Perception, Network, Application). Finally, they discuss challenges, open issues and future directions for these techniques in IoT security.

D. Machine learning for DDoS detection in IoT

In the field of DDoS detection in IoT networks using Machine Learning, Aysa et al. investigate the performance of several Machine Learning approaches for DDoS detection based on network traffic patterns. The authors use a dataset of actual traffic data collected from 9 commercial IoT devices infected with Mirai and

BASHLITE botnets. Preliminary results show that combining Decision Trees with a Random Forest outperforms other approaches. N. Ravi and S. M. Shalinie examine DDoS attacks triggered by malicious IoT devices on IoT servers. They leverage the Software-Defined Network paradigm and semi-supervised Machine Learning algorithm for DDoS detection and mitigation. They reported a 96.28% accuracy rate in the detection of DDoS attacks. In "Boosting-Based DDoS Detection in Internet of Things", Cvitic et al. focus on the IoT-specific DDoS traffic detection model. They propose an approach for classifying devices into four classes based on the predictability of their network behaviour. Their classification accuracy lies between 99.92% and 99.99%. Roshi et al. demonstrate that IoT-specific network characteristics suffice to detect DDoS attacks with high precision using Machine Learning methods. They conclude that consumer gateway devices could discover local sources of DDoS attacks using low-cost and efficient Machine Learning algorithms.

III. Background and Methods

This section consists of two parts: Background and Methods. The first part introduces the terminology describing the IoT architecture, types of DDoS attacks, DDoS defence mechanisms and the role of IoT botnets in DDoS attacks. The second part comprises an overview of studies on IoT-specific Machine Learning algorithms for DDoS detection.

A. IoT Architecture

The IoT architecture consists of four primary layers. The first layer, called the perception layer, involves physical objects such as sensors, cameras, lightbulbs or microphones. The main objective of the physical layer is to collect and store information from the surrounding environment, for instance, motion data, temperature, humidity or acceleration. These physical devices operate under the limitations of constrained energy consumption, low computational performance and sparse memory. The primary portion of data within the IoT ecosystem comes from this layer. The second layer is responsible for connecting heterogeneous IoT devices amongst each other and with the internet. The resource limitations of the perception layer force the network layer to optimize for power efficiency, low memory and lossy communication under noisy conditions. Covering the variety of use-cases requires different communication protocols, such as 6LoWPAN, WiFi, Bluetooth Low Energy, NFC, ultra-wideband, 3G, 4G etc. The third layer, called the middleware layer, provides an abstraction for IoT devices and their connectivity to allow easier application development. It facilitates interoperability between heterogeneous IoT devices and takes care of persistence, retrieval and manipulation of data while offering functionality for device discovery, context-aware understanding of sensor data and security. Finally, the last layer employs the middleware and provides room for creating a great range of applications in domains such as healthcare, transportation, manufacturing, etc. The main objective of the application layer is to present insights from the data to the user and allow user-friendly interaction with the underlying infrastructure.

B. Classification of DDoS Attacks

In practice, simple configuration and hardware constraints of IoT devices, particularly consumer-grade, result in outdated or insecure software and misconfiguration, creating an easy and attractive target for adversaries. The amount of always-on vulnerable IoT devices provides an opportunity for launching large-scale DDoS attacks. IoT-specific DDoS attacks do not differ much from traditional DDoS attacks and involve diverse and sophisticated techniques. Due to its nature, preventing DDoS attacks requires identifying limitations and security vulnerabilities in each IoT layer. There are two main categories of DDoS attacks: application layer attacks and infrastructure layer attacks. The application-layer attacks exploit vulnerabilities of web servers or operating systems by leveraging weaknesses in HTTP, DNS or other application-specific protocols. The main objective is to exhaust host resources by starting a background process, for instance, sending incomplete POST requests very slowly so that the server runs out of concurrent connections (Slowloris attack). The incoming malicious traffic is difficult to tell from the legitimate traffic and thus hard to mitigate. IoT botnets play a primary role in application layer attacks by providing a source of legitimate traffic.

The infrastructure layer attacks exploit vulnerabilities and flaws of the IoT network layer. They are more popular than application layer attacks. This type of attack consists of two categories: volume-based and protocol-based attacks. The volume-based attack is the simplest to perform. The main goal of a volume-based attack is to overwhelm the victim with the sheer amount of traffic. Usually, the attacker employs reflection or amplification techniques for this type of attack. The reflection uses forged packets with a fake source IP address for sending requests to a powerful server. The server responds to

these malicious requests and overloads the victim host specified by the fake source IP header with traffic while hiding the attacker's identity. The amplification attack uses long server responses combined with IP Spoofing to overwhelm the victim with a large amount of incoming traffic. The idea here is that requests are smaller than the server response, e.g. long DNS record, allowing the adversary to magnify the attack scale. Due to its nature, this attack performs effectively under constrained bandwidth and resources of the IoT devices. The protocol-based attack exploits flaws in the network layer to drain the processing capacity of the victim host. ACK and SYN flood are well-known protocol-based attacks that exploit the inner workings of the TCP protocol. In this attack, the adversary starts the TCP three-way handshake process but does not finish, causing the victim server to wait and consume resources.

