Annual ADFSL Conference on Digital Forensics, Security and Law

2022 Proceedings

Smart Home Forensics: Identifying Ddos Attack Patterns on Iot Devices

Samuel Ho
Purdue University

Hope Greeson
Purdue University

Umit Karabiyik
Purdue University

Scholarly Commons Citation

Ho, Samuel; Greeson, Hope; and Karabiyik, Umit, "Smart Home Forensics: Identifying Ddos Attack Patterns on Iot Devices" (2022). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 6.
https://commons.erau.edu/adfsl/2022/presentations/6

SMART HOME FORENSICS: IDENTIFYING DDOS ATTACK PATTERNS ON IOT DEVICES

Samuel Ho[1], Hope Greeson[2], Umit Karabiyik[3]
Purdue University
Computer and Information Technology
West Lafayette, IN 47907, United States
[1]ho176@purdue.edu, [2]hgreeso@purdue.edu, [3]umit@purdue.edu

ABSTRACT

Smart homes are becoming more common as more people integrate IoT devices into their home environment. As such, these devices have access to personal data on their homeowners' networks. One of the advantages of IoT devices is that they are compact. However, this limits the incorporation of security measures in their hardware. Misconfigured IoT devices are commonly the target of malicious attacks. Additionally, distributed denial-of-service attacks are becoming more common due to applications and software that provides users with easy-to-use user interfaces. Since one vulnerable device is all an attacker needs to launch an attack on a network, in regards to IoT devices, there is a need for businesses and homeowners to find out methods of predicting incoming DDoS attacks. The earlier a DDoS attack is discovered, the earlier mitigation and prevention techniques can be applied. One way to predict incoming DDoS attacks is from emerging patterns. To discover these patterns, we constructed a home IoT environment and conducted LOIC and Slow Loris DDoS attacks against this environment. This setup led to the discovery of five distinct patterns that emerged when the IoT devices were being DDoS-ed. In this paper, we will discuss the DDoS attack used, home IoT environment, normal vs attacked traffic patterns, and make recommendations for future research.

Keywords: Internet of Things, Distributed Denial-of-Service, Pattern Analysis, LOIC, Slow Loris, Digital Forensics

1. INTRODUCTION

The Internet of Things (IoT) is influencing our daily routines from the way we react to the way we behave. Some examples of IoT devices are air conditioners that you can control with your smartphone, smart cars that can determine the shortest route, and smart watches that can measure and record statistics of every workout session. These devices communicate with each other over the network environment that they are connected to. In this era of globalization, many homeowners have adopted these IoT devices into their households, evolving their homes into "smart homes".

The increasing amount of IoT devices connecting over the network brings challenges in terms of malicious attacks on the devices (Abomhara & Køien, 2015). Specifically, Distributed Denial-of-Service (DDoS) attacks are becoming more common on IoT devices and more challenging to combat. This can cause concerns on the security aspect of these devices as DDoS attacks are usually a precursor to ransom. Hence, early detection of suspicious activity in IoT devices is salient. In order to achieve this, collecting evidence of network patterns, examining these patterns, and interpreting both the origin as well as the aftermath of a DDoS attack through forensic analysis is necessary for limiting future attacks.

In this paper, we analyze the effects of DDoS attacks on multiple household IoT devices in terms of network traffic patterns. To investigate this, it is imperative that the tests are conducted in a private network environment in order to run applications of questionable security. More specifically, the analysis includes evaluating the metrics of the DDoS attack and any distinctive recognizable patterns. Other methods of analysis include using a packet capture analyzer to scan the network for any type of malicious activity to generate accurate reports for further investigation of the attack.

Previous research focused on using three forensic aspects: Cloud forensics, network forensics, and device-level forensics to digitally investigate IoT forensics (Kebande & Ray, 2016). However, the application of these methods is primarily for the industrial IoT sector. The majority of smart homes simply do not have the forensic preparedness and resources to conduct such analysis. Additionally, Sedaghat (2020) focused on network forensics to detect DDoS on mobile networks by sending large amounts of traffic to figure out patterns of DDoS attacks. However, the methods used are for mobile networks rather than smart home IoT devices.

The remainder of this paper is structured as follows: Section 2 provides the review of the literature in regards to DDoS attacks and IoT devices. Section 3 discusses the methodolgy which includes all variables, definitions, and validity threats related to the present study. It also discusses the applications used to run the DDoS attack, the networking aspect of the present study, as well as how the collected data will be interpreted. Section 4 highlights the results and findings of this study. Finally, Section 5 summarizes the entire study and the contributions acquired from the analysis.

2. RELATED WORK

It is imperative to understand the differences between legitimate and non-legitimate packets in order to further analyze DDoS attacks and their patterns. Research was conducted by Thapngam et al. (2014) to investigate DDoS attack patterns from regular traffic by overloading the server, which was linked to numerous PCs with high traffic. The experiment employed infected zombie machines, also known as bots. The study focuses primarily on two methods for analyzing arrival rates using the correlation coefficient as data. This is an excellent way for distinguishing packets between DDoS attack origins and legitimate users, including proxies (Thapngam et al., 2014). The study proposes two approaches for measuring packet arrival data from a single questionable source utilizing correlation, with the outcome of a dependent or independent connection (Cheng et al., 2002). In the dependent connection of the data, the predictable aspects appeared to be strong (Thapngam et al., 2014). Data that is unpredictable is trended to have an independent correlation (Barry et al., 2001). The researcher could push the proper actions to the right packets because the degree of pattern behavior could be measured. However, the attackers' packets must be blocked, but the user packets must get through the server (Thapngam et al., 2014).

