Appendix A:

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 an increasing number of Distributed Denial of Service (DDoS) attacks. Following the Mirai botnet attack in 2016, it has become apparent that there is much work required in securing IoT networks. Due to the relatively low available resources in IoT devices, there is a need to implement either non-resource intensive security features on the devices themselves, or to implement more stringent security for these devices at the level of the network.**

***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 re-routing leads to the "denial of service" aspect of the attack.

In order to generate such large volumes of data, an attacker uses multiple devices for transmission of malicious data packets. The "distributed" aspect of the DDoS attack comes from the multiple devices which are infected with malware, placed on the devices by the attacker. 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. Due to their relative abundance, Internet of Things devices have become a target for these types of attacks in recent years. IoT 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. Once this malware is uploaded to the device, the attacker can begin to flood the desired network with traffic[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]. As such, it is clear that there is a need to secure these devices, and the networks in which these devices are utilised. As IoT devices become more prevalent in different areas and industries, it becomes increasingly important to not only protect the data being generated, but also to protect the greater network as a whole which is processing this data.

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. Devices within this sector can be in control of, for example, safety systems, and as such, their continuous operation is of vital importance.

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. With an increase in the number of attacks on similar systems, there is the concern that the implementation of such systems could be hindered if more robust security systems are put in place.

II. Review and Analysis of Prior Work

A. Distributed Denial of Service Attacks and its Defenses in IoT: A Survey

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.

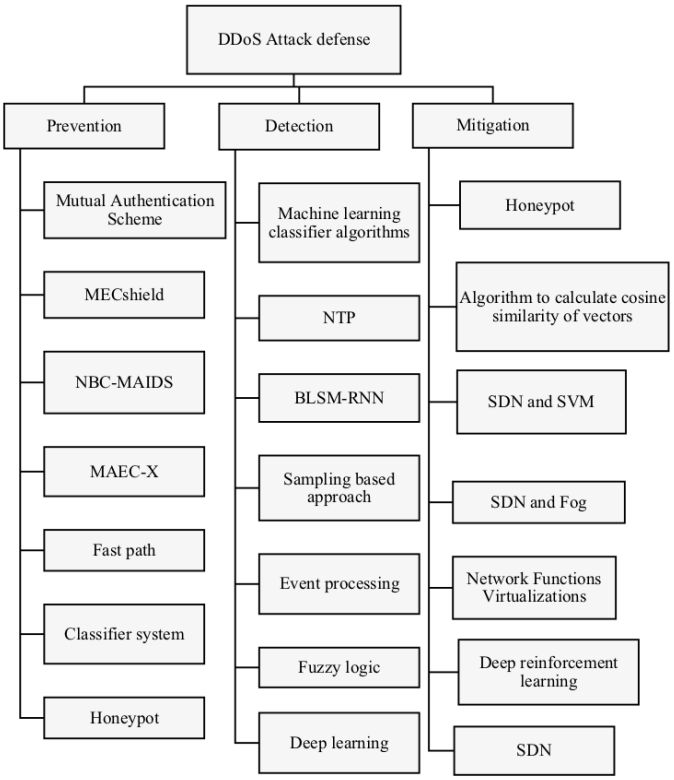

Fig. 1: Salim et al. DDoS attack Defence techniques[3]

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). Honeypot mitigation techniques were shown experimentally to increase attack detection efficiency by up to 60%.

The survey of Salim et al.[3] presents excellent distinctions between types of DDoS attacks, and some of the solutions which are currently being presented. While this survey is useful as an overview of, and introduction to these techniques and solutions, it does not present any new solutions apart from general security information such as "Change passwords", and "Implement a firewall".

B. A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things

With the increasing number of IoT devices being used within industry, and the growing importance of IIoT within the "Industry 4.0" concept, there is an increasing need to secure the data and data systems being used. Within industrial settings, the data being handled by these IoT systems could be vital in terms of safety systems, or mission-critical systems within production. As such, Yan et al. have presented a Multi-level DDoS mitigation framework (MLDMF) which utilises software defined networking (SDN) for the purposes of managing and securing IoT devices[4].