C. DDoS Defence Mechanisms

DDoS defence mechanisms comprise two main categories: traditional and IoT-specific DDoS detection. Traditional DDoS defences run on conventional, homogenous systems and take advantage of powerful resources. On the other hand, IoT-specific solutions are more sophisticated and complex due to limited resources and the variety of devices involved. Both defence mechanisms rely on monitoring network activity and detection techniques for suspicious traffic. Furthermore, there are two subcategories of IoT-specific defence solutions: detection and prevention-based. The main objective of detection-based defence techniques is to discover the presence of DDoS malware. The detection of abnormal activities occurs in the case of traditional DDoS defences on the host or in the network. For IoT-based systems, the detection happens primarily in the network. DDoS detection works by observing the network traffic and identifying abnormal usage patterns and host behaviour. If the system discovers any anomalies, it starts to determine the origin of the malicious requests by analyzing individual hosts' behaviour within the network. Next, it tries to establish the IP address of the attacker and discards the incoming packets, which alleviates the DDoS attack. In the case of IoT networks, the detection system runs on a middlebox or a home gateway within the network and monitors the outgoing traffic. It leverages Machine Learning methods for detecting IoT-specific anomalies in network traffic and identifying malware. Prevention-based defence techniques focus on avoiding any invasion into the IoT devices. One idea is to force the device manufacturer to implement reasonable security measures and firmware updates by legal regulations. In the case of the MIRAI botnet, the infected devices exposed Telnet, SSH and their web services to the internet, protected merely by default firmware credentials. Changing these credentials and disabling the remote access to exposed services on the device requires a firmware update from the manufacturer. Unfortunately, law enforcement lacks processes and legal rules to force device manufacturers to act. The main weakness of the regulatory approach is the difficulty of identifying the devices participating in a botnet and finding the responsible manufacturer. Another drawback is that the process of a large-scale firmware update is complicated and time-consuming without over-the-air updates. Another idea for a preventive approach is to introduce a middleware interface layer that protects unauthorized access to the device. This middleware can provide a user interface and allow setting user access credentials. It is questionable, however, whether additional levels of complexity will find broad user adoption within the consumer segment.

D. Machine Learning for DDos Protection

Machine Learning algorithms for DDoS protection in IoT play a primary role in detecting malware and network traffic anomalies. Depending on the situation, the detection may occur on the IoT device, in the cloud or the network by leveraging additional or existing hardware. Machine Learning is a set of methods that leverage data to make predictions or decisions without specifying a pre-defined set of rules. Machine Learning algorithms fall into three main categories based on how they approach learning. Supervised Machine Learning algorithms require labelled data in the form of input-output mappings. The goal is to create a mathematical model and learn these mappings by optimizing a cost function. After training, the model can perform predictions on previously unseen data. Therefore, the model lifecycle consists of two phases: training and inference. Unsupervised learning uses unlabelled data that contains only input to find hidden patterns and structures. It is particularly effective for discovering groups and clusters of similar samples that may indicate different categories in the data. Reinforcement learning algorithms focus on providing agents that can interact with the environment. The training objective is to maximize a reward function by finding an optimal decision process. Reinforcement learning algorithms find use in autonomous vehicles and playing games against a human opponent. The training process of Machine Learning algorithms is a time and resource-consuming task that requires GPUs

and large amounts of data. Trained models consist of thousands and even millions of parameters. In recent years, Machine Learning approaches outperformed existing methods for image classification, anomaly and malware detection and text generation. For this reason, it is worthwhile to investigate their value in the context of DDoS detection for IoT.

1) On-device Detection: In Malware Images: Visualization and Automatic Classification, the authors propose a novel approach for malware detection on IoT devices. They convert a binary malware executable file into an 8-bit vector and visualize it as fixed width, variable height grayscale image. They observe that images of files from different malware families appear visually distinct from malware files belonging to the same family. Based on their findings, they extract features from the image using GIST, which has proven successful for scene and object classification tasks. The authors use a steerable pyramid, a multi-scale and multi-orientation image representation technique that applies multiple subsampling and smoothing stages resulting in a structure similar to a pyramid. For the classification, they use an unsupervised k-nearest neighbours algorithm. The k-nearest neighbour's method leverages the existing data for clustering based on a similarity metric, for example, Euclidean distance. The classification of previously unseen samples takes place by feature extraction and selection of the k-nearest neighbours of that sample. The prediction is the majority of selected neighbours' labels. The authors evaluate the detection performance on a larger dataset of 25 different malware families comprising 9,458 binaries and tenfold cross-validation. Each evaluation uses a randomly sampled subset of data for the train (90%) and test (10%) sets. The results show that their method achieves similar classification performance to related work but is about 40 times faster. K-nearest neighbour algorithm requires storing the malware data in memory, rendering it ineffective for running on IoT devices. In Lightweight Classification of IoT Malware based on Image Recognition, the authors use the visual representation of malware binaries and provide a resource-efficient classifier specifically for IoT devices. They convert malware binaries to grayscale images and leverage a small-size Convolutional Neural Network for classification. The advantage of neural networks is that they automatically extract non-linear features from data. The resource-consuming training process takes place in the cloud environment, which is beneficial since the device does not have to store data compared to the k-nearest neighbours' algorithm. The resource-constrained devices receive a pre-trained model and perform the classification locally. In the study, the authors propose using a two-tier architecture combining a lightweight, on-device classifier with a powerful cloud-based one. In this case, the objective is to recognize suspicious programs locally on the device and hand them over to the backend server for further analysis. The researchers conduct experiments using the IoT DDoS malware dataset from IoTPOT. The dataset consists of 500 malware examples from multiple malware families. They collect the same number of samples of benign software to augment the data and divide the resulting data into train and test sets. They train their model to differentiate between goodware and malware and perform five-fold cross-validation. They show that the model detects malware with about 94% accuracy while having the least amount of parameters compared to models from other studies. As future improvements, they suggest further optimization of the network in terms of performance by reducing the network size.

REFERENCES

Please number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use "Ref. [3]" or "reference [3]" except at the beginning of a sentence: "Reference [3] was the first . . ."

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished" [4]. Papers that have been accepted for publication should be cited as "in press" [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, “Title of paper if known,” unpublished.
[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
[7] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.