DDoS attack Detection Model based on Entropy Computing

Mark Njore

138014

CNS

Supervisor Name

Dr. Victor Rop

Submitted in Partial Fulfillment of the Requirements of the Bachelor of Science in Computer Networks and Cybersecurity at the Strathmore University

School of Computing and Engineering Science

Strathmore University

Nairobi, Kenya

May 2023

Declaration and Approval

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the research proposal contains no material previously published or written by another person except where due reference is made in the research proposal itself.

Student Name: Mwaura Mark Njore

Admission Number: 138014

Student Signature: _____ Date:_____

The Proposal of **Mwaura Mark Njore** has been reviewed and approved by **Dr. Victor Rop**

Supervisor Signature: _____ Date:_____

Acknowledgement

Even for a moment, I don't fool myself into believing that this work would have been possible without the help of others. That being said I hope I will be able to thank everyone who has helped me in the next few lines. First, I would like to thank my supervisor, Dr. Rop, for all support provided to me during this period. I have him to thank for guiding me through the process and helping with the few corrections made in my research. I would also like to thank our lecturer Mr. Tiberias for providing tips on how to work on the project and how to manage the project timewise. I would also like to express my gratitude towards my colleagues at the university whose inputs were also crucial for my research. Finally, I would like to thank my family for their support during this period.

Abstract

The increase in distributed denial of service (DDoS) attacks poses a significant threat to network infrastructures and necessitates the development of robust detection mechanisms. The purpose of this research proposal is to introduce a DDoS detection model that uses the concept of entropy for effective anomaly detection. Entropy, as a measure of randomness and uncertainty, can capture irregular patterns and anomalies in network traffic, enabling early detection of DDoS attacks. This model involves collecting network traffic data and extracting entropy-based characteristics to capture the underlying characteristics of the traffic, resulting in accurate and efficient detection of DDoS attacks.

The expected outcome of this research is a model capable of DDoS attack detection that improves network security by proactively identifying DDoS attacks. The proposed model aims to improve detection accuracy and thereby minimize the impact of DDoS attacks on network availability and performance by leveraging entropy-based features. The research findings help advance the network security field and provide valuable insight into the effectiveness of entropy-based approaches to DDoS detection. Ultimately, the proposed model could be deployed in real network environments to strengthen security measures and defend against the growing threat landscape of DDoS attacks. This can improve network availability, reduce downtime, and improve overall network security in the face of evolving DDoS threats.

Table of Contents

List of Figures

List of Equations

List of Abbreviations

CPU – Central Processing Unit

DDoS – Distributed Denial of Service

DNS - Domain Name System

DoS – Denial of Service

HTTP - Hypertext Transfer Protocol

ICMP - Internet Control Message Protocol

ML – Machine Learning

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

VM – Virtual Machine

Chapter 1: Introduction

1.1 Background

In today's world, the internet is increasingly becoming an essential aspect of our day-to-day lives. As of April 2023, there were 5.8 billion active Internet users worldwide (Petrosyan, 2023). This accounted for 62% of the world's total population. The number of users is still increasing as there are approximately 27,000 new Internet users every hour (Flynn, 2023). This growth represents not only technological progress but also an increase in opportunities for cybercriminals to take advantage of. This creates the challenge of enforcing security over the internet due to the cyber-attacks that exploit these opportunities.

Cyber-attacks are becoming more complex by the day, with new methods being discovered so frequently that it is becoming a problem to keep up with them. Among these cyber-attacks is a type called a DDoS attack. A Denial-of-Service (DoS) attack by definition is an explicit attempt by attackers to overwhelm a computer target's ability to handle incoming communications, prohibiting legitimate users from accessing the service (Douligeris & Mitrokotsa, 2004; Whitman & Mattord, 2017). A Distributed Denial-of-Service (DDoS) attack is a variation of this whereby the attacker coordinates an attack by using multiple devices at the same time, instead of one machine like in a normal DoS attack. This can be done using bots in a botnet or using zombies (Hoque et al., 2015). The attacker can attempt to flood a network, preventing legitimate network traffic, disrupting connections between two machines, preventing access to a service, or even attempting to prevent a particular individual from accessing a service (Weiler, 2002). These would all be considered DoS attacks as the accessibility of the system or information is affected.

DDoS attacks have been prevalent since as early as the 1990s. In September 1996, an attack on an ISP known as Panix became the first documented case of a DoS attack. The attack was directed at the devices on the networks including mail, news, name, and web servers (Patrikakis et al., 2019). DDoS attacks are becoming more and more frequent. The world has been seeing an increase in DDoS attacks year over year, with there being a 150 percent increase between Q2 of 2021 and Q2 of 2022 and it's only expected to get worse (Turner, 2022). Another

example occurred in February 2020, when Amazon Web Services (AWS), a well-known cloud computing service platform saw as many as 2.3 Terabits per second coming into its servers as a result of the DDoS attack (Nicholson, 2020). This attack surpassed the previous record held by the 2018 GitHub attack at 1.35 Tbps and is considered one of the worst attacks seen to date (Kottler, 2018).