Yan et al. acknowledge that the defence systems available to IoT devices are "unsubstantial". The MLDMF proposed consists of three levels, the edge, fog, and cloud computing levels. Each of these levels serves its own purpose in securing the IIoT network. The edge computing level provides gateways with higher computational power than the IoT devices used in the network, which can implement more "traditional" security features, such as IP address concealment, and malicious software detection.

The fog computing level analyses data from the edge computing level, and, using a number of techniques, can make decisions on how to handle the data. The three described techniques are collect-detect-mitigate (CDM), honey-pot-detect-react (HDR), and cloud-detect-fog-mitigate (CDFM). CDM

allows for modifications to the networks bandwidth based on properties of the traffic. HDR can redirect traffic to a virtual IoT device in order to perform analysis. This technique allows for stopping malware from affecting the network, and allows for modifications to policies based of any new information gained from captured traffic. CDFM shares information between the cloud and fog computing levels in order to inform decision on dropping packets which may be from malicious sources.

The cloud computing level implements machine learning techniques in order to analyse the large amounts of data flowing through the network. This information can be used for the detection and prediction of DDoS attacks, based on the incoming data. Experimentally, the implementation of the proposed MLMDF improves performance within a network undergoing a TCP SYN flood attack by approximately 37.03%.

The use of SDN's for management of IoT devices and the traffic within the network have the disadvantage of adding overhead to the network. There is also the added cost of hardware for the implementation of the proposed system, requiring honeypot servers, and gateways to act as controllers. While the proposed solution may be viable, and these costs may be minimal in the context of an industrial setting, the current scope of the project is more focused on the evaluation of security improvements within the IoT network.

C. Securing Internet of Medical Things Systems: Limitations, Issues and Recommendations

The medical applications of IoT devices have become apparent in recent years. However, with the sensitive nature of the data being generated, privacy and security are of major concern. Yaacoub et al. present an in depth analysis of the dangers of IoMT devices, a number of commonly faced attacks, and a discussion on the possible solutions to these issues[5].

The three relevant recommendations made within this study are the implementation of lightweight cryptographic algorithms for security, alongside a lightweight authentication protocol, and a layered IoT secutrity architecture. The lightweight aspect is key in this assessment, as IoT devices do not have the resources to implement more robust solutions. One suggested security algorithm is the dynamic structure cryptographic algorithm, which is discussed further in Section II-D.

The layered security architecture, much like the MLDMF, separates security responsibilities between different levels. Unlike the MLDMF however, these layers define Quality of Service (QoS) parameters. Due to the nature of the application, IoMT devices must give accurate, real-time feedback. As such, this "zero-tolerance" for error must be represented within the QoS demands of the system.

The proposed use of dynamic structure cryptographic algorithms, and lightweight authentication protocols would greatly improve security within IoT networks. A low latency, non-resource intensive authentication scheme would allow for transmission of data between trusted devices, while allowing real-time processing of data. While focused mainly on IoMT, the insight provided by this study can be translated to IoT in general.

D. One Round Cipher Algorithm for multimedia IoT devices

There is a clear need for a lightweight algorithm for the encoding and decoding of information being transmit between devices in an IoT network. Noura et al. present such an algorithm in the context of Multimedia IoT (MIoT) devices. The proposed solution uses pseudo-random keys for encryption, greatly increasing the difficulty of decoding intercepted transmissions[6].

A number of constraints were considered in the development of this algorithm, including the limited resources available to IoT devices, and the need for an algorithm which can be implemented across devices of varying performance. This leads to a lightweight algorithm which may be used across a number of different devices, regardless of the resources available to that device.

