School of Electronic Engineering

An Evaluation of Distributed Denial of Service (DdoS) Attacks in IoT Networks

Literature Survey

Michael Lenehan
ID Number: 15410402

January 2020

MEng in Electronic and Computer Engineering

Supervised by Liam Meany

Declaration

I hereby declare that, except where otherwise indicated, this document is entirely my own work and has not been submitted in whole or in part to any other university.

Signed: Michael Lenehan Date: 27/01/2020

An Evaluation of Distributed Denial of Service (DDoS) Attacks in IoT Networks - Literature Review

Michael Lenehan

***Abstract*—With the increase in the number of Internet of Things (IoT) connected devices in recent years, and the projected growth in the number of connected devices in the coming years, it is evident that there is a need to investigate the security flaws which have made these devices a target for Distributed Denial of Service (DDoS) attacks. This literature review will investigate the ongoing work in the area of Internet of Things security with regards to DDoS attacks, and will**

***Index Terms*—Internet of Things, Distributed Denial of Service, Security.**

I. Introduction

INTERNET of Things devices have seen a large increase in usage in the past number of years. With estimates of the number of devices exceeding 40 billion[1], and the amount of data produced by these devices in the order of Zettabytes[1] (10^{21}), it is apparent that the recent issues regarding Distributed Denial of Service (DDoS) attacks may be concerning to those utilising the networks.

The motivation of this project is to evaluate the susceptibility of IoT operating systems and devices to these types of attacks. The goal is to develop or recommend a solution for the detection of an attack, and the mitigation of such an attack.

A. Distributed Denial of Service Attacks

Distributed Denial of Service attacks aim to shut down their targets servers through a high volume flood of traffic. This high volume traffic, which can be in the order of Terrabytes of data, serves to overload the available resources of the hosts network, which causes regular user traffic to be rerouted. This rerouting leads to the "denial of service" aspect of the attack.

The distributed aspect of the DDoS attack comes from the multiple devices which are infected with the attackers malware. These devices are known as bots, and are remotely accessed by an attacker to generate high traffic to drain the networks resources.

B. Internet of Things DDoS Attacks

A DDoS attack relies on the attacker gaining remote access to devices in order to initiate a flood of traffic. As such, Internet of Things devices can act as an entry point to the network for an attacker due to the "always-on" nature of the devices and their connection to the network, and their lack of security features.

Attacks, such as the Mirai attack, rely on the default security credentials ,which tend to remain unchanged when configured by end users, to gain access to the devices for the uploading of malicious software[2].

Since the Mirai attack in 2016, and the subsequent release of the Mirai source code, there has been an increase in the number of IoT related DDoS attacks[3].

C. IoT Areas

Internet of Things devices have become common place in everyday life, with devices such as internet connected security cameras, smart-home devices, and wearable smart devices being common in households. However, there are many other use cases outside of the home where IoT devices have been adopted.

Industrial Internet of Things (IIoT) includes devices such as cameras and sensors within industrial settings, which, as with IoT, provides the ability to offload intensive processing to higher performance servers[4]. This division of IoT devices is integral for the "Industry 4.0" concept.

Internet of Medical Things (IoMT) devices include healthcare specific connected devices, such as medical sensors and wearable devices for patient monitoring purposes[5]. These devices allow for an increase in patient comfort, and are an integral component of the "Healthcare v4.0" concept.

II. Review and Analysis of Prior Work

Salim et al.[3] have presented a thorough survey of a number of different DDoS attacks which are common in IoT networks. Their work provides classifications for these attacks, along with providing a number of detection, prevention and mitigation solutions.