DDoS attacks can last for multiple days or even weeks depending on the goal of the attack. An attack can last for several hours, days, or even weeks. In 2015, a DDoS attack on GitHub lasted for a total of 118 hours before it ended (Gheorge, 2015). The effects and consequences to the target host or the target network could then be seen even after the attack ends. One effect is that the system under attack would be unable to access the system or part of the system as a result of the attack. The system would also suffer from a lack of available bandwidth. The DDoS traffic would take up most, if not all of the bandwidth which would then lead to wastage. The resources on the network would also suffer from strain during the attack. Resources such as CPU memory would be used up in processing the traffic from the attack and would not be able to serve the system properly. The impact of these attacks depends on the severity of the attack especially when the target of the attack is an organization and not a single individual.

It is then crucial to detect these attacks when they are happening before it is too late to minimize the damage inflicted.

1.2 Problem Statement

The problem addressed by this research project is the lack of a comprehensive and adaptive DDoS detection system that can accurately detect DDoS attacks in real time. Current detection systems often suffer from high false-positive rates, limited scalability, and insufficient responsiveness to emerging attack patterns. Therefore, there is a need for a DDoS detection system that can overcome these limitations and provide reliable protection for individuals and organizations.

The current state-of-the-art DDoS detection systems face several challenges. Firstly, many existing detection mechanisms suffer from a high false-positive rate, leading to unnecessary disruption of legitimate network traffic. This can result in unnecessary service interruptions and impact the overall user experience. False positives also lead to wastage as network

resources are used to investigate the traffic. Secondly, the scalability of detection systems becomes a concern when faced with large-scale attacks. The ability to handle and process vast amounts of network traffic in real-time is crucial for the timely detection of DDoS attacks. Lastly, as attack techniques evolve, detection systems must be adaptive and capable of identifying new and emerging attack patterns. This necessitates the use of advanced techniques such as machine learning to enhance the system's ability to recognize unknown attacks. Addressing these challenges and developing a DDoS detection model is the primary focus of this research project.

1.3 Objectives

1.3.1 General Objective

The general objective is to develop a model capable of detecting DDoS attacks using entropy computing.

1.3.2 Specific objectives

i. To conduct further research on DDoS attacks

ii. To assess the challenges brought about by DDoS attacks

iii. To design and develop the proposed DDoS attack detection model

iv. To test and validate the DDoS attack detection model

1.4 Research Questions

- What are the types of DDoS attacks?
- What are the challenges brought about by DDoS attacks?
- How can a DDoS detection model be designed and developed?
- How can the DDoS model be tested and validated?

1.5 Justification

The proposed project is essential due to the significant threat that is posed today by DDoS attacks. By developing an entropy-based DDoS detection model, the timely detection of DDoS attacks would result in the effects of the attack being minimized greatly. The resources that would have been targeted would have uninterrupted access and their integrity would also be preserved. The losses that would have been incurred by organizations as a result of DDoS attacks would be avoided almost completely, whether financial or reputational.

This project is important as it could assist organizations and network administrators in safeguarding their systems against DDoS attacks. This could directly benefit organizations where the availability of resources is a key part of their business, for example, online banking, e-commerce, streaming services, and more. Therefore, the project is addressing a pressing need for improved DDoS detection capabilities. The findings and research from this project could also potentially improve the field of cybersecurity and provide material for future research.

1.6 Scope

The scope of this project will cover the design, development, and evaluation of a DDoS detection model based on entropy computing. It will focus on detecting different types of DDoS attacks. The project will cover the software implementation of the model. The scope of this project does not include the mitigation of DDoS attacks, as the focus is mainly on detection. Various performance metrics, such as detection accuracy and response time, will be considered to evaluate how effective the detection system is. The evaluation will involve comparing the proposed model with existing DDoS detection techniques to assess its performance. The scope also does not cover the detection of DDoS attacks using other methods such as machine learning. The scope however does not touch on the deployment of the system in a live environment or the evaluation of its performance under high-volume DDoS attacks. The focus will instead be on evaluating the model in a simulated environment.

1.7 Limitations and Delimitations

While this research project aims to develop a DDoS detection model, it is essential to acknowledge certain limitations that may impact the scope and capabilities of the proposed

model. One limitation is time. Due to the project being a one-semester project, it had a specified timeframe as it was to be completed in a few months. For this reason, the project scope is focusing on the detection of DDoS attacks and not its mitigation or prevention. Another limitation is the lack of access to real-life network environments. With this access, the project could have involved real-life testing of the model for evaluation. The alternative chosen was to run the test in a simulated/virtual environment.

