Advancing IoT Network Security: Examining Traffic Analysis Techniques and Attack Prevention Mechanisms

Benjamin Acuff

CYS 485- Cybersecurity Analysis II

Dr. Awad Mussa

Spring 2023

1.Introduction:

Over the past decade, the Internet of Things (IoT) has exponentially increased its popularity due to several aspects. IoT simplifies daily tasks and makes doing them more efficient. IoT has shown us great potential to make life easier in general. Nevertheless, IoT poses a great security risk. Cybercriminals often exploit IoT devices considering many of these devices have few to no security protocols. IoT devices are vulnerable to providing unauthorized access to networks and sensitive data. The ability to make IoT networks secure is an issue we face in this modern day.

In particular, traffic analysis techniques and attack prevention mechanisms are crucial for securing IoT networks. Cybercriminals use traffic analysis techniques to gather information and discover vulnerabilities in IoT devices. This can lead to many severe consequences for not only individuals but also enterprise organizations. Traditional security measures often cannot prevent such attacks, making more advanced security measures within IoT networks a larger need.

Security professionals have developed many IoT attack prevention mechanisms and traffic analysis techniques to combat the above challenges to improve IoT network security. This research paper aims to examine network traffic analysis techniques and attack prevention mechanisms for advancing IoT network security. However, as stated previously, IoT has only recently gained popularity. Beyond this, IoT was not officially named until the late 1990s and was only conceptualized in the 1980s. Therefore, research on the topic of advancing IoT network security is relatively new and has many limitations.

This research paper will examine IoT network security, its various traffic analysis techniques, and attack prevention mechanisms that have been developed to prevent cyber threats. This paper will analyze the effectiveness of these techniques, tools, and technologies that can be used in modern/future security environments. The literature used in this paper comes from online databases, specifically Northern Kentucky University's online research database through W. Frank Steely Library and Google Scholar.

This research paper will begin by defining IoT network security and exploring various threats and vulnerabilities in the IoT world. The review will then examine different traffic analysis techniques and attack prevention mechanisms that have been developed to counter cyber-attacks with a focus on tools and strategies that are implemented by these systems. Finally, the paper will discuss the effectiveness of these techniques and some challenges that are related to them. The research will analyze the implementation of these mechanisms in an enterprise organization's security plans and provide an overall summary of my findings, that point to future research opportunities.

2. Literature Review:

The body section of this paper will delve deeper into the topic of IoT network security, specifically focusing on the advancement of IoT network security by examining traffic analysis techniques and attack prevention mechanisms. This section will talk about emerging threats in the IoT networking field, problems with attacks, and other challenges faced due to the exploitation of IoT devices. In the process of completing my literature review, I created a literature review table from other research papers and articles from the aforementioned online databases. By creating the literature review table, conclusions and commonalities could be drawn. Please see Table 1 below.

NO	Author(s)/Year/Type/URL	Problem/Product	Intervention/Method/Improvement	Outcomes	Limitation/Gaps/Future Work
1	Elsevier. (2021, November 23). IOT network traffic analysis: Opportunities and challenges for forensic investigators? Forensic Science International: Digital Investigation. Retrieved March 19, 2023, from https://www.sciencedirect.com/science/article/pii/S2666281721000214	IoT devices can easily be exploited used a HTTP proxy. IoT devices often lack encryption and expose sensitive data.	32 IoT consumer devices were taken in a study. Researchers conducted a port scan to determine remote access, analyzed encryption use and exposed content. Used network traffic analysis to identify data destinations and examined mobile app-cloud communication.	Most devices didn't allow remote access, but many lacked data encryption, and data was often traversed to the US and stored on Amazon servers. Many mobile apps could be exploited via a HTTP proxy.	Limitation/Gaps: Limited to only 32 IoT consumer devices. Future work: Involve a more extensive analysis of a wider range of IoT devices to gain a more comprehensive understanding of IoT vulnerabilities.
2	Gupta, B. B., Joshi, R. C., & Misra, M. (2012). Distributed denial of service prevention techniques. arXiv preprint arXiv:1208.3557	Significance of DDoS problems and occurrence, sophistication, and strength of attacks led to ideas of numerous prevention mechanisms.	Analysis of DDoS problems, available attack tools, defense challenges and principles, and a classification of DDoS prevention mechanisms.	Better understanding of the DDoS problem and provides a security team with effective tools and methods to fight against this constantly growing threat.	Limitation/Gaps: Lack of effectiveness of these mechanisms in real-world scenarios. Future work: Testing and comparing different prevention techniques in various DDoS attack scenarios.

