Honours Project Final Report

2019-2020

Submitted for the Degree of:
BEng Networked Systems Engineering

Project Title: A Simulation Study of Distributed Denial of Service (DDoS) Attacks in a WLAN Corporate Environment

Name: James Mearns

Programme: Networked Systems Engineering

Matriculation Number: [redacted]

Project Supervisor: [redacted]

Second Marker: [redacted]

Word Count: 9,017
(*excluding contents pages, figures, tables, references and Appendices*)

"Except where explicitly stated, all work in this report, including the appendices, is my own original work and has not been submitted elsewhere in fulfilment of the requirement of this or any other award"

Signed by Student: James Mearns Date: 22/04/2020

Contents

1. Introduction

1.1 Background

A WLAN (Wireless Local Area Network) is a network in which two or more devices are linked using wireless communication technologies within a defined area (in this case a corporation) [1] [2]. This allows companies to cover a wide area with their networks and provides employees with the freedom to move around within the company building(s) or even work from a mobile device. WLANs also provide a stable connection to the internet via gateways [3] [4]. WLAN networks are flexible, require no cabling therefore have no wiring issues and are much more resilient to physical issues such as fires and environmental hazards.

1.1.2 The History of WLAN

Wireless LANs were not always as powerful and desirable as they are today, they first came into being in 1997 when the IEEE802.11 committee was formed, establishing the standard for what would become globally known as "WiFi" [5] [6]. The WLAN connections of this era were only capable of supporting a maximum data transfer speed of two megabytes per second. This caused companies to believe that WLAN was evolving into a slow and unreliable service and they were reluctant to replace their faster wired connections. However, by 1999 WiFi became available in homes and began to take off, products evolved into IEEE802.11b and then to IEEE802.11g [7]. This brand new WiFi standard was up to five times faster than its predecessor and still stands as one of the most popular options today thanks to its solid fifty-four megabytes per second speed and backwards compatibility features. The most up-to-date WiFi technologies have replaced the *"802.11x"* naming scheme with the much simpler *"WiFi X"*. Today, the fastest type of WLAN network available is known as WiFi 5. In pristine conditions, speeds of almost six hundred megabytes per seconds are attainable.

1.1.3 DoS (Denial of Service)

Denial of Service attacks are malicious attacks which are carried out to deny legitimate users access to an application or service [8]. DoS attacks are carried out by a single user spoofing obscene amounts of traffic to shut down a website/service or otherwise [9] [10]. This method of cybercrime is becoming an increasing danger due to growing global reliance on the internet, which is providing opportunistic hackers with an even greater attack surface. The more the world at large relies on the wireless internet, the greater a threat DoS poses [11] [12] [13].

Distributed Denial of Service (DDoS) attacks are an evolved version of DoS attacks. DDoS attacks use multiple machines and/or virtual attackers to replicate legitimate user traffic to flood and crash a targeted service or application, this makes DDoS a very difficult problem to combat [14] [15].

1.1.4 Threats to Corporate WLAN Environments

It is important to understand that a corporate WLAN environment differs significantly from a generic home or personal WLAN environment. These differences make the effect of DDoS on these networks far more disruptive than it would necessarily be in a personal/home environment, for example, DDoS attacks on corporations have the potential to prevent companies from accessing vital databases or locking them out of sensitive information causing them to lose time, money and the trust of their clients. Furthermore, many modern companies (including small businesses) rely heavily on cloud technology, DDoS attacks can deny access to cloud-based systems thereby blocking access to customers, employees, and technicians.

1.2 Project Outline

1.2.1 Project Aim

The aim of this project is to produce a simulation based on a corporate WLAN environment. The simulation will test environments of three sizes; small, medium and large. The three different environments will then be analysed under the stress of a DDoS attack using network performance statistics such as packet delay, packet loss, bandwidth, throughput, latency, jitter and error rate to determine which network suffers the highest overall strain. OPNET modelling software will be used to simulate common DDoS attacks such as; UDP Floods, TCP Floods, SYN-ACK Floods, Ping-of-Death and Teardrop. Using OPNET, network performance statistics will be taken from each scenario and analysed in order to present a conclusion, determining the effect DDoS has on each of the WLAN environments. Thereby the research question for this project will be:

How do Distributed Denial of Service Attacks affect network performance in WLAN corporate environments in terms of network performance statistics?

1.2.2 Secondary Research Objectives

The completion of a literature review will allow the following objectives to be explored further;

- Examine WLAN topologies used in prior research and adapt to suit this project
  The base of the project will be the three WLAN testbeds which will be constructed to carry out DDoS attacks on. It is important to understand previous research into this topic and topologies which have been used to allow for the construction of accurate testbeds.

- Investigate DDoS and how it operates
  Researching DDoS in a modern environment and understanding the technologies and techniques is vital for the success of this project, understanding how attacks take place and the effect they can have on networks is extremely important when it comes to analysing the effect the attacks have on unique corporate WLAN environments.