Among the limitations was the lack of high-performance computing resources. The device used for this project could only handle a certain number of components on a network and could not be used for evaluation of the model on a large system architecture or a large-scale DDoS attack. For this reason, the project is focusing on detecting attacks on networks that are not very large in size. Another limitation was a limited skill set. The team working on the proposed project does not involve expert programmers or software developers in its personnel and as such does not involve high-level programming. Due to this, the project complexity will not be as high and will only utilize relatively simpler tools and programming languages.

Chapter 2: Literature Review

2.1 Introduction

This section provides a comprehensive overview of the existing literature on Distributed Denial of Service (DDoS) attacks and detection systems. Its purpose is to examine the current state of research and industry practice regarding DDoS attacks and their detection by reviewing a range of research papers, academic articles, and industry reports that focus on this topic. The literature review should serve as a foundation for understanding challenges and advances in DDoS detection and guides the development of the proposed DDoS detection model.

2.2 Further research on DDoS attacks

A DDoS attack as stated before, is an explicit attempt by attackers, to use multiple devices at the same time to overwhelm a computer target's ability to handle incoming communications, prohibiting legitimate users from accessing the service (Douligeris & Mitrokotsa, 2004; Whitman & Mattord, 2017). These attacks are a common problem in today's world of internet security. According to Kaspersky, an average of 824 attacks per day were detected in the month of August 2022 by its DDoS Intelligence system (Kupreev et al., 2022). In this section, we will look further into DDoS attacks to get a deeper understanding of the problem.

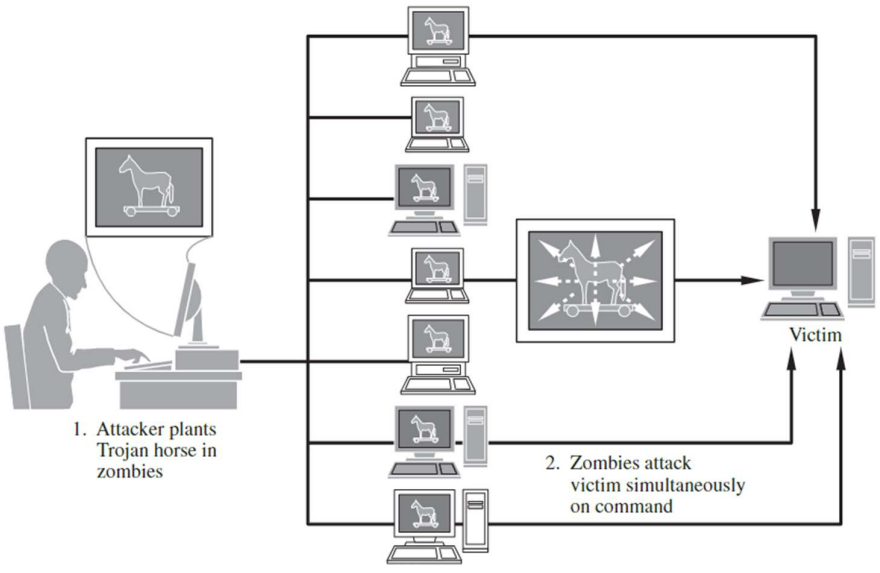

Figure 2.1 A DDoS attack (Pfleeger et al., 2015)

A DDoS attack can be broken down into 4 stages, namely agent selection, compromise, communication, and execution. In the first stage, the attacker goes through the process of selecting. In the first stage, the attacker must find a way to take ownership of various devices. Devices could include PCs, mobile phones, or even IoT devices such as smart TVs. There are many ways hackers can discover these devices and take responsibility for them. This then leads to the next step, compromise. This step is the reason why the attacker specifically crawls the internet to find devices with known vulnerabilities. The attacker will have to find a way to compromise the devices and make them 'slave' devices. This can be done in various ways such as phishing.

The third step, communication is where the attacker establishes a means of communication with the compromised device. This is done so that the device can comply with any directions the programmer sends to the gadget at any given time. This can be done by installing a small program on the compromised device after compromising it. The final step, execution is where the attack takes place. Once the hacker has established a huge number of gadgets under his control, he/she can execute the DDoS attack.

There are a lot of different types of DDoS attacks that can be carried out today and a wide range of classifications have been proposed in the literature, over the past years. The classifications are based on the different features of DDoS attacks such as the architectural model, exploited vulnerability, weakness exploited, protocol level, degree of automation, attack rate, impact, scanning strategy, propagation strategy, and resources involved (Gupta et al., 2009). Among these, the protocol level is mostly used in the classification of these attacks since it is extremely simple to group DDoS attacks (De Donno et al., 2018). Basing the attack on the protocol level used, it is possible to separate the attacks into two categories: Application Level attacks and Network Level attacks (Alomari et al., 2012; Zargar et al., 2013).