IoT gadgets are becoming increasingly popular as more people integrate them into their homes. The focus of Bhardwaj et al. (2019) was on the security flaws found in IoT devices. As a result, there is a knowledge gap in the literature about the privacy and security of these devices, as well as the most effective ways to study them. Hutchinson et al. (2020) wanted to apply IoT forensics, so they created their own IoT forensics lab at Purdue University in order to do so. Similar to the study done in our paper, the researcher connected 11 devices that were included in the smart home lab. Linking each device with the Google Nest Hub Max via the Google Home app enabled the devices to operate with each other interactively, such as controlling the smart light bulb from the Google Nest Hub Max itself (Hutchinson et al., 2020). Through IoT forensics, they discovered user data such as username, full name, email, make and model of mobile device, and OAuth credentials. Although some of the information found such as zip code, names of the devices, etc may not be useful, it can be used as reconnaissance to gain further access into the home network which can lead to spear-phishing or blackmail. They also proposed four possible smart home threat scenarios proposed by Bhardwaj et al. (2019). The most interesting of which would be the Alexa botnet environment issue. This is when Alexa-enabled devices can be used to create a botnet environment that can cause network traffic problems through all connected devices that could result in their malfunctioning. What was interesting is that it was mentioned in the paper that this is similar to a DDoS attack in terms of how critical the threat is (Hutchinson et al., 2020).

One of the most popular network analyzer tools is Wireshark, which was used in this paper to conduct forensic analysis on the DDoS attack. A study was done by (Ndatinya et al., 2015) to analyze the behavior of packets in the network using Wireshark. Packet analysis is extremely significant for two reasons. For starters, packet analysis is part of the starting points of everything vital to a network since it helps us to know the condition of the network in advance of problems occurring. Second, packet analysis is important for diagnosing a network in the event of an attack, and it allows network managers to check into cables and determine the traffic crossing them or any abnormalities that may exist (Ndatinya et al., 2015)(Varghese & Muniyal, 2021). The research analyzed various packets related to different types of attacks and how to determine those attacks with Wireshark, one of which focused on identifying BitTorrent DDoS attacks. Although regular traffic was identifiable once the attacks were injected, it was also evident which attacks were from BitTorrent. A DNS query to resolve the IP address for www.bittorent.com was found in several packets (Ndatinya et al., 2015). The client establishes a TCP connection with the BitTorrent server by sending a SYN signal during a three-way handshake. In succeeding packets, the same client connects to additional servers, such as www.surveymonkey.com and c5.zedo.com, to retrieve data. Because of the anomalous TCP packets, this BitTorrent data transfer is most certainly creating network congestion (Ndatinya et al., 2015). In our study, we followed a similar methodology on packet analysis as discussed in (Ndatinya et al., 2015).

3. METHODOLOGY

The present study's goal was to engage the depth of DDoS attacks on different household IoT devices through forensic analysis. To achieve this goal, we have launched our own DDoS attacks on a smart home environment. The following sections describe the proposed measures, design, lab environment, and data analysis for our study.

3.1 Research Measures

This study employed the single-group posttest-only design as the independent variable is manipulated with a single group and the group is measured. The independent variable is the type of cyberattack. The dependent variable is the presence of traffic patterns following a DDoS attack. This was operationalized as the result of the network traffic analysis on the household IoT devices. Thus, this study attempts to answer the question of "What are the network traffic patterns following a DDoS attack on household IoT devices?" In terms of validity, a possible threat to internal validity is that the entire study was done in a controlled lab environment, eliminating any outside influences and challenges that may occur in the real world.

3.2 Research Design

The primary goal of a Denial of Service (DoS) attack is to try to defeat a web server or host by giving it as much bandwidth as you can such that it breaks. Since they have a limited amount of bandwidth that they are allowed to use, the web servers or hosts will crash/go down if there are too many requests to that specific web page. A DDoS attack is an amplification of a DoS attack, using multiple computers to attempt the same type of attack. Bigger companies such as Google and Microsoft will be hard to bring down. However, smaller websites with less protection and bandwidth can suffer massive impacts on the amount of money they are making. In this case, we are not attacking a website, but rather a router that is responsible for providing layer 2 and layer 3 connectivity in terms of the Open Systems Interconnection (OSI) model.

Low Orbit Ion Cannon (LOIC) was used to conduct the DDoS attack (*Low Orbit Ion Can-*

non. [Software], 2020). LOIC was initially developed to be a network stress testing application by Praetox Technologies. After LOIC's public release, it is now one of the most maliciously used tools due to its user-friendly design and accessibility. The application is written in C#. The way LOIC works is that LOIC sends out continuous TCP, UDP, or HTTP packets to a target URL or IP, intending to disrupt service for a particular host. To broaden the attack surface, different number of treads (also known as bots) were used. Thus, LOIC was either ran with 100 treads, or 10,000 treads.

A Slow Loris attack is a type of DDoS attack that opens connections to a website. As connections end and a new connection frees up from someone else using the website, Slow Loris will repeatedly open up another connection until all the available connections are opened. The open source Python script that was used to run the Slow Loris attacks can be obtained from Github (Yaltirakli, 2015). The main purpose of the script was to open and maintain connections to the router such that when LOIC breaks the connections between the router and the IoT devices, Slow Loris takes up that connection, eventually denying any available connections from the IoT devices to the router. Since the script could only be run once per terminal, multiple terminals needed to be running simultaneously for Slow Loris to be effective. We ran the attack 5 times, each with an increasing number of terminals running the Slow Loris attack - 20, 40, 60, 80, and 100.

The devices that were available to us are a result of Hutchinson et al. (Hutchinson et al., 2020) who implemented a smart home laboratory. For the purposes of this paper, we will only be performing the DDoS attacks on 5 devices (see Table 1).

