Demo Abstract: CUDDoS - Correlation-aware Ubiquitous Detection of DDoS in IoT Systems

Jiahe Zhang, Tamoghna Sarkar, Arvin Hekmati, Bhaskar Krishnamachari
University of Southern California
Los Angeles, California, USA
{jzhang97,tsarkar,hekmati,bkrishna}@usc.edu,

ABSTRACT

In recent years, there has been a significant surge in the deployment of Internet of Things (IoT) devices, which has consequently escalated security threats, notably Distributed Denial of Service (DDoS) attacks. Our prior research developed an LSTM-based framework for detecting futuristic DDoS attacks but largely relied on simulated datasets [1]. To bridge this gap, we designed a Raspberry Pi (RPi) testbed that mimics the complexities of large-scale IoT networks. This setup allows us to simulate realistic DDoS attacks originating from IoT devices and evaluate the effectiveness of various DDoS detection techniques. Specifically, using this RPi testbed, we validated the effectiveness of our LSTM-based framework in identifying futuristic DDoS attacks, observing an F1 score ranging between 0.8 and 0.86 depending on the aggressiveness of the DDoS attack.

KEYWORDS

DDoS attack, IoT, neural networks

ACM Reference Format:
Jiahe Zhang, Tamoghna Sarkar, Arvin Hekmati, Bhaskar Krishnamachari . 2023. Demo Abstract: CUDDoS - Correlation-aware Ubiquitous Detection of DDoS in IoT Systems. In *The 21st ACM Conference on Embedded Networked Sensor Systems (SenSys '23), November 12–17, 2023, Istanbul,Turkiye*. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3625687.3628392

1 INTRODUCTION

The unprecedented proliferation of IoT devices has brought forth not only technological advancements but also escalated security vulnerabilities. Distributed Denial of Service (DDoS) attacks, especially those that exploit large-scale IoT networks, pose a considerable threat to both individual users and organizations. Our previous work laid the groundwork for utilizing machine learning-based architectures to detect futuristic DDoS attacks with tunable aggressiveness [1]. In this context, we introduced the concept of **Multi Models With Correlation (MM-WC)**, an architecture where individual neural network models are trained for each IoT node. Furthermore, these models utilize both their own packet volume data and correlated data from adjacent nodes for more robust DDoS detection. We observed that using LSTM models along with MM-WC showed superior performance in detecting botnets performing DDoS attacks. Although our original paper presented these innovations, it primarily relied on simulated datasets. The system we will demonstrate aims to bridge the gap between these theoretical and practical implementations.

Herein, we extend our preliminary work by introducing a real-world emulation of IoT networks to detect DDoS attacks, providing a practical validation of the LSTM/MM-WC framework. Using a carefully designed testbed of 51 Raspberry Pi (RPi) devices, we mimic the complexities of a large-scale IoT system. To the best of our knowledge, this work is the first to deploy Edge Machine Learning for DDoS detection in a testbed of such a size replicating some of the complexities and intricacies of real-world IoT networks. We have designed the flow-level traffic and complexities of networked devices to closely mirror real-world scenarios. Furthermore, we introduce real-time inference capabilities by deploying the trained LSTM/MM-WC model on each Rpi device. This enables each node to autonomously detect DDoS attacks using real-time traffic, further enhancing the practicality of our framework.

We will demonstrate through our testbed the reliable performance of the LSTM/MM-WC framework in identifying DDoS attacks, even when the attackers employ sophisticated camouflage techniques. The demonstrated system allows experimenting with the futuristic DDoS attack and seeing the detection framework performance in real-time on a GUI framework. Additionally, for those interested in delving deeper, our code and dataset can be accessed at https://github.com/ANRGUSC/ddos_demo.

2 SYSTEM OVERVIEW

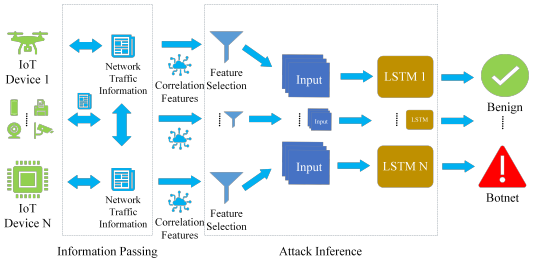


Figure 1: Structure of the LSTM/MM-WC model for IoT DDoS Detection

Model Design: In prior work, we demonstrated the exceptional performance of the LSTM/MM-WC model in detecting more sophisticated futuristic DDoS attacks [1]. This model utilizes the traffic information of all nodes for making the DDoS detection inference. Figure 1 illustrates the structure of this model. Each IoT node is