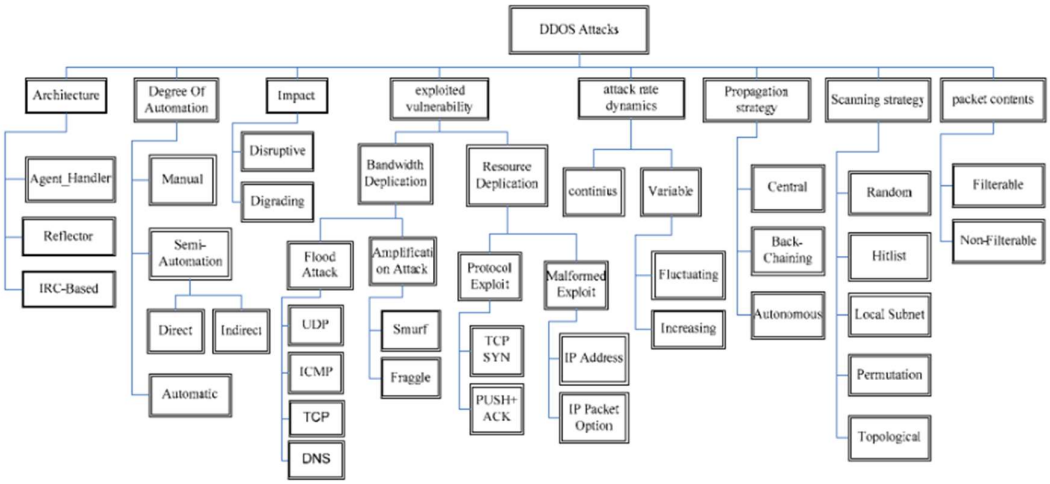

Figure 2.2 DDoS attack Classification (Asosheh & Ivaki, 2008)

The first type, Application Level attacks, target application-level protocols to exhaust the system resources. Examples of these attacks are DNS Amplification attacks, DNS Flood attacks, and HTTP Flood attacks. Network Level attacks on the other hand target either network or transport layer protocols to perform the attack. Examples of this type of attack are UDP Flood attacks, ICMP Flood attacks, PUSH and ACK attacks, and TCP SYN attacks (Bishop, 2006).

2.3 Impacts of DDoS attacks

DDoS attacks have emerged as a significant threat to individuals, organizations, and even entire industries. The aim is to explore the impacts of DDoS attacks, highlighting the consequences they have on targeted entities.

One of the most straightforward and visible effects of a DDoS attack is the disruption of online services. By overloading a target system or network with traffic, an attacker can exhaust available resources and prevent the system from responding to legitimate requests. This results in service unavailability, downtime, and lost productivity. For businesses and organizations that rely heavily on online operations, such as e-commerce platforms, financial institutions, and government agencies, service interruptions can lead to significant financial losses and customer dissatisfaction.

DDoS attacks can also have a severe monetary impact on both individuals and businesses. Individuals are rarely affected but there have been cases where criminal groups have threatened their victims with a DDoS attack unless they paid 5 bitcoins which at the time was more than $5,000 (Makrushin, 2017). Organizations targeted by DDoS attacks often experience revenue loss because they are unable to generate sales, fulfil orders or provide services during the attack. This is especially harmful to e-commerce platforms in particular, as every minute of downtime can mean significant financial losses. For instance, the security of Bitfinex, a cryptocurrency trading company, was breached and $72 million in Bitcoins were stolen on 2nd August 2016. This resulted in all trading being halted for one week, hence, no trades were observed on the exchange during this period (Baldwin, 2016). Another example of this effect is the attack on the International Netherlands Group which resulted in a significant negative change in company stock price (van den Dool, 2013). Additionally, organizations may incur additional costs associated with incident response, mitigation services, and system repairs and updates to better defend against future attacks. These financial stresses can have long-term effects on an organization's financial stability and growth.

Reputation is another asset that can be affected by a DDoS attack. DDoS attacks can cause severe reputational damage to the targeted companies. Customers experiencing service interruptions or extended downtime can lose confidence in the company and its ability to protect their data and provide reliable services. This loss of trust can result in customer dissatisfaction, loss of market share and long-term damage to the brand's reputation. Research done by Abhishta (2019) shows that there are significant changes in customer behaviour in the wake of a large, successful DDoS attack on a provider whose business model includes protecting customers against such attacks. Furthermore, these changes in behaviour are not just temporary, but lasting changes in customer behaviour and permanent loss of customers were observed. Negative publicity about a successful DDoS attack can also attract media attention, adding to the reputational damage and damaging a company's image.