In terms of legality, it is legal to attack your own servers for stress-testing. However, it is considered a felony to perform a DDoS attack on a public or non-personal network according to the Computer Fraud and Abuse Act of 1986 (U.S. Government Printing Office, n.d.). Due to the possible legal issues that come with conducting a DDoS attack, ensuring that the architecture is set up in the private network is essential for this research. Upon inspection of the router, we discovered that the TP-Link Archer C1900 only has 4 ethernet ports, meaning we would have to deploy both wired and wireless infrastructure. We used the wireless access point of the TP-Link router, but did not connect a WAN uplink to the public domain as one would normally do. Instead, we set up the WAN interface on the TP-Link router and assigned the LAN gateway IP address to the WAN interface. The wireless infrastructure uses an RFC 1918 (Rekhter et al., 1996) compliant IP address scheme for our private network. All devices used were placed into a 172.16.1.0/24 network segment. DHCP assignment was used to assign IP addresses to the router and all the IoT devices (See Table 2).

3.3 Test Environment

The test environment was set up to mimic a real IoT household. The first step was to set up an internal network segment as discussed earlier. After pressing the WPA/Reset button at the back of the TP-Link Archer C1900 to factory reset it, we used the default TP-Link web GUI to configure the wide area network (WAN) and local area network (LAN) on a Dell Inspiron 15 3000 laptop. The Google Nest Hub Max was set up to connect to the LAN, which assigned it a DHCP IP address. A Samsung A50 smartphone was used as the central connection device. After hard resetting the Samsung A50, a Google account was created to allow downloads from the Google Play Store. The Google Home application was installed from the Google Play Store to allow connection to the Google Nest Hub Max. Next, three mobile applications - Wyze, Gosund, and August were installed to test the functionality of each individual device. After ensuring the Wyze camera, Gosund smart plug, and August smart lock were fully functioning independently, all three devices were linked on through the Google Nest Hub Max. Fig. 1 shows a visual representation of the logical network architecture.

Table 1: List of the IoT devices used in this study

Device	Description
TP-Link Archer C1900	Central router for LAN networking
Google Nest Hub Max	Smart hub to perform voice activated activities
August Smart Lock Pro	WiFi enabled home security device
Wyze Camera	Security camera
Gosund Smart Plug	Automation device

Table 2: IP addressing of the IoT devices used in this study

Device	IP Address
TP-Link Archer C1900	172.16.1.10
Samsung A5 Smartphone	172.16.1.141
Google Nest Hub Max	172.16.1.221
August Smart Lock Pro	172.16.1.133
Wyze Camera	172.16.1.151
Gosund Smart Plug	172.16.1.206
Dell Laptop	172.16.1.249

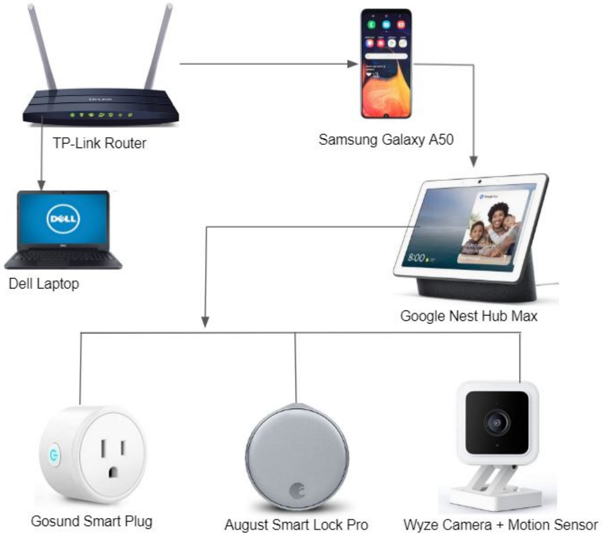


Figure 1: Logical Network Diagram

3.4 Research Analysis

Wireshark, an open-source packet analyzer, was used to capture the network traffic to be further analyzed. Wireshark was chosen for this experiment as it is the world's most popular network monitoring tool. It is used by many commercial and non-profit organizations, government agencies, and educational institutions because it provides a microscopic view of what's going on on their networks (Sharpe & Warnicke, 2011). Following the capture of DDoS packets, the data acquired during the attack was further analyzed to discover what sorts of packets are gathered, the patterns of this data, and the details of the attack.

Wireshark was used during the DDoS attack to begin collecting packets in live view, culminating a large set of packets from the attack. Both LOIC and Slow Loris were used as the attack application which was collected by Wireshark. The attacks were divided into segments for data collection, with each segment lasting 300 seconds. Time was recorded in seconds to ensure accuracy. We set a baseline by capturing an initial traffic sample with no attacks running. After the 300-second time frame was reached, the Wireshark packet capture was terminated and stored for further analysis after each section of attacks.

The captured packets were filtered in a number of ways to identify any distinguishing patterns between regular traffic and DDoS attack activity. The "I/O Graphs" tab was used to provide a visual representation of network traffic. This was the first step of comparing the patterns of an attacked graph versus the normal traffic. This phase of analysis was simply looking at the patterns of traffic flow over the network by filtering out all the IoT device's IP addresses as well as TCP error packets. This was to filter out all external traffic that was not a part of the IoT devices as well as TCP errors to ensure the most accurate data was analyzed.

The next phases of the analysis consisted of diving deeper into the attack surface by looking at the specific numbers and percentages to accurately compare normal traffic from attacked network traffic. This consisted of comparing the averages of packets per second, average bytes per second, and average packet size by looking at the file properties under statistics. The TCP error flags were compared by using the filter command "tcp.analysis.flag" and the average percentage was calculated and displayed in the form of a graph. The unexpected packet loss was also compared in the same manner as TCP error flags using the command "tcp.analysis.lost_segment or tcp.analysis.retransmission". Lastly, the packet length was investigated to see how much difference the size of the packet was transferred over the network as well as how fast those packets were bursting. This was analyzed using the packet length tab under statistics.

