Preventing Distributed Denial of Service Attacks in IoT Networks
UP879148

1.0 Abstract

The rapid rise of the Internet of Things has resulted in a large increase in the amount of small IoT networks (less than 15 devices) being depended on for a wide range of tasks. Many of these networks use cheap mass-produced components which contain security vulnerabilities, exposing the network to a wide range of attacks. One of the most serious attacks is known as Distributed Denial of Service (DDoS) where multiple attackers aim to shut down an IoT network. The goal of this paper is to investigate existing methods of preventing a flood-based DDoS attack on a small IoT network and then propose a solution which builds on existing research, with the aim of improving the efficiency and latency over existing solutions. The paper created a small-scale lightweight firewall which was put on an IoT network and the data transmission results where recorded before and after firewall implementation. This allowed for analysis of latency and overall effectiveness. Overall, the results of the firewall experiment showed the proposed solution was effective at preventing DDoS attacks on small IoT networks. Additionally, the solution had a latency of 1.56% which is better than the expected 2.5%. This means that the initial aim that the paper set out to solve was a success as the solution exceeded the initial hypothesis.

2.0 Introduction

The world is becoming ever more dependent upon small-scale IoT networks to perform a wide range of tasks. In 2015 it was predicted that there are between 25-50 billion IoT devices currently being used with an annual growth of 32% (Sheth, 2016) - highlighting the importance of IoT research. However, the rapid growth of IoT has resulted in many security vulnerabilities. (Alladi et al, 2020) One of the most common and damaging attacks is a Distributed Denial-of-Service (DDoS) attack where multiple attackers attempt to overwhelm a network in order to deny availability. (Douligeris & A. Mitrokotsa, 2003).

This paper aims to investigate existing methods of DDoS prevention in small-scale (less than 15 devices) IoT networks and build upon the existing research. The ultimate aim is to propose a new solution which can build and improve upon the existing methods and research of DDoS prevention. The reason for focusing the scope of the research to small-scale IoT networks is that homes and small businesses have great potential for IoT deployment. (F Santoso & N Vun, 2015) Additionally, there is a limited amount of physical components available for this research so limiting the scope to a small-scale IoT network is suitable.

4.0 Background

4.1 IMPROVED CONFIGURATION

The correct configuration is essential for security and the smooth running of a network. Poorly configured or maintained devices, passwords and settings can expose a network to a wide range of attacks. (Alladi et al, 2020)

Research into DDoS attacks on IoT networks conducted by Constantinos Kolias et al. demonstrates how the Mirai Botnet can cause a DDoS attack on weakly configured IoT devices by constantly propagating to them. The study states that once devices are infected the botnet has the infected devices constantly propagate to the server with the aim to overload it and shut it down.

Constantinos et al highlight 5 key vulnerabilities which can make IoT devices especially vulnerable to botnets such as the Mirai Botnet. These are constant and unobtrusive operation, feeble protection, poor maintenance, considerable attack traffic and noninteractive or minimally interactive user interfaces. The reason is that the rapid rise of IoT has led to devices that have led to often exposed devices with a limited capacity of which often the people responsible do not have a full understanding of.

Consequently, the paper's suggested solution is for users and system administrators to be more aware of the risks posed and the IoT components they are using, as it claims that most DDoS attacks on IoT networks are a result of human error.

Other studies such as one by J. Margolis et al back up the research done by Constantinos et al. J. Margolis et al reinforce the key points that improving the configuration of the IoT network can make significant improvements in preventing DDoS attacks. Some such solutions mentioned are changing the network credentials to prevent unauthorized access and closing unused ports to reduce potential attack avenues.

The scope of the research shows that poor network configuration can be universal, meaning it can be a major issue for all networks from the smallest to the biggest and by extension, the solutions can apply to everyone emphasising its importance. However, the problem of poor configuration is generally easy to fix with an increase in awareness from the network manager.