It can be seen that DDoS attacks have extensive effects beyond immediate service disruption. Commercial loss from attacks, together with reputational damage, can significantly weaken businesses and organizations. It is then imperative for organizations to recognize the severity of the impact of DDoS attacks and implement security measures to mitigate these risks. By

protecting against DDoS attacks, businesses can protect their online presence, maintain customer trust and ensure operational stability and resilience in a digital environment.

2.4 Review of existing systems

2.4.1 Machine Learning Techniques

Machine learning is the field of computer science that focuses on providing computers with the ability to solve problems through learning, such as in humans (Mitchell, 1997). It is a subset of artificial intelligence where computer algorithms are used to learn from data. The Machine learning model is trained using historical data. The data is then analysed by a learning algorithm, which generates a reasoning function that could be used to map new inputs that have not been seen before. ML techniques can be categorized by their purpose into supervised, unsupervised, semi-supervised, reinforcement and deep learning (Sarker, 2021).

One advantage of this technique is that they identify patterns indicative of a DDoS attack with high accuracy. ML models trained on tagged datasets can learn to distinguish between normal and malicious traffic, reducing false positives and false positives which results in higher accuracy. According to Idhammad et al., (2018), various experiments were performed using three public datasets namely NSL-KDD, UNB ISCX 12 and UNSW-NB15. An accuracy of 98.23%, 99.88% and 93.71% and false positive rates of 0.33%, 0.35% and 0.46% were achieved respectively. Another advantage is it can detect attacks in real time. ML algorithms can detect anomalies and suspicious patterns, trigger proactive responses and stop attacks before they disrupt any service. Research done by Bhayo et al. (2023) the HADEC framework takes less than 5 min to process 1 GB of a log file having 15.83 GB of generated live traffic.

2.4.2 Signature-based detection systems

These systems deploy signature or pattern detection and store the signatures of known attacks in a database. Each communication is monitored and compared with the database entries to discover any occurrences of DDoS attacks. The database is updated with new attack signatures occasionally to detect new types of attacks. Snort and Bro are examples of systems that use signature-based attack detection.

The advantage of this technique is that they are very effective in detecting well-known and documented attacks (Chandola et al., 2009). By matching network traffic against the signatures in the database, this method can accurately identify specific attack types. Another reason why these systems are used is that they produce low false positive rates (Mirkovic & Reiher, 2004). By using predefined patterns, these methods effectively distinguish malicious traffic from normal network traffic, minimizing the possibility of misidentifying legitimate user activity as an attack.

2.4.3 Anomaly-based detection systems

Systems that deploy anomaly-based detection have a model of normal system behaviour, such as normal traffic levels or the expected system performance. The current state of the system is periodically compared with the models to detect any differences or anomalies.

According to Zekri et al., (2017), the main advantage of these systems is that they excel at detecting unknown and zero-day attacks. By identifying deviations from expected patterns, detection of even the most novel and sophisticated DDoS attacks is possible, providing a proactive defence mechanism against evolving threats. Another benefit is that anomaly-based techniques tend to have low false positive rates. These methods reduce the likelihood of misidentifying legitimate traffic as malicious by focusing on deviations from normal behaviour.

2.5 Existing gaps

Gaps are existing in DDoS attack detection as the systems are all inadequate in some way. This section will focus on some of the gaps and limitations of these systems.

One limitation is the inability to detect zero-day attacks. Signature-based DDoS detection systems are unable to detect zero-day attacks (A. Fakeeh, 2016). This is because they can only identify attacks by matching them with known attack patterns.

Data availability is also another issue in detection systems, especially those using Machine Learning. ML algorithms rely heavily on training data for accurate recognition. Due to the limited availability of such data, it can be difficult to obtain large and diverse datasets containing labelled DDoS attacks. Furthermore, if the training data is biased toward a particular

attack type, the model may have difficulty detecting new and evolving attack techniques, resulting in reduced effectiveness.

Another issue is the scalability of these systems. ML and signature-based systems rely on training datasets and signature databases respectively. If these do not get updated regularly the systems will become inefficient in detecting the attacks. This process of updating requires significant effort and resources in itself.

High computational requirements are also another limitation of these systems. The process of monitoring network traffic while using ML, anomaly-based or signature-based detection systems can consume significant computing resources. This can lead to overhead which can impact network performance and latency, especially during large-scale DDoS attacks. Training and deploying the ML models also requires substantial processing power and storage resources.