3	Joshi, M., & Hadi, T. H. (2015, July 27). A review of network traffic analysis and prediction techniques. arXiv.org. Retrieved March 19, 2023, from https://arxiv.org/abs/1507.05722	Nowadays, highly confidential and valuable information is communicated within the network. Proper network traffic analysis is crucial to maintain information security.	Surveyed previous studies of network traffic analysis from the last decade. Enlisted and discussed various approaches to analyze and predict network traffic analysis including data mining techniques, neural network and component analysis, and linear and nonlinear time series models.	An overview of the research work in the analysis and prediction of network traffic.	Limitation/Gaps: Only covers previous studies and does not provide any new contributions to the field of network traffic analysis and prediction techniques. Future work: Developing new and more efficient techniques for analyzing and predicting network traffic.
4	Khan, S., Gani, A., Wahab, A., Shiraz, M., & Ahmad, I. (2016, March 9). Network forensics: Review, taxonomy, and open challenges. Journal of Network and Computer Applications. Retrieved March 19, 2023, from https://www.sciencedirect.com/science/article/pii/S1084804516300121	Cybercriminals are often covering their tracks to avoid detection. How can network forensics techniques (NFT) do the following: a. Affect accessibility to network artifacts and infrastructure. b. Allow adequate evidence against intruders. c. Convey information about intruders, rather than convey false negatives.	Review NFT used to identify and investigate legal evidence against intruders in the network. Aims at the origin of attack, reliability and integrity of the evidence, visualization of attack paths, and determines worst attack paths.	By using thematic taxonomy to classify NFT based on their implementation and target data sets, experts can analyze existing techniques and identify open research challenges.	Limitation/Gaps: While the research provides thematic taxonomy to classify NFT, there are no comprehensive evaluations of their effectiveness in real-world scenarios. Future work: Testing and comparing different NFT in real-world scenarios to identify strengths and weaknesses.
5	Marchetti, M., Pierazzi, F., Colajanni, M., & Guido, A. (2016). Analysis of high volumes of network traffic for advanced persistent threat detection. Computer Networks, 109, 127-141.	Advanced Persistent Threats (APTs) are a large problem for modern enterprises. APTs are the most challenging attacks to detect and span over long periods of time.	Proposing new methods for preventing APTs. Large volumes of network traffic can be analyzed to identify weak signals that are related to suspicious APT activities and ranking the most suspicious internal hosts. The ranking helps security teams focus on a smaller subset of machines. This was tested in a network environment of around 10,000 hosts and proved to be effective.	The approach in the study provides a way to automatically detect APTs in large and complex networks using security analytics.	Limitation/Gaps: Although the method is effective, it relies heavily on manual analysis by security specialists, which can be time consuming and labor intensive. Future work: Focus on developing new tools and techniques to address emerging technologies and their impact on network forensics investigations.
6	Meghanathan, N., Allam, S. R., & Moore, L. A. (2010). Tools and techniques for network forensics. arXiv preprint arXiv:1004.0570.	As the number of people using the Internet increases, the number of illegal activities that occur increase. What tools and techniques for network forensics can help us uncover information about security attacks in the court of law.	An exhaustive survey of several tools and techniques available to conduct network forensics are provided within this study. All tools surveyed in this study are free to use. Simulations were run to find out the convergence time for attack paths with different lengths and attack routers with different probabilities of marking.	Explored in detail IP traceback mechanisms, convergence times for attack paths with different lengths, honeynet architecture and use of honeypots, both physical and virtual, in detecting malicious attack traffic and protecting	Limitation/Gaps: Does not cover cloud computing and big data, some large trends in the field. Future work: Focusing on developing tools and techniques for addressing cloud computing and big data.

				production systems.	
7	Olivier, F., Carlos, G., & Florent, N. (2015). New security architecture for IoT network. Procedia Computer Science, 52, 1028-1033.	Network security threats increase with internet evolution. Special concerns are dedicated to the security of IoT devices. Every object and device will be equipped with networking capabilities.	Investigates how software-defined networking (SDN) can improve the security of IoT devices. This strategy can operate with or without the SDN-Domain infrastructure.	Provided an overview of new SDN-based network architectures with distributed controllers. The solution can be used in the context of Ad-Hoc networks and IoT.	Limitation/Gaps: IoT security using SDN is promising, but there is a lack of evidence proving that it is effective in real-world scenarios. Future work: Testing and comparing the proposed architecture with other IoT security solutions in various deployment methods and scenarios.
8	Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to zero trust architecture: Reviews and challenges. Security and Communication Networks, 2021, 1-10.	Advancement of tech brings new and smarter ways of living. Cloud tech and IoT brings many changes to today's IT systems. As these systems grow, hackers skills increase to a rapid degree.	This paper introduces concepts of Zero trust (ZT) and Zero trust architecture (ZTA). It discusses the concept and application of ZTA as well as challenges. Some challenges include lack of standardization and vendor lock-in problems. Lastly, information on migration from perimeter-based architecture to ZTA is provided.	ZTA is unlike the traditional approach of trusting anyone in a defined perimeter. ZTA processes each request and grants access based on verification, rather than assumption.	Limitation/Gaps: N/A Future work: Exploring the scalability of ZTA. As enterprises grow, ZTA could become challenging to implement. It would be beneficial to investigate how this could be overcome.