- Examine the Effect of DDoS on Various Application Services
  Studying the effect DDoS has on different application services will help identify the current impact DDoS has on individual services. This research will aid in showing the amount of delay/strain which different attacks can place on independent application services. This will provide a good base for the final simulation when overall network performance is being analysed.

- Investigate the Impact of DDoS on Wireless Corporate Environments
  Investigation into recent or relevant DDoS attacks on corporate environments alongside prevalent research papers will show the general effect DDoS can have on WLAN corporate environments. The results of this study will provide a clearer idea of how DDoS can affect corporate networks and help identify which network performance statistics should be focussed on during the final analysis.

1.2.3 Primary Research Objectives

Objectives which have been completed during this phase are as follows.

- Development of a base testbed topology in OPNET and duplication of this to create appropriate scenarios
  Based on secondary research, a base testbed has been created as accurately and realistically as possible. This base testbed will then be populated with clients and attackers. The number of attackers will vary from five to sixty depending on the scenario. The networks in each scenario have default configurations applied and full connectivity established.

- Conducted simulations and gathered network performance statistics for analysis
  Using OPNET, simulations of DDoS floods were carried out on each of the scenarios. Data has been collected for each scenario every time simulation is run for use in further analysis. The simulations have been run multiple times over different time periods to ensure an accurate average of all relevant data has been collected.

- Compared data collected from each scenario
  Analysis of data collected from each scenario helped show which scenario put the most strain on the network presented. Data collected has been analysed thoroughly using accurate averages and as-is data points. This data has been compiled and compared for use in the drawing conclusion at the close of this project.

- Presented a conclusion based on comparison and analysis of data
  Data gathered has been compiled and presented in a legible manner to compare performance metrics in each topology under the stress of DDoS floods from varying numbers of attackers. The data comparison has been presented graphically and analysed through text. The resulting comparisons show the effect of DDoS on different corporate WLAN environments thus providing an apt conclusion regarding the overall effect of DDoS on corporate WLAN environments.

2. Literature Review

This section of the report will provide an in-depth analysis of research conducted by others related to the Secondary Objectives mentioned in Section 1.2.2. The objectives are as follows;

- Examine WLAN topologies in prior research
- Investigate DDoS and how it operates
- Examine the effect of DDoS on various application services
- Investigate the effect of DDoS on wireless corporate environments

Understanding these underlying objectives and compiling research carried out by others will allow for a more complete and thorough simulation project to be carried out.

2.1 Examine WLAN Topologies

Understanding topologies used in related research will be vital in ensuring that the topologies generated for this project are accurate and functional to best demonstrate the effect of DDoS attacks. In [20] it is noted that a common topology used in networks is a star topology and the average bandwidth between router devices is 100Mbps. Furthermore, this research notes that 80% of all end devices are clients, leaving 20% to be servers. Further research conducted in [21] uses 80 nodes in a uniform distribution and steadily increases the node count over time to obtain accurate throughputs, detection rates and delays. This is prominent to this research as it is vital that attacker counts and node counts vary to obtain the most accurate statistics possible. In the same paper, the simulations are run 10 times over to ensure best averages are obtained.

In a study conducted in [22], 7 hosts are connected to a wireless access point which then has various DDoS attacks carried out on it, aiming specifically for WH1. This research uses this topology with varying attacks and attacker numbers. Understanding this and other research topologies will help this project to provide an accurate simulation and output.

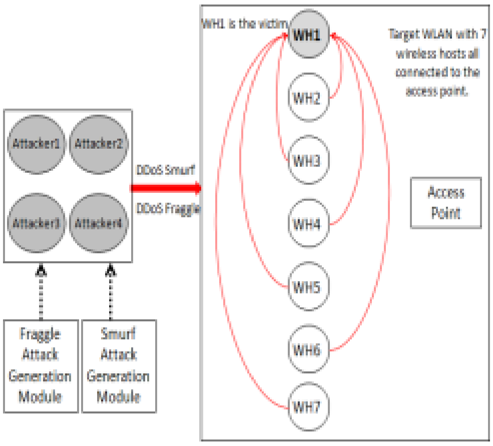

WH1 is the victim
WH1
WH2
WH3
WH4
WH5
WH6
WH7
Target WLAN with 7 wireless hosts all connected to the access point.
Access Point
Attacker1
Attacker2
Attacker3
Attacker4
DDoS Smurf
DDoS Fraggle
Fraggle Attack Generation Module
Smurf Attack Generation Module

Figure 2

2.2 Investigate DDoS and how it Operates

Sections 1.1.3-1.1.6 of this project provided an overview of DDoS attacks, BOTNETs and the three primary types of DDoS attacks. For this project to be carried out as accurately and successfully as possible it is imperative that a full understanding of DDoS and any relevant technologies is developed. Exploring how DDoS operates and why attacks are carried out will allow the author to gain meaningful insights into DDoS operations and technologies and therefore allow for a more accurate and useable simulation to be developed

2.2.1 How Distributed Denial of Service Operates

Distributed Denial of Service is a Denial of Service attack which makes use of many different hosts to make the attack even more disruptive. The users of the host machines are often completely unaware that their machines were infected via Trojans or other viruses and this can result in the number of infected hosts reaching thousands at least [23]. DDoS attacks are carried out in three primary phases; Recruitment, Propagation and Attack.