SenSys '23, November 12–17, 2023, Istanbul, Turkiye

ACM ISBN 979-8-4007-0414-7/23/11.
https://doi.org/10.1145/3625687.3628392

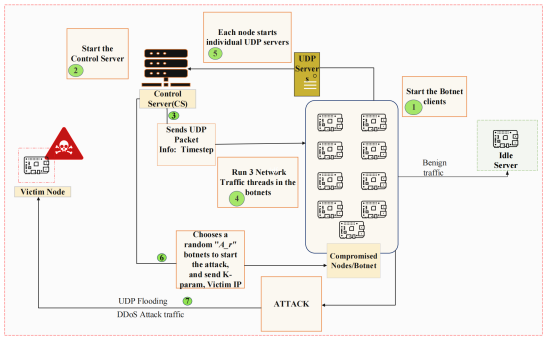
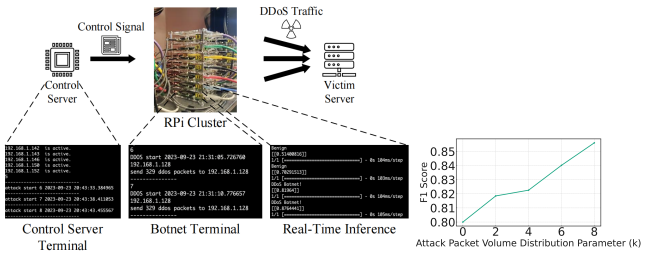


Figure 2: Network architecture and information flow



(a) System Architecture **(b) Evaluation Result**

Figure 3: System Demonstration

trained with its dedicated LSTM model and conducts inference autonomously. We disseminate the packet rate (packets exchanged over a fixed time interval) from each individual RPi node to adjacent nodes, utilizing the correlation characteristics inherent in each node's activity.

System Design: Figure 2 presents the proposed network architecture, designed for emulating real-world IoT behavior and sophisticated DDoS attacks. Our design leverages a Behavior Dataset (BD) sourced from a dataset consisting of real IoT nodes situated in an urban environment to emulate complex IoT node activities and advanced DDoS threats [1]. Each node maintains a BD, which serves as a benchmark for simulating benign IoT node activities, consequently obfuscating DDoS traffic within benign traffic. The network architecture can be divided into three parts: the control server (CS), the IoT nodes, and the victim/idle server. Unlike the Command-and-Control (C&C) server in the Mirai botnet, our CS not only manages DDoS attacks but also regulates the benign behavior of each individual node. In the BD, data is sampled at 10-minute intervals, thereby introducing a "time step" as the unit for IoT node activities in our system.

Upon system startup, the CS sequentially reads the BD and maintains a time step. Each time step corresponds to a data point in the BD. If the ACTIVE flag in the data point is set to 1, the CS issues a control signal to the associated node, keeping it active and instructing it to send benign traffic to the idle server within that time step. When an attack is initiated, the CS dispatches a "start-attack" signal to the relevant node, prompting it to operate as part of the botnet for the duration of that time step. In this DDoS attack, we employed a parameter, k, previously introduced in our work [1]. The parameter k is tunable; a higher value of k leads to a more aggressive DDoS attack, resulting in a greater number of packets being sent to the victim server. Using the outlined method, we emulate both IoT node activity and complex DDoS traffic within our system. Each node shares its packet volume once per time step, thereby providing correlational features to other nodes. Simultaneously, every node maintains a queue of 10 historical records, which are subsequently utilized by the LSTM/MM-WC for predictive inference.

3 DEMONSTRATION

The system we plan to demonstrate is illustrated in Figure 3a. The system is deployed on a network consisting of 51 RPi 3B units to emulate a real-world IoT environment. The RPi network comprises a Control Server responsible for managing IoT node behavior, a Victim/Benign Server designated to receive network traffic, and 49 IoT Nodes where detection inference is conducted. The figure illustrates our ability to log into a) set parameters for simulating attacks as well as b) visualize the outputs of the DDoS attack detection model via command line interfaces. We also plan to demonstrate graphical user interfaces that allow easy parameter and simulation configuration such as attack parameters (k value, duration, start time, ratio of botnets) as well as a real-time dashboard for visualizing the detection framework.

Sample Experimental Evaluation: As an example of the capabilities of the testbed, we evaluated attacks corresponding to various k values: 0, 2, 4, 6, and 8. We also tested attack durations of 10 and 20 minutes and examined scenarios where 50% and 100% of the IoT nodes participated in the attack. The LSTM/MM-WC model was assessed using the traffic data collected from RPis, yielding F1 scores ranging from 0.80 to 0.86. Additionally, we conducted real-time DDoS detection inference with k = 8, a 10-minute attack duration, and a 100% attack ratio, achieving an F1 score of 0.82.

The results in Figure 3b indicate that higher F1 scores correlate with increased k values. This supports the fact that more aggressive DDoS attacks make botnets more detectable. Furthermore, the results from the RP test-bed are consistent with our previous findings from the synthesized dataset [1], demonstrating robust performance in realistic emulation scenarios.

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. This document has been edited with the assistance of ChatGPT. We certify that ChatGPT was not utilized to produce any technical content and I accept full responsibility for the contents of the paper.

REFERENCES

[1] 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).