4.2 FIREWALL PREVENTION

A firewall aims to filter out unauthorized traffic coming into the network, which can be done by IP, protocol or ports, such as packets sent by an attacker during a DDoS flood attack. (Bhosale et al, 2017) Firewalls can provide a significant increase in security and are often the first line of defence against an external threat to the network. There are five main types of firewalls being, Packet Filtering, Circuit-Level Gateways, Application Gateways, Multilayer Inspection Firewalls and Stateful Firewalls. Firewalls are configured using rules which determine what packets are allowed into the network and which packets are rejected. (Salah-ddine Krit & Elbachir Haimoud, 2017)

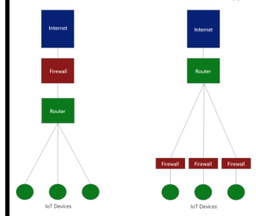

Figure 1 - Network firewall configuration comparison.

One method of implementing a firewall on an IoT network is to implement a distributed firewall. This involves having a firewall on each IoT device rather than on the entry point of the network. This is more costly than having a single firewall for the whole network and is also far less scalable. However, the solution offers the advantage that there is no single point of failure in the network and also provides a performance advantage as there is no bottleneck unlike in a traditional firewall network. (Ryan Lund et al, 2020)

Research has also been carried out to create a low-cost and open-source Firewall for IoT networks. The system involves a Raspberry Pi which acts as an intermediary device between the network and the router, with all traffic passing through it. The experiment conducted showed that their proposed solution was capable of IPv4 masquerading, spoof protection and preventing MITM attacks, as well as DDoS. While effective, it is mentioned that the component represents a single point of failure and the limited computational power may get overwhelmed. (Gupta et al, 2017)

The research mentioned both state that firewalls are necessary and substantial if any network is to be secure from outside attacks (Salah-ddine Krit & Elbachir Haimoud, 2017), highlighting the important role they play in network security. The research shows two avenues of IoT firewall development and research, being the distributed firewall solution which offers higher performance and security at the expense of being more expensive and far less scalable and also the traditional single firewall which can be implemented at low-cost and still provides good protection to a network.

4.3 MACHINE LEARNING PREVENTION

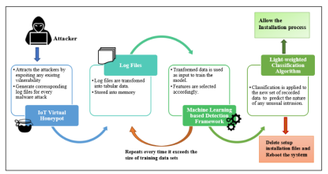

Figure 2 - Virtual Honeypot diagram. (Vishwakarma & Jain 2019)

Existing research demonstrates how machine learning can be used to prevent DDoS attacks on IoT networks. A framework is known as the IoT Virtual Honeypot and aims to lure attackers into a virtual device so that their methods of attack can be analysed in order to gain a better understanding of new malware and attacks. The research shows that the Virtual Honeypot is effective for catching a wide range of botnets and keeping them away from the real network. (Vishwakarma & Jain 2019)

Other research into using machine learning tools to detect and prevent DDoS attacks on IoT networks shows that packet-level machine learning can separate normal traffic from the attacker's traffic. To do this, the paper conducts an experiment involving creating a pipeline for detecting anomalies. This involves capturing the traffic and recording information on it. Traffic can then be grouped and classified and using methods such as decision trees and deep neural networking it is possible to differentiate legitimate traffic from the attacker's traffic. Overall, the results of the study suggest that the framework effectively detects and prevents DDoS attacks on IoT devices. However, it is stated that more research is required to make such tools applicable in a real-world setting and the research was carried out under the assumption that the network includes a device such as a router. (Rohan Doshi et al, 2018)

While the area of using machine learning tools to prevent DDoS attacks on IoT devices is effective and set to be expanded upon over the coming years. The solutions mentioned should be taken in their proper context/scope and are not as applicable to the small/average IoT network, which is the focus of this paper, as other solutions such as a Firewall. The main reason is that many IoT devices currently lack the resources for real-time machine learning detection tools. For potentially larger/commercial IoT networks these solutions are more applicable. It is suggested that a cloud-based solution could be an area of further research to provide real-time DDoS detection to devices with less resource capacity. (Vishwakarma & Jain 2019)

3.0 Problem Statement

This paper aims to assess the effectiveness of a firewall solution for preventing DDoS attacks on a small IoT network. The experiment will be run with and without a firewall (independent variable). Then a critical analysis, for both experiments, of the rates of data transmission (Mb/s) (dependent variable) to measure latency and the total downtime (seconds) of the server to evaluate the effectiveness of the firewall.

The hypothesis predicts that the proposed solution will be able to effectively prevent a flood attack through packet filtering, while having a data transmission latency of around 2.5%.