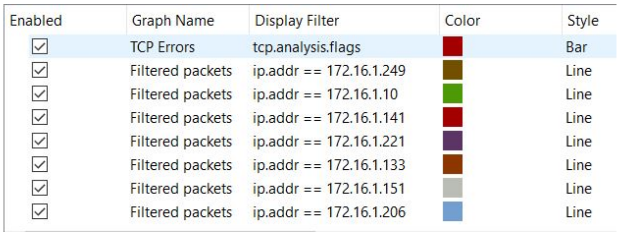
4. RESULTS

4.1 I/O Graph

The initial findings were done using Wireshark's I/O graph, and the patterns were filtered to display all of the IoT device's IP addresses as well as TCP Error flags. Fig. 2 shows the color coded filters, where it displays the red bar for TCP errors and the remaining lines are the IoT devices. The total number of packets in the normal traffic was 4207, whereas the average number of packets in the attacked traffic was 1774. The total amount of attacked traffic was only half of what the total amount of regular traffic was. Thus, we can conclude that a Slow Loris DDoS attack may slow down traffic by 50% on average.

Four I/O graphs were compared in order to visualize the findings. Fig. 3 shows the I/O graph for the baseline, Fig. 4 shows the Slow Loris attack using 60 terminals, Fig. 5 shows the Slow Loris attack using 100 terminals, and Fig. 6 shows the combination of LOIC and Slow Loris attack. As can be observed from the graphs, normal traffic has few red bars and larger intervals between time frames, but attacked networks have significantly more red bars and narrower gaps between packets. Furthermore, the attacked network shows fewer packets per second, but normal traffic shows two to three times more packets per second. According to the findings of the I/O graph, when traffic shows a considerable decline in packets per second and the time frame reveals more frequent and narrower intervals between time frames, the system may be facing DDoS attacks on the network.

Although an I/O graph can give an overall visualization of the packets over the network and thus can give a generalized idea of the patterns and flows, it is just as important to break down the detailed numbers. The averages of packets per second, average bytes per second, and average packet size were analyzed by looking at the file properties under statistics. The average packets per second for the normal traffic was 13.9 packets, whereas the attacked traffic contained an average of 5.6 packets per second. This finding revealed the attacked traffic contained on average, half of the number of packets per second compared to normal traffic. Similarly, the findings for average bytes per second displayed similar information, where the normal traffic contained 3120 bytes per second and the average attacked traffic contained 1129 bytes per second. This indicated that attacked traffic contained three times fewer bytes per second than of normal traffic. Lastly, average packet size was calculated. Findings suggested there was no significant difference in packet size from normal packets versus attacked packets. The average packet size for normal traffic contained 225 packets and the average packets for attacked traffic had 196 packets.



Enabled	Graph Name	Display Filter	Color	Style
☑	TCP Errors	tcp.analysis.flags	🟥	Bar
☑	Filtered packets	ip.addr == 172.16.1.249	🟫	Line
☑	Filtered packets	ip.addr == 172.16.1.10	🟩	Line
☑	Filtered packets	ip.addr == 172.16.1.141	🟥	Line
☑	Filtered packets	ip.addr == 172.16.1.221	🟪	Line
☑	Filtered packets	ip.addr == 172.16.1.133	🟧	Line
☑	Filtered packets	ip.addr == 172.16.1.151	⬜	Line
☑	Filtered packets	ip.addr == 172.16.1.206	🟦	Line

Figure 2: I/O Graph: Color Coded Filters

4.2 TCP Error Flags

When the TCP Error flags were compared between regular traffic and attacked network traffic, the findings revealed a significant pattern between the two types of traffic flow. According to the data, the attacked network traffic had twice