Table 1

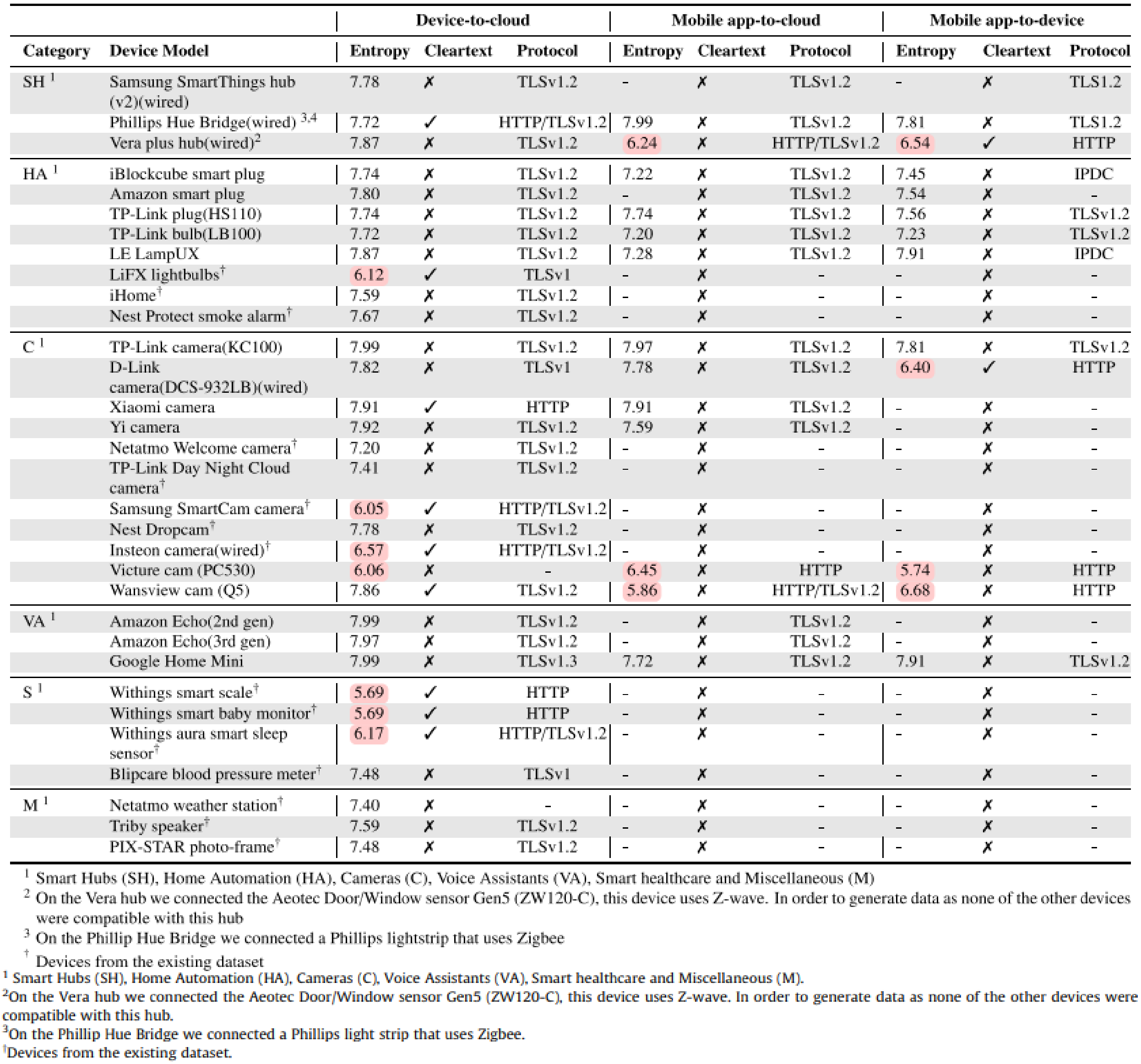
2.1 Concerns in IoT Network Security:

In a recent survey, over 50% of practitioners felt like they were not prepared to handle IoT devices and that there is a shortage of tools for IoT forensics. After noticing this in their study, Wu, Breitinger, and Niemann (2021) asked four questions:

> "RQ1: Does a device expose ports that allow an investigator to connect/access a device? RQ2: Do IoT devices utilize encryption when sending/receiving information from the cloud and corresponding App? RQ3: To which countries do the IoT devices and Apps communicate/establish connections (which is an indicator where data resides)? RQ4: Do IoT device applications (Apps) utilize encryption when sending/receiving information?"

To answer those questions, they examined the network traffic of 32 consumer IoT devices. 17 IoT devices were purchased and the remaining 15 were part of an existing dataset. (p. 1-2)

A major concern with this study was simply the fact that many of the devices that were used in the experiments did not use encryption. See table 2 below.