Another limitation of these systems is high false negative rates. One of the major challenges of anomaly-based techniques is their susceptibility to high false negative rates (Mirkovic & Reiher, 2004). Because these techniques rely on detecting deviations from normal behaviour, they may misidentify normal behaviour as an attack.

2.6 Conceptual Framework

This section presents a conceptual framework for the proposed DDoS detection model. It outlines the key components and processes involved in the detection system, including inputs, processes, storage and outputs.

Entropy can be described as a measure of uncertainty. Entropy is a scientific concept that is most commonly connected with randomness, state of disorder, or uncertainty (Pardhi et al., 2022). This is the main reason for considering entropy as a DDoS detection system. The higher the randomness the higher the entropy is and vice versa. So, whenever the entropy is less than a threshold value, we can say that a DDoS attack occurs. The threshold entropy value can be determined by observing the model under normal traffic conditions. The following equation can then be used to calculate the value of the entropy, H.

$$H = -\sum_{x=1}^{n} P_i \log_2 P_i$$

Equation 2.1 The mathematical equation for Entropy calculation

The model would include a network topology with an SDN controller, multiple switches and hosts and this is where the target of the attack would be as seen in the diagram below. A predefined window size would need to be defined as we will calculate the entropy on a per-window basis. The model would also have a counter to determine whether or not an attack has occurred.

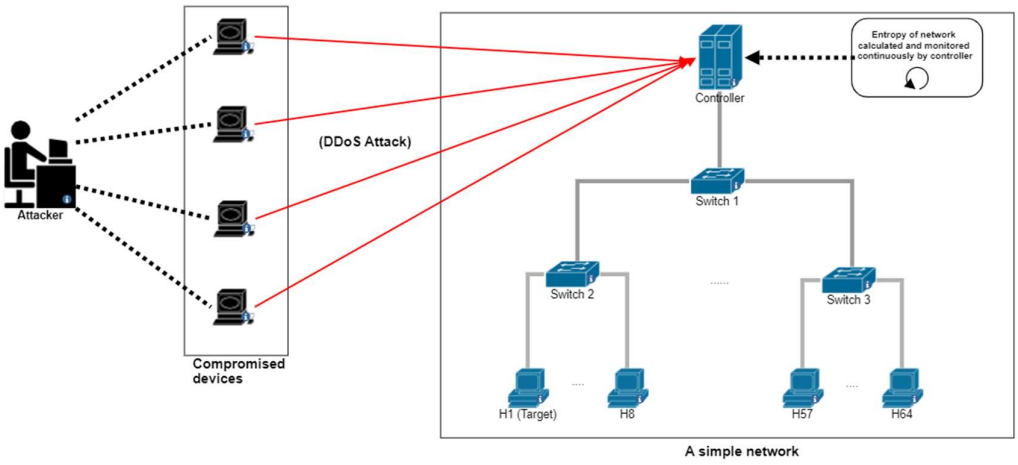

Figure 2.3 Conceptual framework

As new packets would enter the network, the controller would check the destination address of the packet and adds it to a list. It then checks if the packets have reached a pre-set number, for example, 50, and if it has not, it does nothing and continues monitoring packets. The pre-set number of packets is the number of packets we choose to have in a given window. If the number of entries in the list is 50, the controller calculates the entropy of that window and the list is cleared. If the value of the entropy is above the threshold value, the system continues monitoring the incoming packets like normal. If the value of the entropy value is below the threshold, the system adds one to a counter value and if the counter value equals a pre-set value,

for example, 5, a DDoS attack notification is sent. If the value of the counter has not equalled 5, it continues monitoring the incoming packets.

Chapter 3: Methodology

3.1 Introduction

System development methodology refers to a framework that is used to structure, plan and control the process of developing an information system. This chapter involves a deeper description of the approaches and methodologies to be used in the development and testing of the proposed entropy-based DDoS detection model.

3.2 Research approach

The research approach that will be used is Object-Oriented Analysis and Design (OOAD). By allowing the identification of key entities, their relationships, and the behaviour of the system, OOAD offers a systematic approach to building software systems. The technique includes multiple phases, such as requirements collecting, system analysis, system design, and system implementation.

3.3 Methodology

For this project, the Agile methodology has been chosen. Agile methodology has gained significant recognition and popularity in project management due to its iterative and flexible approach. One of the main reasons for choosing the Agile methodology is its inherent adaptability. Highly structured methodologies struggle to manage changes and unplanned deployments, leading to delays and inefficient resource allocation. However, Agile methodologies consider change to be a natural part of the development process. Agile uses iterative cycles called sprints to enable teams to respond quickly to changing requirements, adjust priorities, and adjust project scope accordingly.