5.0 Design

This experiment will involve building an IoT device and connecting it to a server. DDoS attacks will be performed on the server with and without the packet-filtering firewall in place. This will provide a set of results that will enable an analysis of the firewall's effectiveness.

The reason for the experiment focusing on a packet-filtering firewall is because the research into existing methods of DDoS prevention mentioned in 2.0 demonstrated that firewalls are an optimal solution for protecting a small IoT network, compared to machine learning which requires more resources than our small network components can handle. There seems to be a gap in the existing firewall research for a small IoT network. The existing solutions that were researched proposed designs that either used a virtual firewall on each IoT device or a single firewall on a separate component. This experiment aims to combine the two methods to have a single firewall which will reduce the cost compared to having a physical component and will increase the scalability and maintainability compared to firewalls on each IoT device.

The experiment will be using a NodeMCU/ESP8266 which is a Lua based chip that has Wi-Fi capabilities. (NodeMCU Documentation, 2021) The NodeMCU will be connected to a red and green LED using a breadboard and programmed in Lua using ESPlorer. The green LED will be turned on if there is a connection to the test server. The red LED will be turned on if there is no connection to the test server. This means we will know if the DDoS has impacted our IoT device's ability to use the internet by the colour of the light.

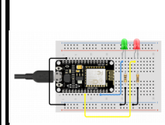

Figure 3 - Circuit diagram.

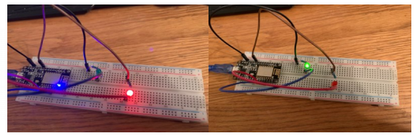

Figure 4 - Physical circuit (no connection).

Figure 5 - Physical circuit (connected).

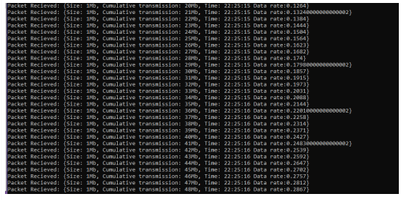

Figure 6 - Test server accepting packets.

There will be a simple NodeJS based TCP server running on a localhost 127.0.0.1:8080 that will be able to communicate with the IoT device and receive and send packets of data. Telnet will be used to connect to the server and send data to the server, this allows for the creation of as many connections as needed. Additionally, the server is able to write packet information to a text file which allows the data to be more easily recorded for analysis.

The server is configured to have a capacity of 1Mbps. During the experiment the IoT device will be sending 0.2Mbps of data to the server, this will occur for one minute uninterrupted. There will be three attackers in this experiment each of which will send 0.3Mbps to our server. Every 20 seconds we will introduce a new attacker meaning after 60 seconds the total rate of transmission to our server exceeds the 1Mbps capacity which will shut down the server.

During the experiment, the time at which the server went down and also the transmission rate of the data from the IoT will be recorded to see if the firewall has had an impact on performance. The data will then be represented in a series of graphs and tables which can be analysed for patterns.

While it is expected that this experiment should provide good data for assessing the effectiveness of the proposed packet filtering firewall, there are constraints and limitations. Firstly, there was a limited amount of physical components available to build the IoT device, this meant that in the experiment there is only one such device. Secondly, there was a limitation in the software available. The software needed to be free to use and have sufficient capabilities to model an IoT network, initially GNS3 was used, which is a tool for visualising and simulating networks (GNS3 Documentation, 2021), however, it has limited wireless functionality so was not suitable. Finally, due to Covid-19, it was impossible to run the experiment on a network that is free of traffic. There are always going to be other devices taking up bandwidth. This could have a minor impact on the latency measurements. To mitigate this, the experiment was conducted at times where the network is light on traffic such as at night. Additionally, the experiment will be repeated 20 times to aid the reliability and consistency of the data.

7.0 Discussion

The evaluation of the results show that the firewall solution is effective at stopping a DDoS packet-flood attack on a small IoT server. The results show the firewall was able to effectively filter incoming traffic, thus preventing a downing of the server by attackers. This is shown when comparing figure 8 and figure 9. At 60 seconds the transmission in figure 8 terminates when the total rate exceeds the server capacity of 1Mb/s. In contrast figure 9 does not shut down due to the attacker's packets being filtered.