		Device-to-cloud			Mobile app-to-cloud			Mobile app-to-device		
Category	Device Model	Entropy	Cleartext	Protocol	Entropy	Cleartext	Protocol	Entropy	Cleartext	Protocol
SH [1]	Samsung SmartThings hub (v2)(wired)	7.78	✗	TLSv1.2	-	✗	TLSv1.2	-	✗	TLS1.2
	Phillips Hue Bridge(wired) [3,4]	7.72	✓	HTTP/TLSv1.2	7.99	✗	TLSv1.2	7.81	✗	TLS1.2
	Vera plus hub(wired)[2]	7.87	✗	TLSv1.2	6.24	✗	HTTP/TLSv1.2	6.54	✓	HTTP
HA [1]	iBlockcube smart plug	7.74	✗	TLSv1.2	7.22	✗	TLSv1.2	7.45	✗	IPDC
	Amazon smart plug	7.80	✗	TLSv1.2	-	✗	TLSv1.2	7.54	✗	-
	TP-Link plug(HS110)	7.74	✗	TLSv1.2	7.74	✗	TLSv1.2	7.56	✗	TLSv1.2
	TP-Link bulb(LB100)	7.72	✗	TLSv1.2	7.20	✗	TLSv1.2	7.23	✗	TLSv1.2
	LE LampUX	7.87	✗	TLSv1.2	7.28	✗	TLSv1.2	7.91	✗	IPDC
	LiFX lightbulbs†	6.12	✓	TLSv1	-	✗	-	-	✗	-
	iHome†	7.59	✗	TLSv1.2	-	✗	-	-	✗	-
	Nest Protect smoke alarm†	7.67	✗	TLSv1.2	-	✗	-	-	✗	-
C [1]	TP-Link camera(KC100)	7.99	✗	TLSv1.2	7.97	✗	TLSv1.2	7.81	✗	TLSv1.2
	D-Link camera(DCS-932LB)(wired)	7.82	✗	TLSv1	7.78	✗	TLSv1.2	6.40	✓	HTTP
	Xiaomi camera	7.91	✓	HTTP	7.91	✗	TLSv1.2	-	✗	-
	Yi camera	7.92	✗	TLSv1.2	7.59	✗	TLSv1.2	-	✗	-
	Netatmo Welcome camera†	7.20	✗	TLSv1.2	-	✗	-	-	✗	-
	TP-Link Day Night Cloud camera†	7.41	✗	TLSv1.2	-	✗	-	-	✗	-
	Samsung SmartCam camera†	6.05	✓	HTTP/TLSv1.2	-	✗	-	-	✗	-
	Nest Dropcam†	7.78	✗	TLSv1.2	-	✗	-	-	✗	-
	Insteon camera(wired)†	6.57	✓	HTTP/TLSv1.2	-	✗	-	-	✗	-
	Victure cam (PC530)	6.06	✗	-	6.45	✗	HTTP	5.74	✗	HTTP
	Wansview cam (Q5)	7.86	✓	TLSv1.2	5.86	✗	HTTP/TLSv1.2	6.68	✗	HTTP
VA [1]	Amazon Echo(2nd gen)	7.99	✗	TLSv1.2	-	✗	TLSv1.2	-	✗	-
	Amazon Echo(3rd gen)	7.97	✗	TLSv1.2	-	✗	TLSv1.2	-	✗	-
	Google Home Mini	7.99	✗	TLSv1.3	7.72	✗	TLSv1.2	7.91	✗	TLSv1.2
S [1]	Withings smart scale†	5.69	✓	HTTP	-	✗	-	-	✗	-
	Withings smart baby monitor†	5.69	✓	HTTP	-	✗	-	-	✗	-
	Withings aura smart sleep sensor†	6.17	✓	HTTP/TLSv1.2	-	✗	-	-	✗	-
	Blipcare blood pressure meter†	7.48	✗	TLSv1	-	✗	-	-	✗	-
M [1]	Netatmo weather station†	7.40	✗	-	-	✗	-	-	✗	-
	Triby speaker†	7.59	✗	TLSv1.2	-	✗	-	-	✗	-
	PIX-STAR photo-frame†	7.48	✗	TLSv1.2	-	✗	-	-	✗	-

[1] Smart Hubs (SH), Home Automation (HA), Cameras (C), Voice Assistants (VA), Smart healthcare and Miscellaneous (M)

[2] On the Vera hub we connected the Aeotec Door/Window sensor Gen5 (ZW120-C), this device uses Z-wave. In order to generate data as none of the other devices were compatible with this hub

[3] On the Phillip Hue Bridge we connected a Phillips lightstrip that uses Zigbee

† Devices from the existing dataset

[1] Smart Hubs (SH), Home Automation (HA), Cameras (C), Voice Assistants (VA), Smart healthcare and Miscellaneous (M).

[2]On the Vera hub we connected the Aeotec Door/Window sensor Gen5 (ZW120-C), this device uses Z-wave. In order to generate data as none of the other devices were compatible with this hub.

[3]On the Phillip Hue Bridge we connected a Phillips light strip that uses Zigbee.

†Devices from the existing dataset.

Table 2 - Out of the 32 IoT devices, the highlighted entropy values are the devices that did not use encryption (Wu et al., 2021, p. 4)

They found that several devices do not use encryption and traffic is easy to intercept. The devices that were sending cleartext were smart cameras and healthcare devices. Smart healthcare devices expose personal data that can identify features of a person of interest. Another example includes a smart camera, specifically the Xiaomi camera, detecting motion and sending unencrypted packets of not just the video but also the credentials to an Amazon Web Services server.

In conclusion, from this study, we can understand that as the total number of IoT devices is increasing daily, forensics investigators will have too many devices to analyze. Using an entropy test, we have a useful tool for discovering devices that send unencrypted traffic. This is clearly a large problem considering many United States citizens have countless amounts of IoT devices surrounding them at home. This study can help us understand the importance of advancing IoT security.

2.2 Importance of Network Traffic Analysis:

According to Joshi and Hadi (2015), "Network traffic analysis is a significant stage for developing successful and preventive congestion control schemes and to find out normal and malicious packets." (p. 1) In relation to IoT devices, network traffic analysis is especially important as we know these devices are becoming increasingly popular throughout the years and can be found in many environments, businesses, and public spaces.