Another reason is that Agile methodologies focus on iterative development so that the work steps of a project can be carried out on a regular basis. This iterative approach allows for faster feedback loops, leading to the early detection of problems and deviations from project goals. This also allows changes to be incorporated early, minimizing the risk of rework. This iterative nature of Agile methodology ensures a more efficient and leaner development process.

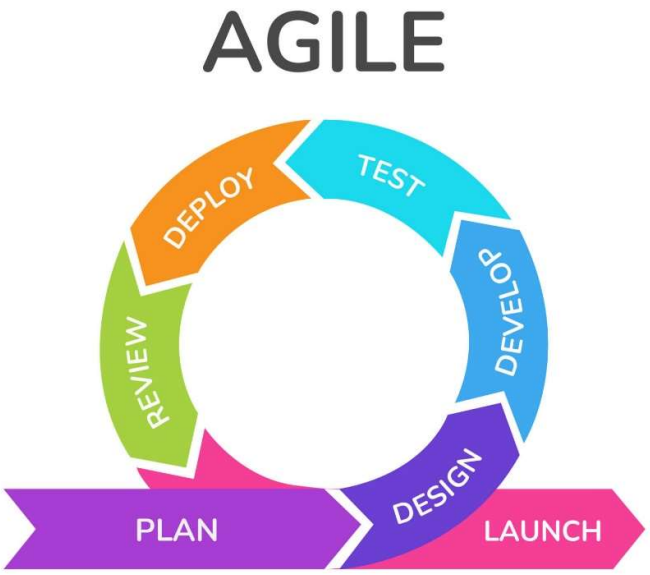

Figure 3.1 Agile methodology overview

3.3.1 Plan

This is the first step of the agile methodology. It is where the vision of the project is created and involves gathering relevant data, mapping processes and coming up with the scope. The data in this phase is analysed to ensure they are realistic and achievable. The functional requirement of the proposed system is that it should be able to detect DDoS attacks. The non-functional requirement is that it should be able to show the user what is happening during the attack.

3.3.2 Design

This step uses the data gotten from the planning phase to come up with the design of the system to optimize it with the right technology. According to the data obtained, the system should include a simple network topology.

3.3.3 Development

This phase involves the actual creation and coding of the system based on the designs obtained from the design phase. The system will be created using Python as a suitable programming language for the design.

3.3.4 Testing

This is the phase where the developed system is put to the test to find out if there are any bugs or problems in it. White box testing will be used for this phase.

3.3.5 Deployment

This is the phase that involves installation, configuration and making changes to optimize the performance of the model.

3.3.6 Review

This is the phase where the data obtained from the deployment phase is carefully examined to validate the quality, functionality and other components of the model. After doing this, further improvements can be made to the model or it can be launched.

3.3.7 Launch

This is the final phase of the methodology where the model is officially complete and ready. This is usually done after closely examining the reviews gotten earlier and not identifying any issues.

3.4 Deliverables

These will be the products of the project. These are:

- The proposed DDoS detection model
- The research proposal and documentation of the project

3.5 Tools and Techniques

3.5.1 VirtualBox

Oracle VM VirtualBox is cross-platform virtualization software that allows users to extend their existing computer to run multiple operating systems. It will be used to run the model environment.

3.5.2 Mininet

This is a high-performance network emulator that will be used to create the simulated network.

3.5.3 Python programming language

This will be the programming language used to write the code that simulates the DDoS attack, more specifically Python 3.

3.5.4 Scapy

This is a powerful interactive packet manipulation library in Python which can forge or decode packets of a wide number of protocols. It will be used to generate the packets used in the model.

Bibliography

A. Fakeeh, K. (2016). An Overview of DDOS Attacks Detection and Prevention in the Cloud. *International Journal of Applied Information Systems*, *11*(7), 25–34. https://doi.org/10.5120/ijais2016451628

Abhishta, A. (2019). *The blind man and the elephant* [PhD, University of Twente]. https://doi.org/10.3990/1.9789036549127

Alomari, E., Manickam, S., Gupta, B. B., Karuppayah, S., & Alfaris, R. (2012). Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. *International Journal of Computer Applications*, *49*(7), 24–32. https://doi.org/10.5120/7640-0724

Asosheh, A., & Ivaki, N. (2008). A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification. *WSEAS Transactions on Computers*, *7*, 281–290.

Baldwin, C. (2016, August 3). Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong. *Reuters*. https://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP

Bhayo, J., Shah, S. A., Hameed, S., Ahmed, A., Nasir, J., & Draheim, D. (2023). Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. *Engineering Applications of Artificial Intelligence*, *123*, 106432. https://doi.org/10.1016/j.engappai.2023.106432

Bishop, M. (2006). *Introduction to Computer Security* (1st ed.). Addison-Wesley Professional.