In order to test the robustness of this algorithm, a number of tests were performed, separated under headings which include "Statistical analysis", "Visual degradation", and "Resistance against well-known types of attacks". With regards to the statistical analysis, the algorithm was shown experimentally to have very low correlation between adjacent pixels of the encoded image, with output values of close to zero. With regards to visual degradation, there was a signal-to-noise ratio (SNR) of 8.5894dB, which is regarded within the study to be a "low value", showing that the algorithm has acceptable robustness to degradation during encoding and decoding. Through a number of attack tests, the algorithm was shown to be robust to statistical attacks, and the size of keys used attributed to robustness to brute force attacks.

In terms of performance, when tested on two common embedded Linux platforms, the Raspberry Pi Zero W, and the Raspberry Pi 2, this algorithm gave encryption time gains of up to 29%, and decryption time gains of up to 33% when compared with a similar implementation.

One suggestion made in this study is that the algorithm has been implemented in C, whereas the implementation compared to with regards to performance is implemented in assembly. As such, further performance benefits could be gained from this lower level implementation.

This algorithm proposal demonstrates that a lightweight, "flexible" cryptographic algorithm can be implemented in a robust and highly performing manner. While the proposed algorithm

is intended to be used in the context of multimedia transmissions, and is tested in the transmission of an image, it is clear that the uses of the algorithm could be extended beyond this scope.

III. Relation to the Project Problem

The focus of this project will be to evaluate IoT systems in terms of the devices, networks, and operating systems for their susceptibility to DDoS attacks. As such, the survey of Salim et al.[3] provides an excellent background in the types of attacks, and is a starting point for assessing the types of solutions which are available to deal with these attacks. By understanding the types of attacks which commonly occur, more accurate evaluations can be performed between IoT systems.

IIoT is becoming a large source of data, and accounts for a large number of IoT devices. The proposal laid out by Yan et al.[4] gives an insight into how security issues within industry are being approached. This type of system can be investigated as an IoT network as a whole. Simulation of this type of network is a possible solution for the evaluation of a network consisting of SDN gateways and multiple controllers.

The suggestions laid out in the work of Yaacoub et al.[5] can clearly be applied to IoT networks and devices of all types, and are not specific to the field of IoMT. The implementation of a lightweight authentication protocol for IoT networks is an area which could be investigated further within the scope of the project.

The dynamic structure cryptographic algorithm proposed by Noura et al.[6] shows promising results in terms of relative performance and robustness. An evaluation of these algorithms, or potentially an implementation should be further investigated, and are completely within the scope of the project. The proposed algorithm appears to solely be implemented for the purpose of transmitting images, however the extension of this algorithm to other data types could prove useful for security.

It should be noted that these solutions can all potentially be implemented in various combinations. An in depth evaluation should consider any permutation of the aforementioned solutions. For the purposes of testing and evaluating these solutions, either simulation or virtualization will be used. While simulation will require less available computing resources, it is possible that virtualization of the network, as described in [4] will provide a more complete insight to the effects of changes to network level, or operating system/device level parameters.

IV. Conclusion

It is clear from the completion of this literature review that there are a number of proposed solutions for the current issues of security with regards to IoT devices and DDoS attacks. As the scope of the project is to evaluate IoT systems at the operating system (OS), network, and device levels for their susceptibility to attack, the solutions discussed in this review can be used as a baseline for improving upon.

Further work must be done in order to determine the open source tools which will be used for the evaluation of these systems. As this literature review deals solely in the solutions to the security issues in these networks, i.e. the mitigation and detection techniques used, an assessment must follow into the available tools for the purposes of evaluation of these networks.

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.

[6] H. Noura, A. Chehab, L. Sleem, M. Noura, C. Raphaël, and M. M. Mansour, *One round cipher algorithm for multimedia iot devices*. [Online]. Available: https://link-springer-com.dcu.idm.oclc.org/content/pdf/10.1007/s11042-018-5660-y.%20pdf.