Network traffic analysis has many challenges. The network can be analyzed at different levels of viz, at packet level, flow level, and network level for security management. The generic structure of a network traffic analysis starts with a data set. There have been hundreds of standardized data sets used in the past years. These data sets are used by researchers for network traffic analysis. (p. 2-3)

After a data set, we move on to preprocessing techniques. Joshi and Hadi claim that preprocessing is a very important phase. Preprocessing is used to change real-world data into a humanly understandable format. We use these methods to improve the quality of data before the data mining stage. Again, there are many methods for preprocessing just as there are data sets. (p. 4)

In our third stage, we start the analysis. This is also known as the data mining stage. Data mining is used for "knowledge-discovery." Within data mining, Joshi and Hadi have categorized these techniques under four categories – clustering, classification, hybrid, and association. The clustering technique involves putting data into groups based on certain characteristics of the data. The classification technique attempts to put traffic into one of two groups: normal or malicious. The hybrid models are simply a combination of two or more network traffic analysis methods. Out of each system, the hybrid model achieved the best results. Finally, the association rules are mainly used to identify patterns among attributes of data. These are also very important when it comes to the analysis of network traffic. (p. 5-9)

Our last stage is known as evaluation metrics. Some of the metrics used are True Negatives (TN), True Positives (TP), False Negatives (FN), False Positives (FP), Detection rate (DR), Precision rate (PR), and many more. These metrics are used using a confusion matrix. (p. 10) Once we finish our evaluation metrics, network traffic analysis has been completed.

In conclusion, during the past fifteen years, analysis and prediction of network traffic have increased the attention of researchers in various fields of computer networks. Countless researchers have created algorithms for analyzing and predicting network traffic. Network traffic analysis is crucial for advancing network security and highly relates to the IoT field.

2.3 Distributed Denial of Services (DDoS) Threats and Prevention Mechanisms:

As we mentioned earlier, as the popularity of IoT devices increases, so does the amount and severity of security threats. In the next two sections, we will talk about Distributed Denial of Service (DDoS) and Advanced Persistent Threats (ATPs). Beyond this, we will also talk about the analysis of these attacks, modern prevention methods, and their relation to the Internet of Things.

Gupta et al. gave a brief overview of what a DDoS is in their paper, *Distributed Denial of Service Prevention Techniques*. (2012) “A Distributed Denial of Service attack is commonly characterized as an event in which a legitimate user or organization is deprived of certain services, like web, email or network connectivity, that they would normally expect to have.” (p. 269) Distributed Denial of Service attacks were identified in the late 1990s, right as IoT devices made a major breakthrough. DDoS is known as a resource overloading problem. Attackers often send a large number of packets to a computer network.

Attacks that target system memory resources, aim to crash network handling software rather than consume bandwidth with large volumes of traffic. Certain packets are sent to confuse an operating system or other resources on a victim’s device. Another type of system resource attack has a structure that can trigger a bug within the network software. In turn, this causes the target system to overload, disabling any communication mechanisms it has. It can also make a host crash, freeze, or reboot. One way or the other, the system cannot communicate over the network until the system has completely loaded back up.

We can understand that IoT devices are particularly vulnerable to network attacks such as DDoS because they often have very limited memory and processing power. With this being said, IoT devices become extremely easy targets for attackers, as they are not designed with security in mind anyway. In some enterprise organizations, IoT devices can be used to monitor critical infrastructures, such as smart homes, the healthcare industry, industrial automation, banking, and many more. If IoT devices are disrupted by a DDoS attack, it can cause an enterprise to have serious consequences.

Thankfully, Gupta et al. have analyzed these DDoS issues and have been able to provide security teams with effective methods to fight against this constantly growing threat. Some general techniques and filtering techniques are provided in *Distributed Denial of Service Prevention Techniques.* (2012) General techniques are common preventive measures such as system protection and replication of resources.

The first general technique that is provided is disabling unused services. There is an idea that the fewer applications and open ports on the host side, the less of a chance there is for attackers to exploit a system. The next technique involves installing the latest security patches. This method is straightforward and removes all known security holes that could be exploited by an attacker. Our third technique provided is disabling IP broadcasting. The only way to prevent intermediate broadcasting attacks such as Smurf attacks and ICMP flood attacks is to disable the IP broadcast. Our fourth technique is simply implementing and using a firewall. Firewalls can prevent users from launching simple flooding attacks from machines behind the wall. Firewalls are configurable, meaning they have rulesets that can be changed to allow or deny protocols ports or IP addresses. Next, we have the global defense infrastructure technique. This technique prevents DDoS attacks by installing filtering rules in routers of the internet. Although, this technique is only possible in theory. Our last technique is IP hopping. DDoS attacks can be prevented by changing the IP address of the active server. (Gupta et al., 2012, p. 272)

Moving on to our filtering techniques, we start with ingress filtering and egress filtering.

Ingress filtering is a “restrictive mechanism” that drops traffic with specific IP addresses that do not match a domain prefix connected to the ingress router. Egress filtering is simply an outbound filter. This outbound filter makes sure that only assigned or allocated IP address space can leave the network. To best utilize ingress and egress filtering, knowledge of expected IP addresses at a particular port is needed. For large enterprises with highly complex topologies, it is difficult to obtain this knowledge.