The results also show slightly better performance than outlined in the hypothesis being a 1.56% drop compared to the 2.5% expected. There is a trend however, that as the data being sent by attackers increases there is a small drop in performance. However, this was expected and the increase in latency is not significant. The visualisation of this can be seen in Figure 7.

However, the results are limited in several areas which should be taken into account. As mentioned in the design section, there was a limited amount of components which were available meaning the results do not show how scalable the solution would be with more devices or with a higher rate of data transmission. It is possible that latency would be increased further, to an undesirable level, with more IoT devices and with a higher bandwidth.

While the limitations limit the scope, the results do show a high degree of reliability and repeatability for the size of the network which was tested. The experiment was repeated 20 times and the data was fairly consistent throughout. There were some small outliers in the measurements however, it is likely these were a result of external factors which could not be mitigated fully such as a reduction in Wi-Fi speed and the amount of repetitions done indicate they were not caused by the firewall.

8.0 Conclusion

This paper aimed to determine the effectiveness of a proposed low-cost and lightweight packet-filtering firewall in a small IoT network at preventing packet-flood DDoS attacks. The initial hypothesis predicted that the firewall would be effective at filtering out unauthorized packets and would have a latency of around 2.5%.

To test the hypothesis the experiment used a NodeMCU/ESP8266 based device connected to a local server. The device contained LEDs to show if the device was connected or not. Packet-flood attacks were simulated on the server with the aim to measure downtime and latency to evaluate the effectiveness of the firewall solution. The experiment was conducted 20 times to ensure repeatability and consistency.

The results aligned with the initial hypothesis showing that the solution was effective at preventing a packet-flood DDoS attack on a small IoT network. The server was not shut off by the DDoS attack when using a firewall. Additionally, the latency was only 1.56% which is lower than the 2.5% predicted in the initial hypothesis. While successful it is important to view the results in their proper context. The limitations on hardware and network availability meant that the scalability of the solution could not be fully assessed.

9.0 Future Work

Further research into this area should focus on increasing the reliability and repeatability of the results presented in this paper. This can be done by addressing the limitations of the experiment. Future research should attempt to conduct the experiment using a high-quality IoT network with no existing traffic to reduce the chances of network fluctuations impacting the latency results.

Additionally, further research using higher data rates would be able to identify the effectiveness of the proposed solution in larger networks. While the design is aimed around small IoT networks, due to limitations in equipment and software the theoretical upper bound of data that the firewall can cope with was not able to be identified.

10.0 References

Alladi, T., Chamola, V., Sikdar, B., & Choo, K. R. (2020). Consumer IoT: Security vulnerability case studies and solutions. IEEE Consumer Electronics Magazine, 9(2), 17-25. https://doi.org/10.1109/mce.2019.2953740

Bhosale, K. S., Nenova, M., & Iliev, G. (2017). The distributed denial of service attacks (DDoS) prevention mechanisms on application layer. 2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS). https://doi.org/10.1109/telsks.2017.8246247

Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer Internet of things devices. 2018 IEEE Security and Privacy Workshops (SPW). https://doi.org/10.1109/spw.2018.00013

Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: Classification and state-of-the-art. Computer Networks, 44(5), 643-666. https://doi.org/10.1016/j.comnet.2003.10.003

ESP8266. (2021). Overview - NodeMCU Documentation. https://nodemcu.readthedocs.io/en/release/

Getting started with GNS3. (2021). GNS3 Documentation | GNS3 Documentation. https://docs.gns3.com/docs/

Gupta, N., Naik, V., & Sengupta, S. (2017). A firewall for Internet of things. 2017 9th International Conference on Communication Systems and Networks (COMSNETS). https://doi.org/10.1109/comsnets.2017.7945418

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. Computer, 50(7), 80-84. https://doi.org/10.1109/mc.2017.201

Krit, S., & Haimoud, E. (2017). Overview of firewalls: Types and policies: Managing Windows embedded firewall programmatically. 2017 International Conference on Engineering & MIS (ICEMIS). https://doi.org/10.1109/icemis.2017.8273003

Lund, R., Fenzl, A., & Villanueva, C. (2020). Distributed Firewall for IoT. https://scholarcommons.scu.edu/cgi/viewcontent.cgi?article=1163&context=cseng_senior