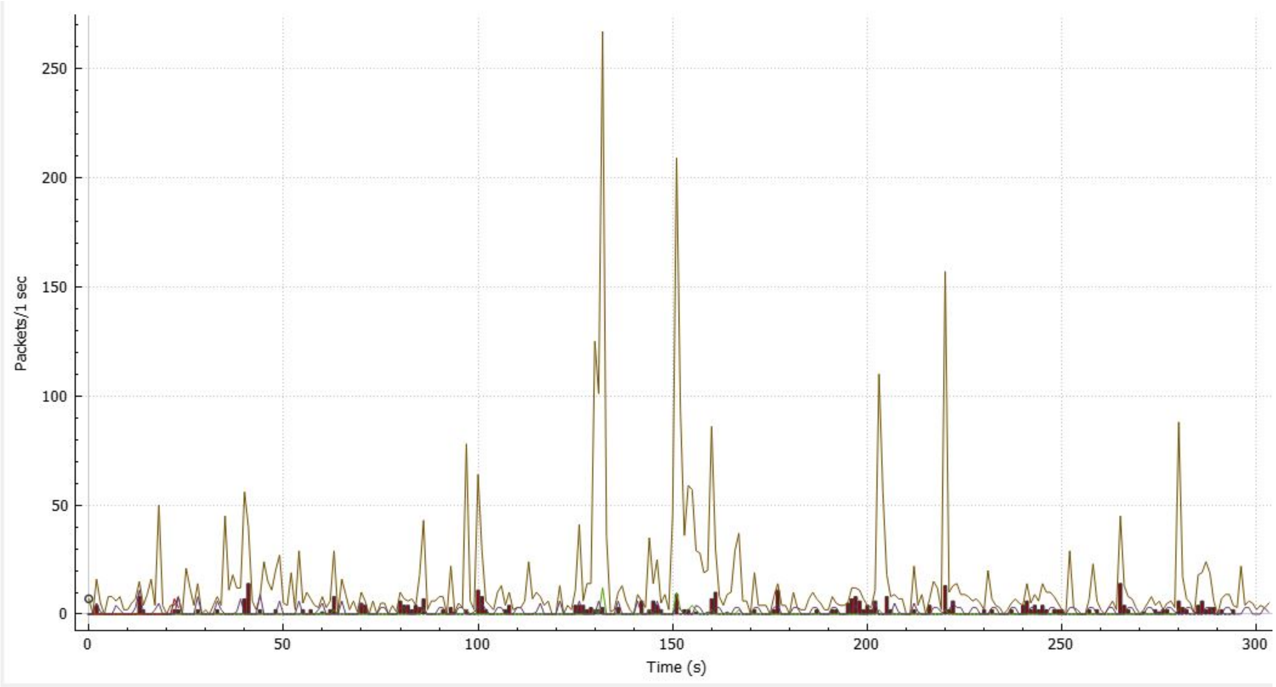


Figure 3: I/O Graph: Normal Traffic

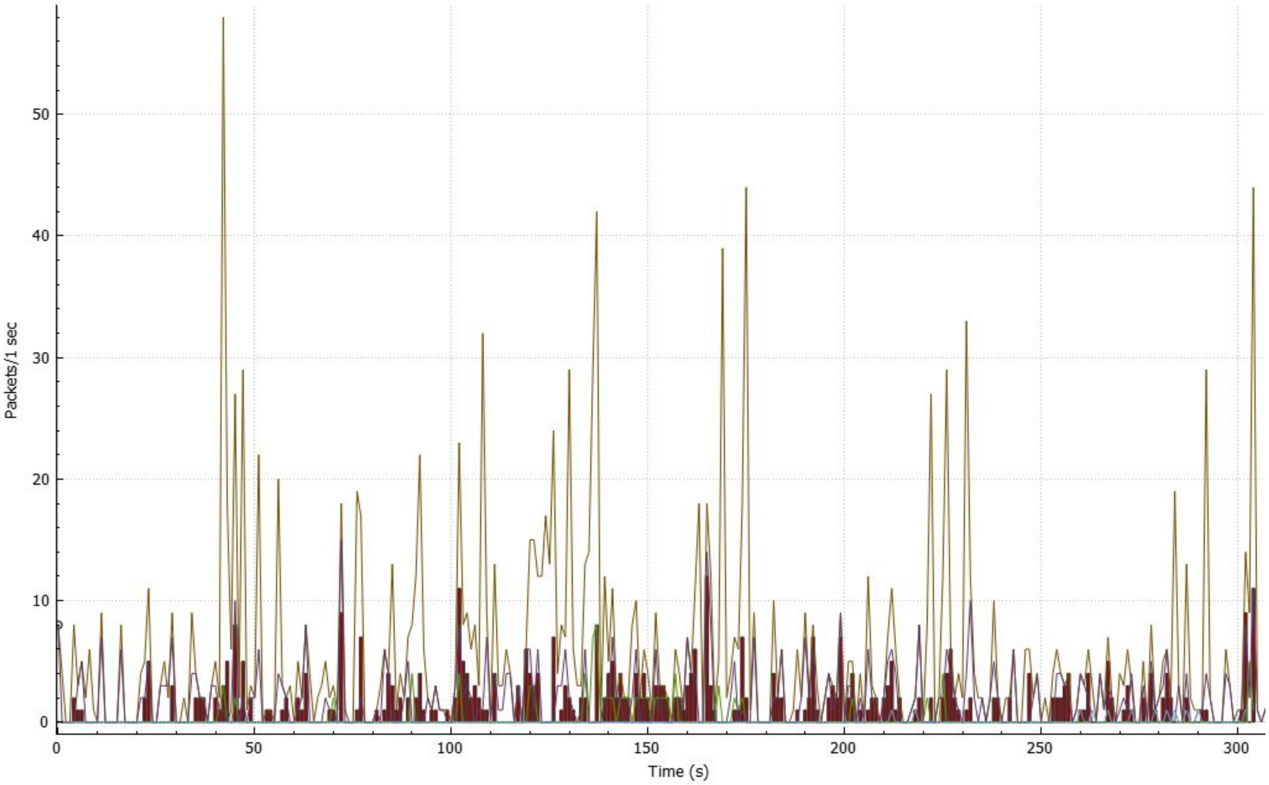


Figure 4: I/O Graph: Slow Loris 60 Terminals

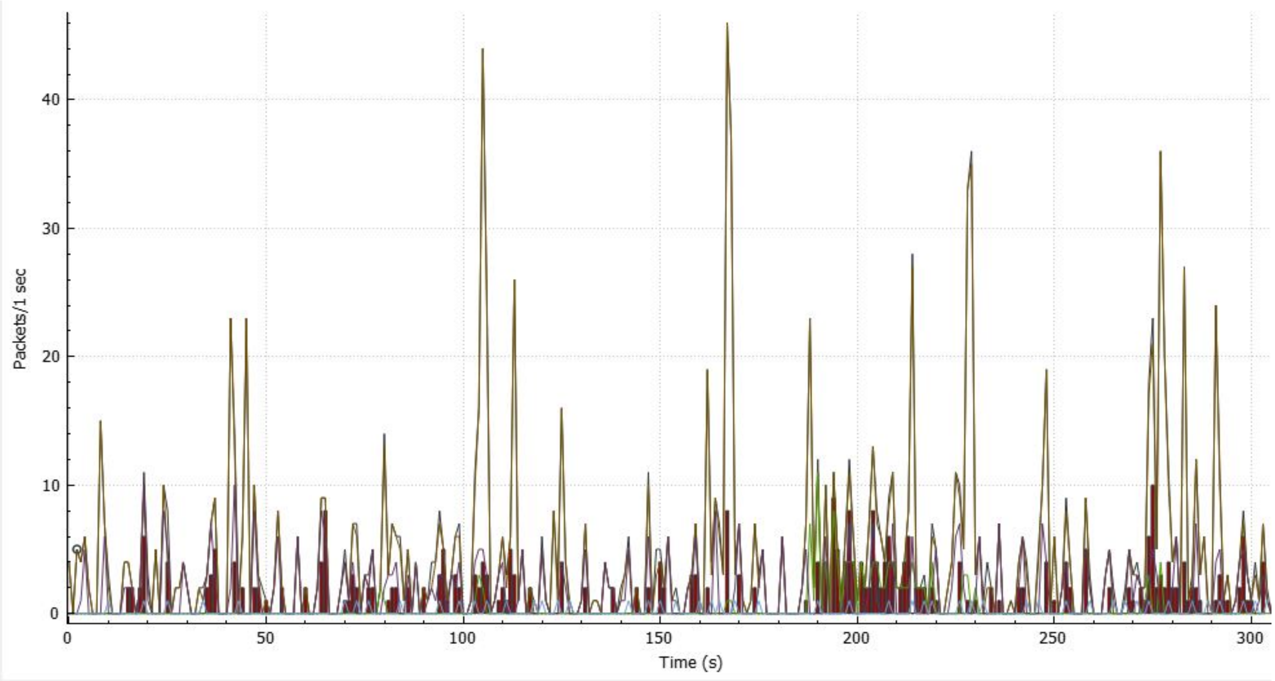


Figure 5: I/O Graph: Slow Loris 100 Terminals

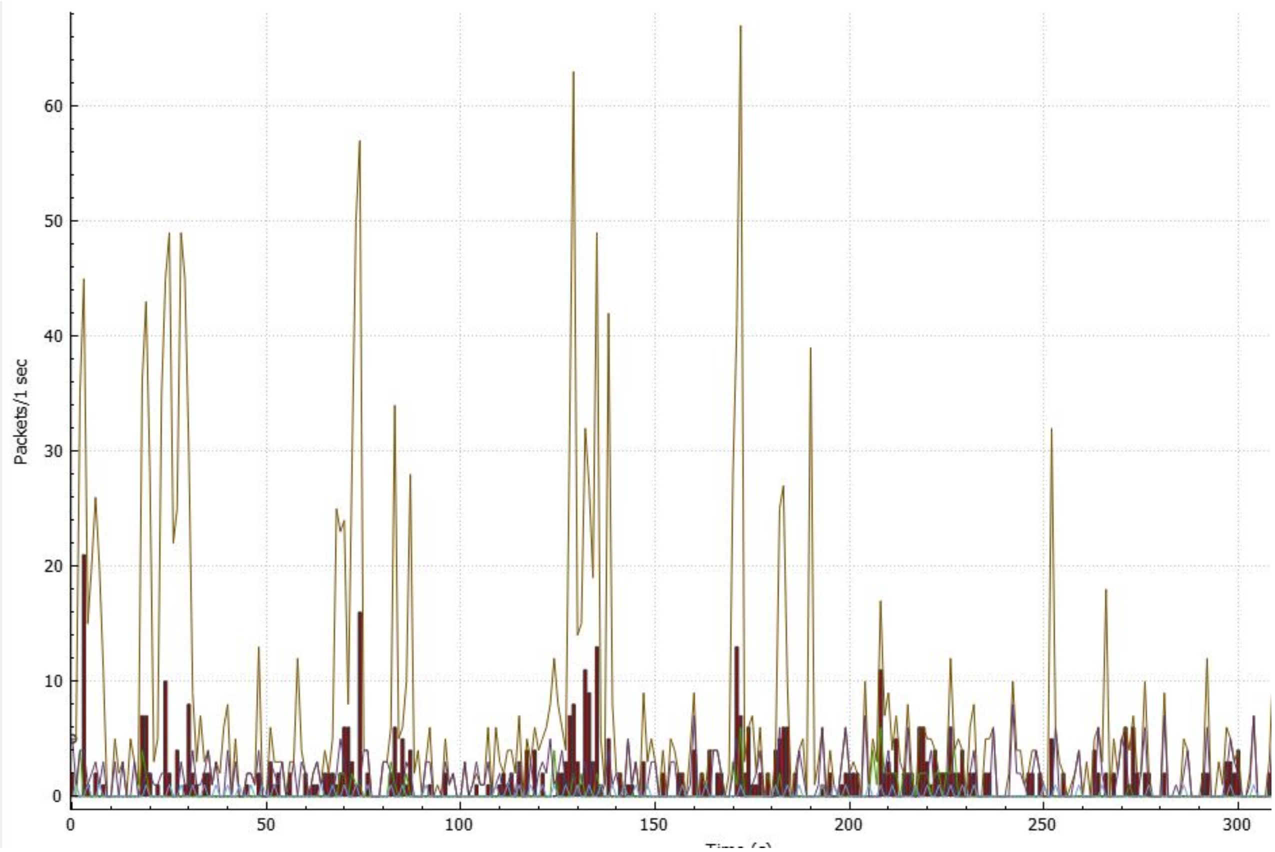


Figure 6: I/O Graph: LOIC and Slow Loris

as many TCP packet defects as regular traffic. The normal traffic showed very little amount of TCP Error flags (9.8%), whereas Slow Loris and LOIC attacks contained on average 23.1% TCP Error flags. Specifically for Slow Loris, the attack using 20 terminals contained 28.3% TCP Error flags, 40 terminals 29.5%, 60 terminals 23.9%, 80 terminals 20.9% and 100 terminals 22.7%. For LOIC, 100 bots contained 18.8% TCP Error flags, 10,000 bots contained 20.6%, and a combination of LOIC and Slow Loris contained 22.1%. The number of overall packets versus TCP Error packets for each segment of attacks can be seen in a bar graph format in Fig. 7.