Our second filtering technique is router-based packet filtering. This method is an extension of ingress filtering and uses routing information to filter out spoofed IP packets. Gupta, Joshi, and Misra said, “It is based on the principle that for each link in the core of the Internet, there is only a limited set of source addresses from which traffic on the link could have originated.” (p. 272) Router-based packet filtering checks source addresses in IP packets and can assume which packets are spoofed. Then the packet can be filtered.

Our third filtering technique is history-based IP filtering. During DDoS attacks, generally, most of the source IP addresses have never been seen before. Essentially, this technique involves using an IP address database (IAD) to keep frequent sources of IP addresses. While an attack is ongoing, and the source address is not in the IAD, the packet is completely dropped. History-based IP packet filtering is not effective when an attack comes from real IP addresses. It also requires an offline database to keep track of IP addresses. Cost, storage, and information sharing are very high. Therefore, this method is not recommended.

The last filtering technique is the capability-based method. This provides a way to control traffic directed towards itself. During this approach, the source first sends request packets to the destination. The router marks are added to a request packet while going through the router. Now, the destination can choose whether it would like to grant permission to send it or not. If permission is granted, then the destination returns the capabilities. If it doesn’t, then it does not supply capabilities in the returned packet. The main takeaway from this architecture is that the destination can control traffic according to its own policy. In turn, DDoS attack probabilities are decreased. (Gupta et al., 2012, p. 273)

2.4 Advanced Persistent Threats (APTs) and APT Prevention Mechanisms:

According to Marchetti et al., “Advanced Persistent Threats (APTs) represent the most critical menace to modern organizations.” (p. 127) APTs are not like other attacks. ATPs are "human-driven infiltrations" that span over long lengths of time. They are made and customized towards a targeted enterprise after background intelligence analysis has been performed. An enterprise organization that has been attacked by an APT can cause millions of dollars in damage, and its reputation could even be lost.

In *Analysis of high volumes of network traffic for Advanced Persistent Threat detection*, Marchetti et al. proposes new methods for preventing APTs. The contributions of this research study can be summarized below:

- "Characterize network statistics of real and large network environments, and define a model aimed to detect APT-related activities with specific attention to data exfiltrations;" (p. 128)
- "We propose a set of algorithms that are able to score suspiciousness of APT activities by evaluating movements and positions of the internal hosts in a multidimensional feature space over time;" (p. 128)
- "We design and implement a prototype that is applied to a real networked system consisting of about 10K hosts and that demonstrates the feasibility and effectiveness of the proposed approach" (p. 128)

As we will not get into the dire specifics of this research study, we can understand that the first framework that can identify and rank suspicious hosts that are possibly involved in data exfiltrations related to ATPs. By using this approach, network traffic data is gathered and analyzed. A set of features that is inclined to detect possible data exfiltrations. These are given suspiciousness scores for each internal host. Finally, a ranked list of suspicious hosts possibly involved APT-related activities is created. (p. 139)

This framework that was proposed can reinforce IoT network security by providing a quick, automated, and highly efficient way to detect possible APTs. This information can be used by security professionals from around the world within enterprise organizations to investigate and respond to potential APTs. By doing this, enterprises can reduce the risk of cyberattacks, specifically APTs. Choosing to combine this framework with other network security frameworks can further enhance and advance our study on the security of IoT networks.

2.5 Software-Defined Networking:

As we move into the future generation of IoT devices and the internet, we must understand that traditional security measures such as the implementation of firewalls, intrusion detection systems, and many more will only temporarily be enough to secure the next generation of the internet. The so-called, “borderless architecture” of the Internet of Things causes concern over NAC (network access control) and software verification. (Olivier et al., 2015, p. 1028) In *New Security Architecture for IoT Network*, Olivier et al. provide an overview of a new SDN-based (software-defined networking) network architecture with distributed controllers. Overall, increasing the security and stability of IoT networks.

Software-Defined Networking (SDN) came out as a way to increase the functionality of a network, decrease the cost, decrease hardware complexity and enable original research. SDN architecture models consist of three layers. An infrastructure layer, a control layer, and an application layer. SDN architecture holds the ability to extend the security perimeter to the network access endpoint devices by setting up security policy rules for devices on a network. (Olivier et al., 2015, p. 1029)

Let’s get into the SDN-based architecture for the Internet of Things. IoT was created to promote scalability, high levels of traffic, and mobility. Traditional network protocols and equipment are not designed for these things. This leads researchers to propose new network architecture models for IoT.