Chandola, V., Banerjee, A., & Kumar, V. (2009). *Anomaly Detection: A Survey*. http://cucis.ece.northwestern.edu/projects/DMS/publications/AnomalyDetection.pdf

De Donno, M., Dragoni, N., Giaretta, A., & Spognardi, A. (2018). DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation. *Security and Communication Networks*, *2018*, e7178164. https://doi.org/10.1155/2018/7178164

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

Flynn, J. (2023, January 12). How Many People Use The Internet? [2023]: 35 Facts About Internet Usage In America And The World. *Zippia*. https://www.zippia.com/advice/how-many-people-use-the-internet/

Gheorge, A. (2015, May 31). *GitHub under `Largest DDoS in Site History`*. https://www.bitdefender.com/blog/hotforsecurity/github-under-largest-ddos-in-site-history/

Goncharov, M. (2012). *Russian Underground 101*. https://go.trendmicro.com/archive/docs/wp-russian-underground-101.pdf

Gupta, B. B., Joshi, R. C., & Misra, M. (2009). Defending against Distributed Denial of Service Attacks: Issues and Challenges. *Information Security Journal: A Global Perspective*, *18*(5), 224–247. https://doi.org/10.1080/19393550903317070

Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS Attacks: Trends and Challenges. *IEEE Communications Surveys & Tutorials*, *17*(4), 2242–2270. https://doi.org/10.1109/COMST.2015.2457491

Idhammad, M., Afdel, K., & Belouch, M. (2018). Semi-supervised machine learning approach for DDoS detection. *Applied Intelligence*, *48*(10), 3193–3208. https://doi.org/10.1007/s10489-018-1141-2

Kottler, S. (2018, March 1). February 28th DDoS Incident Report. *The GitHub Blog*. https://github.blog/2018-03-01-ddos-incident-report/

Kupreev, O., Gutnikov, A., & Shmelev, Y. (2022, November 7). *Report on DDoS attacks in Q3 2022*. https://securelist.com/ddos-report-q3-2022/107860/

Makrushin, D. (2017, March 23). *The cost of launching a DDoS attack*. https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS Defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*. https://doi.org/10.1145/997150.997156

Mitchell, T. M. (1997). Does Machine Learning Really Work? *AI Magazine*, *18*(3), Article 3. https://doi.org/10.1609/aimag.v18i3.1303

Nicholson, P. (2020, June 24). *AWS hit by Largest Reported DDoS Attack of 2.3 Tbps | A10 Networks*. https://www.a10networks.com/blog/aws-hit-by-largest-reported-ddos-attack-of-2-3-tbps/

Pardhi, P. R., Rout, J. K., & Ray, N. K. (2022). A Study on Performance Comparison of Algorithms for Detecting the Flooding DDoS Attack. *2022 OITS International Conference on Information Technology (OCIT)*, 433–438. https://doi.org/10.1109/OCIT56763.2022.00087

Patrikakis, C., Masikos, M., & Zouraraki, O. (2019, August 26). *Distributed Denial of Service Attacks—The Internet Protocol Journal—Volume 7, Number 4—Cisco*. https://web.archive.org/web/20190826143507/https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html

Petrosyan, A. (2023, May 22). *Internet and social media users in the world 2023*. Statista. https://www.statista.com/statistics/617136/digital-population-worldwide/

Pfleeger, C. P., Pfleeger, S. L., & Marguilies, J. (2015). *Security in Computing* (5th ed.). Pearson.

Sarker, I. H. (2021). Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Computer Science*, *2*(3), 160. https://doi.org/10.1007/s42979-021-00592-x

Turner, G. (2022, August 4). DDoS attack durations see sharp rise throughout Q2 2022. *DIGIT*. https://www.digit.fyi/ddos-attack-durations-see-sharp-rise-throughout-q2-2022/

van den Dool, P. (2013, April 10). *ING ondanks maatregelen getroffen door nieuwe DDos-aanval*. NRC. https://www.nrc.nl/nieuws/2013/04/10/ing-nieuwe-cyberaanval-sneller-afgeslagen-door-maatregelen-a1435706

Weiler, N. (2002). Honeypots for distributed denial-of-service attacks. *Proceedings. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 109–114. https://doi.org/10.1109/ENABL.2002.1029997

Whitman, M. E., & Mattord, H. J. (2017). *Principles of Information Security* (6th ed.). Cengage Learning.

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials*, *15*(4), 2046–2069. https://doi.org/10.1109/SURV.2013.031413.00127

Zekri, M., Kafhali, S. E., Aboutabit, N., & Saadi, Y. (2017). DDoS attack detection using machine learning techniques in cloud computing environments. *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*, 1–7. https://doi.org/10.1109/CloudTech.2017.8284731

Appendices:

Appendix 1: Gantt Chart