PhD Forum Abstract: DDoS attack detection in IoT systems using Neural Networks

Arvin Hekmati
hekmati@usc.edu
University of Southern California
Los Angeles, California, USA

ABSTRACT

This short paper summarizes our recent/ongoing works [2–4] on detecting DDoS attacks in IoT systems. In our studies, we conducted a thorough examination of using machine learning to detect Distributed Denial of Service (DDoS) attacks in large-scale Internet of Things (IoT) systems. Unlike prior works and typical DDoS attacks that focus on individual nodes transmitting high volumes of packets, we explored the more sophisticated and advanced future attacks that use a large number of IoT devices while hiding the attack by having each node transmit at a volume that mimics benign traffic. We introduced innovative correlation-aware architectures that consider the correlation between the traffic of IoT nodes and compare the effectiveness of centralized and distributed detection models. Through extensive analysis, we evaluated the proposed architectures using five different neural network models trained on a real-world IoT dataset of 4060 nodes. Our results showed that the combination of long short-term memory (LSTM) and transformer-based models with the correlation-aware architectures offer superior performance, in terms of F1 score and binary accuracy, compared to the other models and architectures, especially when the attacker conceals its actions by following benign traffic distribution on each transmitting node. Furthermore, we investigated the performance of heuristics for selecting a subset of nodes to share their data in resource-constrained scenarios for correlation-aware architectures.

CCS CONCEPTS

• **Security and privacy** → *Malware and its mitigation.*

KEYWORDS

DDoS attack, IoT, neural networks, dataset

ACM Reference Format:
Arvin Hekmati. 2023. PhD Forum Abstract: DDoS attack detection in IoT systems using Neural Networks. In *The 22nd International Conference on Information Processing in Sensor Networks (IPSN '23), May 9–12, 2023, San Antonio, TX, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3583120.3589564

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
IPSN '23, May 9–12, 2023, San Antonio, TX, USA
© 2023 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0118-4/23/05.
https://doi.org/10.1145/3583120.3589564

1 INTRODUCTION

Denial of Service (DoS) attacks are a form of cyberattack in which the attacker aims to disrupt the normal functioning of a victim server, hindering legitimate users from accessing its system. This is achieved by overwhelming the server with an excessive amount of traffic, making it unavailable[7]. Distributed Denial of Service (DDoS) attacks are a type of cyberattack in which the attacker leverages a network of compromised devices, often referred to as "zombies," to launch a coordinated attack on a victim server. The use of multiple devices significantly increases the scale and impact of the attack, making it much more difficult for the victim server to defend against[6]. The most prevalent type of DDoS attack takes place at the transport layer, where the attacker floods the victim server with as many packets as possible through methods such as UDP flooding and SYN flooding. There are also DDoS attacks that target the application layer, where the attacker aims to overload the victim server by sending slow, but steady requests that consume all of its resources. These slow-rate DDoS attacks occur when the attacker sends data to the victim server at a very slow pace, but at a rate that is sufficient to prevent the connection from timing out[8].

The Mirai botnet is one of the most well-known DDoS attacks that leverages Internet of Things (IoT) devices. This botnet infects thousands of IoT devices, directing an overwhelming amount of network traffic, in the order of Terabits per second (Tbps), towards the victim server, causing widespread disruption and affecting millions of end-users [5].

Given the growing and dangerous threat posed by DDoS attacks, our recent work investigates the use of machine learning (ML) techniques as a means to prevent such attacks. One of the major limitations of existing research on DDoS detection mechanisms is that they rely on the assumption that the packet volume transmitted from IoT nodes or the packet flow timing during an attack is significantly (orders of magnitude) higher than the benign traffic from these nodes. While these differences in traffic properties can provide a significant advantage to ML models in detecting DDoS attacks, our recent studies [2–4] take a forward-looking approach and consider the possibility of more sophisticated attacks in which the attacker can mimic the behavior of benign IoT traffic. With the vast number of IoT devices currently available, attackers can potentially take control of millions of these devices and launch an attack by sending fewer packets with timing similar to benign traffic, making it more difficult to distinguish the attack from normal behavior.

This abstract summarizes and covers our findings in our recent/ongoing works [2–4].

2 DDOS ATTACK DETECTION MECHANISM

To simulate futuristic DDoS attacks, in our works [3, 4], we introduce a parameter called "k" that allows for the adjustment of traffic volume during the attack. The real urban IoT dataset introduced in [2] records the binary activity of each device and has been enhanced in our other work [3] by incorporating the packet volume transmitted by each device at each timestamp. Our work is based on the observation that real urban IoT benign traffic can be modeled as a (truncated) Cauchy distribution, which aligns with prior findings that Ethernet traffic exhibits similar characteristics [1].

In our latest work [4], we proposed four different architectures for training neural network models for IoT devices. These architectures take into account the use of correlation information among the IoT devices and the choice between a centralized model for all nodes or individual models for each device. The four architectures are named as follows: multiple models with correlation (MM-WC), multiple models without correlation (MM-NC), one model with correlation (OM-WC), and one model without correlation (OM-NC). The architectures with correlation information (MM-WC and OM-WC) provide each IoT node access to not only its own packet volume but also that of other nodes. To further evaluate the performance of these architectures, we have considered five different types of neural network models: multi-layered perceptron (MLP), convolutional neural networks (CNN), long short-term memory (LSTM), transformer (TRF), and autoencoders (AEN). Through extensive analysis [4], we aimed to determine the best architecture and neural network model for detecting DDoS attacks on IoT devices.