For IoT or sensor networks, it is important to understand that each device cannot have embedded SDN-compatible switches and SDN controllers. However, it is assumed that each device with low resources can be associated with one neighbor node that does have SDN capability. In Figure 1 below, we have two types of nodes within a domain. If a node has sufficient resources, we call it an OF node. If it has insufficient resources, we call it a sensor or smart object. Each domain has an SDN controller which controls all traffic within the domain. The edge controller of the SDN domain has all rules synchronized. (Olivier et al., 2015, p. 1031)

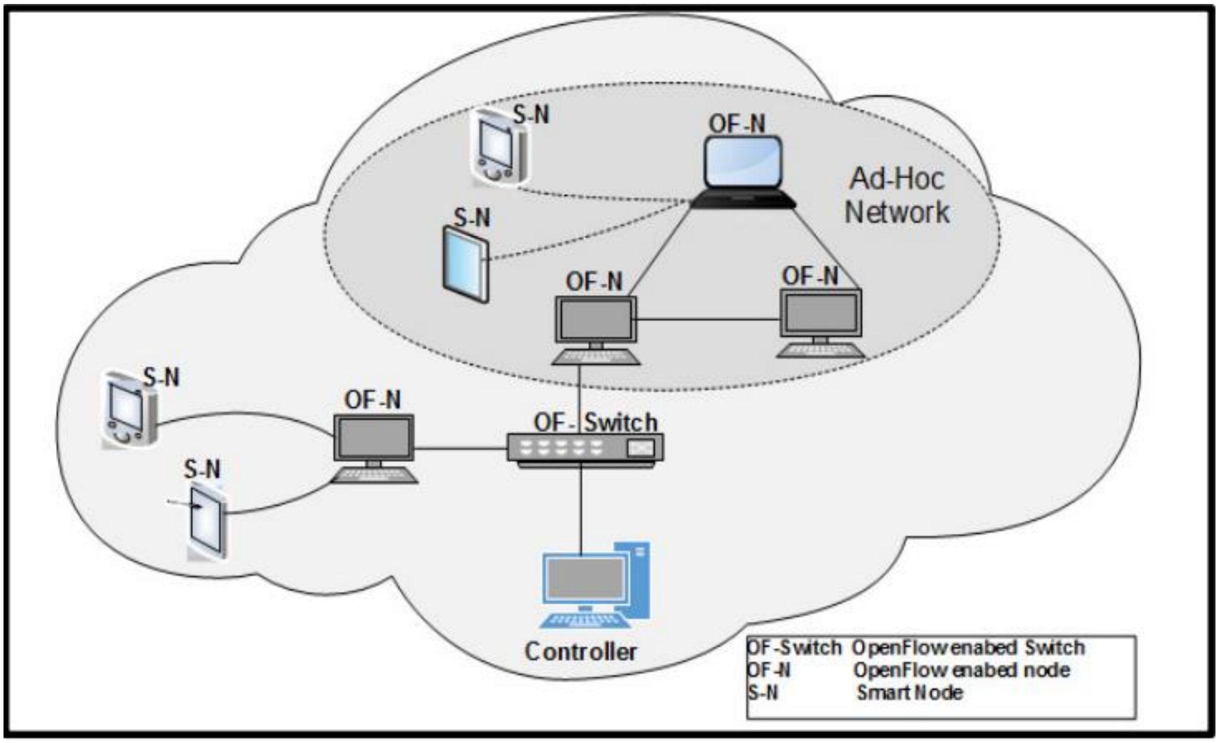


Figure 1. Domain-SDN; (Olivier et al., 2015, p. 1030)

In another proposed architecture. We have multiple SDN domains. In each domain, it is assumed in each single domain, there is one SDN controller or multiple SDN controllers. These controls act to manage only the devices within its domain. A domain for example can represent an enterprise organization network or a data center. Please see Figure 2 below.