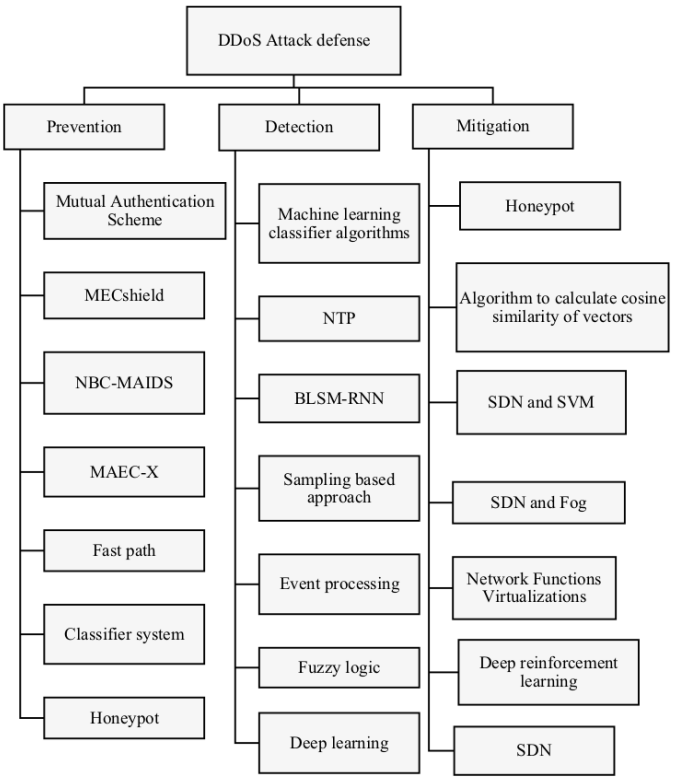

Fig. 1: Salim et al. DDoS attack Defence techniques[3]

As seen in Figure 1, there are 21 proposed solutions; 7 Prevention, 7 Detection, and 7 Mitigation. These solutions act at the device level, edge computing level, and cloud level.

Prevention of attacks deals in stopping traffic flow between nodes flagged for suspicious or "abnormal" traffic. These techniques involve monitoring the traffic between the nodes, and either stopping data flow (Mutual Authentication Scheme), highlighting suspicious traffic to other nodes in the network (MECshield, NBC-MAIDS, Multi-access Edge Computing, Fast Path, Classifier System), or diverting attack traffic (Honeypot).

Detection of attacks deals in correctly detecting that the traffic flow is due to an attack. These techniques utilise machine learning (Machine Learning Classifier Algorithms, BLSM-RNN, Fuzzy Logic, Deep Learning) and event processing (CEPID, Sampling-based Approach) in order to detect attack traffic, in some cases, with very high accuracy. The Machine Learning Classifier Algorithms technique had a recorded detection accuracy in real time IoT devices of 0.99%.

Mitigation of attacks deals in stopping a detected DDoS attack. This attack mitigation is implemented by blocking dataflow from malicious nodes within the network (SDN and SVM, ECESID, Deep Reinforcement Learning, and SDN).

III. Relation of Prior Work to the Project Problem

Subsubsection text here.

IV. Conclusion

The conclusion goes here.

Acknowledgment

The authors would like to thank...

References

[1] *The growth in connected iot devices is expected to generate 79.4zb of data in 2025, according to a new idc forecast*, Jun. 2019. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017, ISSN: 1558-0814. DOI: 10.1109/MC.2017.201.

[3] M. M. Salim, S. Rathore, and J. H. Park, "Distributed denial of service attacks and its defenses in iot: A survey," *The Journal of Supercomputing*, Jul. 2019, ISSN: 1573-0484. DOI: 10.1007/s11227-019-02945-z. [Online]. Available: https://doi.org/10.1007/s11227-019-02945-z.

[4] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, *A multi-level ddos mitigation framework for the industrial internet of things*. [Online]. Available: https://ieeexplore.ieee.org/document/8291111/.

[5] J.-P. A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier, and A. Chehab, *Securing internet of medical things systems: Limitations, issues and recommendations*, Dec. 2019. [Online]. Available: https : / / www . sciencedirect . com / science / article / pii / S0167739X19305680.