4.3 Unexplained Packet loss

When dealing with traffic flow via the internet, packet loss is to be expected; nevertheless, too many packet losses might signal a network attack. The findings revealed that when a DDoS attack happens on the system, there is a considerable percent of increased packet loss compared to regular traffic when examining unexplained packet loss over the network. The outcomes of this investigation revealed that the attacked network experienced four times the amount of packet loss as a network with normal packet flow. The normal traffic contained a packet loss of 1.9% whereas the attacked network contained on average 8.1% packet loss. Specifically for Slow Loris, the attack using 20 terminals contained 9.9% packet loss, 40 terminals 10.3%, 60 terminals 8.5%, 80 terminals 8.0%, and 100 terminals 8.1%. For LOIC, the attack using 100 bots contained 6.4% TCP packet loss, 10,000 bots contained 6.7%, and a combination of LOIC and Slow Loris contained 6.9% packet loss. A visualized graph can be found in Fig. 8.

4.4 Packet Lengths

The length and the burst rate of packets were analyzed to determine any distinctive patterns between normal and attacked traffic. The findings suggested the length of the packets indicated no drastic difference. The normal packet lengths of 20-39 (bytes) contained 47.61%, whereas the average of the attacked traffic contained 46.15%. However, the burst rate was discovered to have a distinctive pattern between normal and attacked traffic. The normal packet burst rate had 0.66 seconds per packet and the attacked traffic burst rate was 0.28 seconds per packet on average. The findings suggested the burst rate of packets was two times faster with an attacked traffic than normal traffic.

5. CONCLUSIONS AND RECOMMENDATIONS

The integration of IoT smart devices in home environments has grown exponentially due to the efficiency and functionality of these devices. However, introducing Internet connected devices into your home network environment means introducing vulnerabilities and risks of being attacked. Given the possibility of being attacked, homeowners should be able to tell or predict when they are being attacked. Our study focused on DDoS attacks, specifically TCP attacks using LOIC and Slow Loris. When these attacks are being ran, certain patterns can be seen clearly through packet analysis tools such as Wireshark. To summarize, there were 5 obvious patterns that emerged when the DDoS attacks were running. First, attacked traffic contains a lesser number of packets captured per second compared to normal traffic. Second, normal traffic has a low percentage of packet loss, whereas attacked traffic has a high percentage of packet loss. These two patterns coincide with the nature of a Slow Loris attack. As Slow Loris runs, it opens connections and takes up bandwidth. Thus, there will be less network traffic as the bandwidth has been occupied or used up. Third, attacked traffic has a unusually high number of TCP error packets compared to regular traffic. This pattern aligns with a TCP DDoS attack which was conducted using LOIC. Fourth, normal traffic packets contain more bytes per second, whereas attacked traffic contains lesser bytes per second. Fifth, the burst rate of packets of attacked traffic is two times faster than the burst rate of packets of normal traffic. With the discovery of these patterns, business and homeowners can know when their network has been