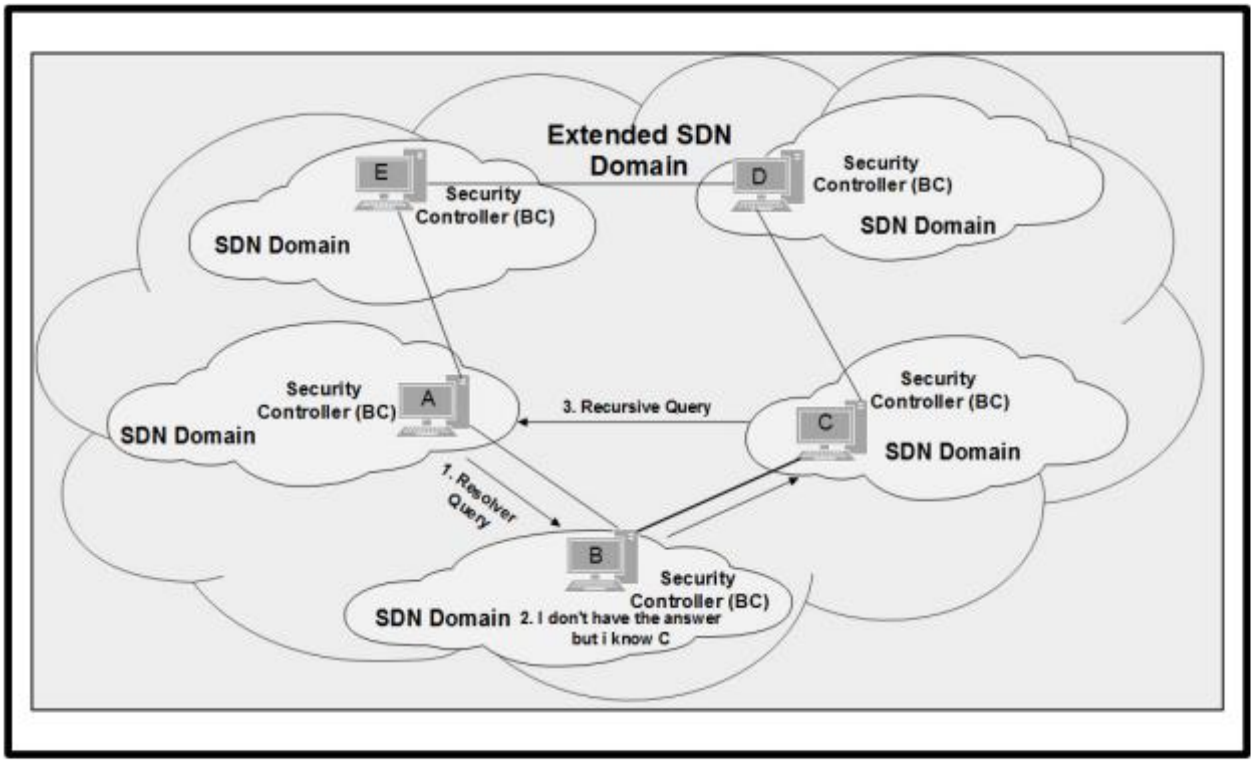


Figure 2. SDN Domain interconnection – Extended SDN Domain; (Olivier et al., 2015, p. 1030)

By using NAC and security techniques Olivier et al. designed an extended secure SDN-based architecture for IoT. In this architecture, a controller manages the security of one SDN domain. Now, we can extend this solution to include multiple controllers with regard to available resources on each control platform. After this, we are able to extend the distributed control architecture by interconnecting all SDN domains via border controllers, which leads us to have a secure model for the IoT. (p. 1032)

From this research, we can understand how SDN-based network architectures can work with IoT networks. In the future, more security mechanisms and possibilities should be explored in the context of SDN. Olivier et al. plan to test their system at an even larger scale in order to optimize its design. They also hold an objective to build and test this architecture in real-world environments.

3. Conclusion:

In conclusion, this research paper goes into the subject of advancing IoT network security through the examination of network traffic analysis techniques and attack prevention mechanisms. IoT and its popularity have significantly grown over the past decade. We understand that it also brings many security risks as cybercriminals exploit IoT devices due to the lack of security protocols. We know that traditional security measures often do not suffice when it comes to securing IoT networks. Therefore, we have explored some of the advanced security measures needed to bring security factors to these networks.

To reduce cyber threats, security professionals have developed many traffic analysis techniques and attack prevention mechanisms. This paper has analyzed the effectiveness of these techniques, tools, and technologies, used in modern and future network security environments. By studying and researching the behavior of IoT devices, we notice that there are virtually zero security measures, meaning network security for IoT devices is crucial.

This paper starts by defining concerns in IoT network security. We then delve into different network traffic analysis techniques and attack prevention mechanisms that have been created to stop cyber-attacks with a focus on some tools and strategies implemented by modern-day systems and security experts. Throughout the paper, we discuss the effectiveness of these techniques and methods along with some challenges that are also presented with them for the future. Towards the end of the paper, we talk about future architecture utilizing software-defined networking that can decrease threats within IoT networks and their domains.

Again, it is worth taking note and understanding that research on the topic of advancing IoT network security is relatively new, and there are many limitations. Nevertheless, this research paper has the goal of providing a comprehensive overview of some of the techniques, tools, and models used for network traffic analysis and IoT network security. The findings of this research paper help us understand why traffic analysis techniques and attack prevention mechanisms are crucial for securing IoT networks. By implementing these mechanisms in modern/future network environments, an enterprise organization can improve its network security, specifically IoT network security. This paper provides an overall summary of my literature findings, literature review, and suggests future research opportunities.

References

Elsevier. (2021, November 23). *IOT network traffic analysis: Opportunities and challenges for forensic investigators?* Forensic Science International: Digital Investigation. Retrieved March 19, 2023, from https://www.sciencedirect.com/science/article/pii/S2666281721000214

Gupta, B. B., Joshi, R. C., & Misra, M. (2012). Distributed denial of service prevention techniques. arXiv preprint arXiv:1208.3557

Joshi, M., & Hadi, T. H. (2015, July 27). *A review of network traffic analysis and prediction techniques*. arXiv.org. Retrieved March 19, 2023, from https://arxiv.org/abs/1507.05722

Khan, S., Gani, A., Wahab, A., Shiraz, M., & Ahmad, I. (2016, March 9). *Network forensics: Review, taxonomy, and open challenges*. Journal of Network and Computer Applications. Retrieved March 19, 2023, from https://www.sciencedirect.com/science/article/pii/S1084804516300121

Marchetti, M., Pierazzi, F., Colajanni, M., & Guido, A. (2016). Analysis of high volumes of network traffic for advanced persistent threat detection. Computer Networks, 109, 127-141.

Meghanathan, N., Allam, S. R., & Moore, L. A. (2010). Tools and techniques for network forensics. arXiv preprint arXiv:1004.0570.

Olivier, F., Carlos, G., & Florent, N. (2015). New security architecture for IoT network. Procedia Computer Science, 52, 1028-1033.

Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to zero trust architecture: Reviews and challenges. Security and Communication Networks, 2021, 1-10.