Margolis, J., Oh, T. T., Jadhav, S., Kim, Y. H., & Kim, J. N. (2017). An in-depth analysis of the Mirai Botnet. 2017 International Conference on Software Security and Assurance (ICSSA). https://doi.org/10.1109/icssa.2017.12

Santoso, F. K., & Vun, N. C. (2015). Securing IoT for smart home system. 2015 International Symposium on Consumer Electronics (ISCE). https://doi.org/10.1109/isce.2015.7177843

Sheth, A. (2016). Internet of things to smart IoT through semantic, cognitive, and perceptual computing. IEEE Intelligent Systems, 31(2), 108-112. https://doi.org/10.1109/mis.2016.34

Vishwakarma, R., & Jain, A. K. (2019). A honeypot with machine learning based detection framework for defending IoT based Botnet DDoS attacks. 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI). https://doi.org/10.1109/icoei.2019.8862720

6.0 Results

Time (seconds)	Transmission Rate - no firewall	Transmission Rate - firewall
5	0.198 (-1%)	0.2 (%)
10	0.2 (0%)	0.2 (%)
15	0.2 (0%)	0.198 (-1%)
20 (first attacker)	0.197 (-1.5%)	0.198 (-1%)
25	0.199 (-0.5%)	0.196 (-2%)
30	0.2 (0%)	0.197 (-1.5%)
35	0.2 (0%)	0.199 (-0.5%)
40 (second attacker)	0.199 (-0.5%)	0.195 (-2.5%)
45	0.198 (-1%)	0.196 (-2%)
50	0.2 (0%)	0.194 (-3%)
55	0.2 (0%)	0.196 (-2%)
60 (third attacker)	0 (0%)	0.194 (-3%)

Table 1 - Average transmission rate before and after firewall implementation.

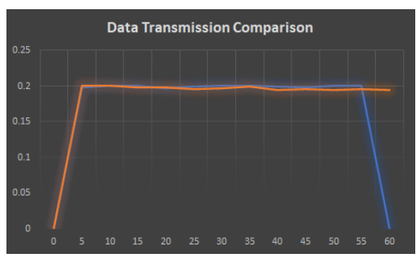

Figure 7 - Comparison of transmission rates with and without firewall.

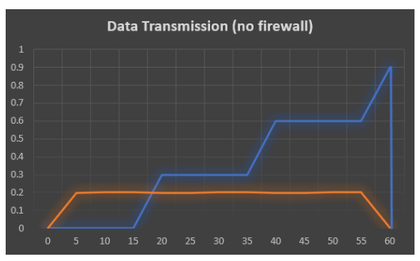

Figure 8 - Transmission rates without the firewall.

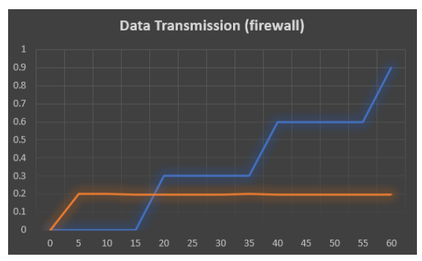

Figure 9 - Transmission rates with the firewall.

Table 1 shows the transmission rates for the IoT device before and after the firewall was implemented as well as the percentage of the transmission drop from 0.2Mb/s. The average rate without a firewall is 0.199Mb/s (-0.375%) while the average rate with a firewall is 0.197Mb/s (-1.56%). Consequently, the results with the firewall show an average data transmission reduction of 0.002Mb/s (-0.1%). Additionally, for both, as each attacker was introduced there was a slight performance impact. Without a firewall, the performance seemed to recover somewhat. With a firewall, no attackers saw a data transmission reduction of 0.5%, after the first attack was introduced there was a data transmission reduction of 1.77%, after the second attacker was introduced the data transmission reduction was 2.5%.

Figures 7, 8, 9 visualise the information shown in Table 1 into line graphs.

Figure 7 shows a comparison between the data transmission with and without a firewall. The blue line represents the transmission without a firewall and the orange line represents the transmission with a firewall.

Figure 8 shows the transmission rate with no firewall. The blue line represents the attacker's transmission and the orange line represents the IoT device's transmission. The extra line shows that once the attackers reached 0.9 the server crashed.

Figure 9 Shows the transmission rates with the firewall. The line representations are the same as figure 8.