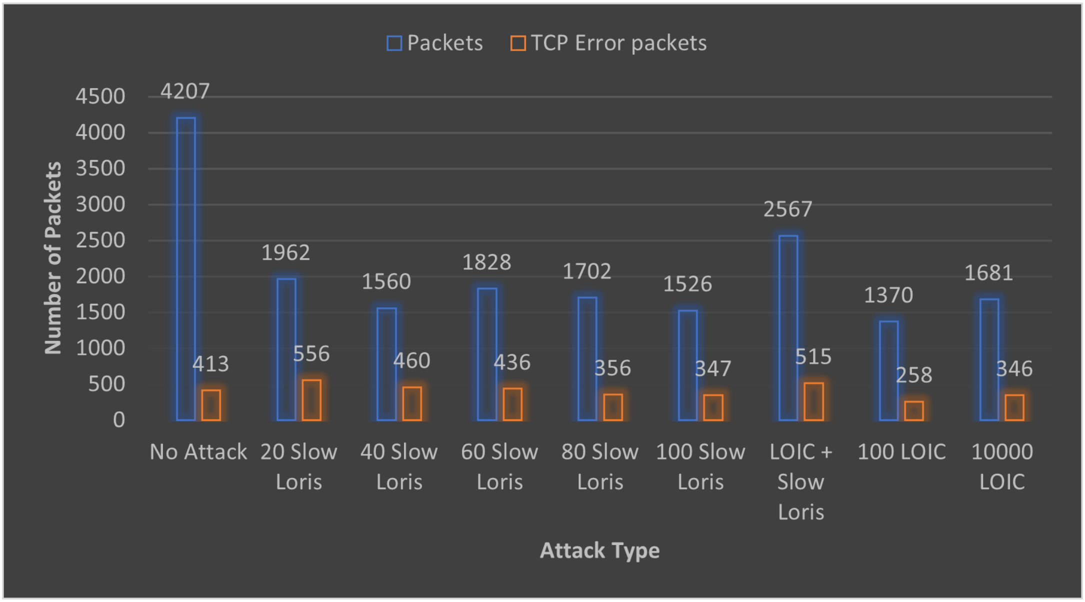


Figure 7: TCP Error Flags

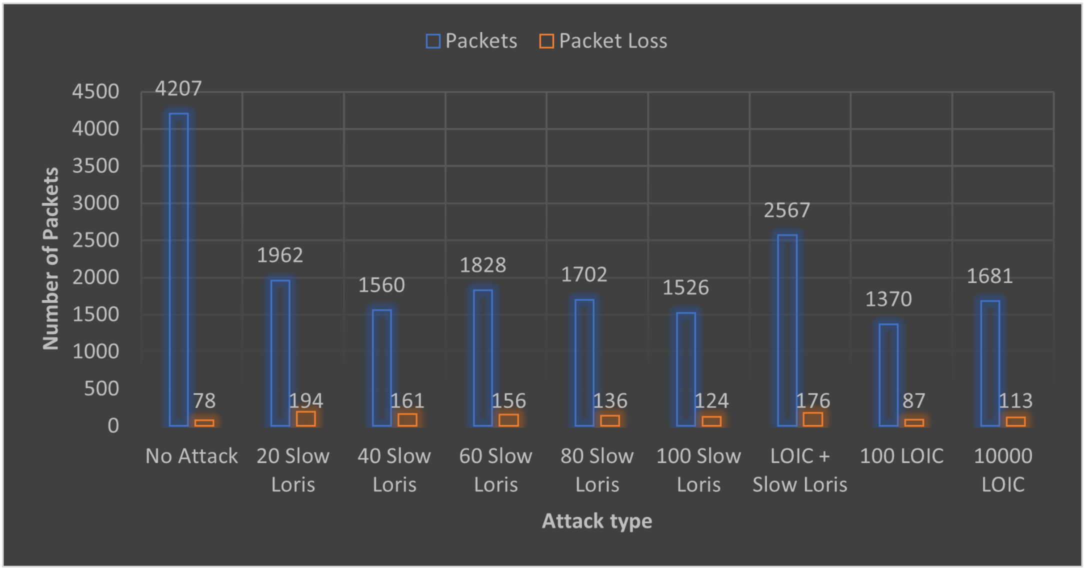


Figure 8: TCP Packet Loss

DDoS-ed.

There are a few recommendations that can be made for future research. Due to limited resources, all attacks were only run once. Ideally, multiple trials should be run to reduce the likelihood of outliers occurring. Besides that, each packet capture and attack was run for 300 seconds. Given more time and disk space, the packet captures and attacks should be run for a longer period of time to ensure more detailed data is collected. Different software and metrics could be used to conduct attacks against the IoT devices. The scope of our study was limited to certain DDoS attacks. However, future research can explore the network patterns that may emerge when their IoT devices are under attack. Lastly, more focus can be put on the unexplained packet loss in Section 4 for extending this work and conducting real-world testing. Exploring classifiers trained to detect unnatural network activity will be key to justifying the packet loss.

REFERENCES

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65–88.

Barry, M., Campbell, A. T., & Veres, A. (2001). Distributed control algorithms for service differentiation in wireless packet networks. In *Proceedings ieee infocom 2001. conference on computer communications. twentieth annual joint conference of the ieee computer and communications society (cat. no. 01ch37213)* (Vol. 1, pp. 582–590).

Bhardwaj, A., Sharma, A., Mangat, V., Kumar, K., & Vig, R. (2019). Experimental analysis of DDoS attacks on OpenStack cloud platform. In *Proceedings of 2nd international conference on communication, computing and networking* (pp. 3–13).

Cheng, C.-M., Kung, H., & Tan, K.-S. (2002). Use of spectral analysis in defense against DoS attacks. In *Global telecommunications conference, 2002. globecom'02. ieee* (Vol. 3, pp. 2143–2148).

Hutchinson, S., Yoon, Y. H., Shantaram, N., & Karabiyik, U. (2020). Internet of Things Forensics in Smart Homes: Design, Implementation, and Analysis of Smart Home Laboratory. In *2020 asee virtual annual conference content access.*

Kebande, V. R., & Ray, I. (2016). A generic digital forensic investigation framework for internet of things (iot). In *2016 ieee 4th international conference on future internet of things and cloud (ficloud)* (pp. 356–362).

Low Orbit Ion Cannon. [Software]. (2020). `https://sourceforge.net/projects/loic`. (Accessed on 03/01/2022)

Ndatinya, V., Xiao, Z., Manepalli, V. R., Meng, K., & Xiao, Y. (2015). Network forensics analysis using Wireshark. *International Journal of Security and Networks*, *10*(2), 91–106.

Rekhter, Y., Moskowitz, B., Karrenberg, D., Groot, G. d., & Lear, E. (1996). *Rfc1918: Address allocation for private internets.* `https://www.rfc-editor.org/rfc/rfc1918.html`. RFC Editor. (Accessed on 03/01/2022)

Sedaghat, S. (2020). The Forensics of DDoS Attacks in the Fifth Generation Mobile Networks Based on Software-Defined Networks. *Int. J. Netw. Secur.*, *22*(1), 41–53.

Sharpe, R., & Warnicke, E. (2011). *Wireshark user's guide.* `http://www.wireshark.org/docs/wsug\_html\_chunked/index.html`. (Accessed on 03/01/2022)

Thapngam, T., Yu, S., Zhou, W., & Makki, S. K. (2014). Distributed Denial of Service (DDoS) detection by traffic pattern analysis. *Peer-to-peer networking and applications*, *7*(4), 346–358.

U.S. Government Printing Office. (n.d.). *Statute-100-pg1213.pdf.* `https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/`

STATUTE-100-Pg1213.pdf. (Accessed on 03/01/2022)

Varghese, J. E., & Muniyal, B. (2021). A Pilot Study in Software-Defined Networking Using Wireshark for Analyzing Network Parameters to Detect DDoS Attacks. In *Information and communication technology for competitive strategies (ictcs 2020)* (pp. 475–487). Springer.

Yaltirakli, G. (2015). *Slowloris.* https://github.com/gkbrk/slowloris. (Accessed on 03/01/2022)