The results of our simulations [4] demonstrated that utilizing the correlation information among the nodes plays a crucial role in detecting DDoS attacks, especially when the attacker is attempting to conceal the attack by mimicking benign traffic packet volume distribution. Our findings showed that the architecture of MM-WC MM-WC in combination with LSTM neural network model is the most effective in detecting DDoS attacks. Additionally, OM-WC architecture combined with the TRF neural network model also performs exceptionally well, comparable to the MM-WC/LSTM model. However, we prefer the MM-WC/LSTM model due to its resilience to the single point of failure.

Given the vast number of IoT devices that can be utilized in DDoS attacks, using the correlation information of all nodes results in a substantial amount of features that the neural network models must learn. To address this challenge, in our latest work [4] we have explored methods for actively selecting the nodes to consider for the correlation information in training the neural network models. Our analysis has considered three methods: a) Pearson correlation of the IoT nodes' activity behavior, b) Euclidean distance of the IoT nodes, and c) SHapley Additive exPlanations (SHAP) for identifying the most relevant features. Our findings indicated that actively selecting the nodes for both training and prediction using Pearson correlation results in satisfactory performance in terms of binary accuracy and F1 score for detecting DDoS attacks, with a slight decrease compared to utilizing the correlation information of all nodes.

3 CONCLUSION AND FUTURE WORK

In this study, we presented a summary of our recent/ongoing studies [2–4] in which we evaluated various architectures and neural network models for detecting DDoS attacks on IoT nodes. Our results showed that the MM-WC/LSTM model outperforms the other models. Additionally, we explored different techniques for actively selecting nodes to share their information. Our findings suggest that using Pearson correlation to select the nodes results in a reasonable level of accuracy in detecting DDoS attacks, compared to using information from all nodes. In future work, we plan to design a robust model to handle the case where information from IoT nodes is lost during transmission for training the correlation-aware architectures. Furthermore, we aim to formulate a policy for blocking flagged malicious IoT nodes while taking into account the importance of these nodes to end-users and avoiding the risk of false-positive flags and loss of access.

ACKNOWLEDGMENTS

This material is based upon work supported by the Defense Advanced Research Projects Agency (DARPA) under Contract Number HR001120C0160 for the Open, Programmable, Secure 5G (OPS-5G) program. Any views, opinions, and/or findings expressed are those of the author(s) and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government. I am grateful for the guidance, insightful comments, and reviews of Professor Bhaskar Krishnamachari, and for all the work and inputs of my coauthors on the prior studies cited herein. This document has been edited with the assistance of ChatGPT. I certify that ChatGPT was not utilized to produce any technical content and I accept full responsibility for the contents of the paper.

REFERENCES

[1] Tony Field, Uli Harder, and Peter Harrison. 2002. Network traffic behaviour in switched Ethernet systems. In *Proceedings. 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems*. IEEE, 33–42.

[2] Arvin Hekmati, Eugenio Grippo, and Bhaskar Krishnamachari. 2021. Large-Scale Urban IoT Activity Data for DDoS Attack Emulation. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems* (Coimbra, Portugal) *(SenSys '21)*. Association for Computing Machinery, New York, NY, USA, 560–564. https://doi.org/10.1145/3485730.3493695

[3] Arvin Hekmati, Eugenio Grippo, and Bhaskar Krishnamachari. 2022. Neural Networks for DDoS Attack Detection using an Enhanced Urban IoT Dataset. In *2022 International Conference on Computer Communications and Networks (ICCCN)*. 1–8. https://doi.org/10.1109/ICCCN54977.2022.9868942

[4] Arvin Hekmati, Nishant Jethwa, Eugenio Grippo, and Bhaskar Krishnamachari. 2023. Correlation-Aware Neural Networks for DDoS Attack Detection In IoT Systems. *arXiv preprint arXiv:2302.07982* (2023). https://doi.org/10.48550/ARXIV.2302.07982

[5] Artur Marzano, David Alexander, Osvaldo Fonseca, Elverton Fazzion, Cristine Hoepers, Klaus Steding-Jessen, Marcelo H. P. C. Chaves, Italo Cunha, Dorgival Guedes, and Wagner Meira. 2018. The Evolution of Bashlite and Mirai IoT Botnets. In *2018 IEEE Symposium on Computers and Communications (ISCC)*. 00813–00818. https://doi.org/10.1109/ISCC.2018.8538636

[6] Manjula Suresh and R. Anitha. 2011. Evaluating Machine Learning Algorithms for Detecting DDoS Attacks. *Communications in Computer and Information Science* 196, 441–452. https://doi.org/10.1007/978-3-642-22540-6_42

[7] Karan Verma, Halabi Hasbullah, and Ashok Kumar. 2013. An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET. In *2013 3rd IEEE International Advance Computing Conference (IACC)*. 550–555. https://doi.org/10.1109/IAdCC.2013.6514286

[8] Noe Marcelo Yungaicela-Naula, Cesar Vargas-Rosales, and Jesus Arturo Perez-Diaz. 2021. SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning. *IEEE Access* 9 (2021), 108495–108512. https://doi.org/10.1109/ACCESS.2021.3101650