2.2.2 DDoS (Distributed Denial of Service)

A Distributed Denial of Service attack aims to render a network resource or host device inaccessible by disabling or disrupting internet services by flooding them with illegitimate traffic. DDoS attacks are generally carried out from a remote, internet-based location. These attacks occur when numerous compromised computer systems flood a targeted system with traffic, causing a denial of service effect for legitimate users of the victim network/system. As shown in *Fig I*, the compromised devices flood the target with false requests and traffic, often without even needing a direct connection to the service they are affecting [16].

DDoS attacks are carried out using “Bots” (also referred to as ‘drones’ or ‘zombies’) [17], these are a special type of malware which grants the attacker control over any infected machines. These infected machines then come together to form the base for the DDoS attack to take place, this configuration is known as a “BOTNET” [18]. Most BOTNET-based DDoS attacks can be categorised as one of three types; agent-handler, IRC-based or web-based. The figure below illustrates how a very basic DDoS attack would take place.

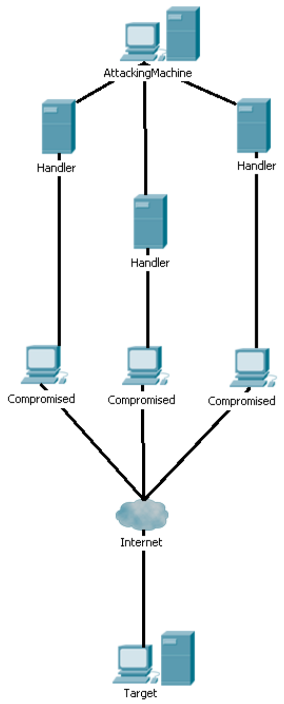


Fig I. The attacking machine connects to handlers and compromised devices, allowing the flooding of the targeted service to begin. This attack aims to falsify a large amount of web traffic to delay or stop legitimate traffic. Services such as VoIP will suffer greatly from attacks such as this, dropping audio quality or becoming redundant entirely. This can cause major issues in companies relying on this service.

2.2.3 Agent-Handler DDoS

This type of attack compromises all clients, handlers and agents taking part. In this attack, the 'Client' is contacted by the attacker within the system. The 'Handlers' are internet software packages being used to be communicate with the 'Agents'. The attacker will attempt to install the 'Handlers' on a compromised network system such as a router or a server for maximum effect. 'Agents' are software which will be planted within compromised systems where they will stay until the DDoS attack is carried out. This attack is also commonly referred to as the *"Master-Demon DDoS"* [19]. The goal here is to overload the target system so that it can no longer differentiate between client-handler and handler-agent.

2.2.4 IRC (Internet Relay Chat) DDoS

This attack model is akin to the previous except the 'Client' is directly connected to the 'Agents' via an IRC channel instead of utilising 'Handlers'. This method allows the attacker to proceed through verified IRC ports. Using these ports to send commands to the 'Agents' the attacker makes the tracking of DDoS packets very difficult. 'Agent' software hides and communicates through the channel and uses this to inform the 'Client' when it is operational [19]. Furthermore, IRC channels generate huge amounts of traffic which means the attacker can disguise their presence with ease. This is the most widely used form of DDoS.

2.2.5 Web-based DDoS

Whilst IRC is still the most prominent method of DDoS, web-based attacks are popping up more frequently in modern times. Bots in a web-based model are split into two distinct groups; bots which report statistics pertaining to a certain website and bots which are designed to be commanded and controlled via complex scripts and commands in order to carry out the attack [19].

2.2.6 Recruitment & Scanning

The first phase involves generating a BOTNET. This is done using worms to compromise vulnerable machines which the attacker can identify by scanning through networks [24]. There are many methods of network scanning which can be employed by attackers to compromise machines; random scanning, hitlist scanning, topological scanning, permutation scanning and local subnet scanning. All these methods involve the use of a 'worm'. Each method of scanning can be described as follows;

- *Random Scanning* - The worm will aggressively scan and identify vulnerable machines without requiring any input from the attacker. Scanning random IP addresses throughout the network produces massive amounts of traffic making this type of scanning more likely to be detected by intrusion detection systems [24].
- *Hitlist Scanning* – This type of scanning aims to minimise the infection time required to hijack numerous machines. This technique involves a prospective attacker generating a list of machines they consider to be vulnerable, they then release a worm which will work its way through the list until it infects a machine, when it does it will propagate half the list to that machine. Using this method, a single worm can infect all vulnerable machines on its list [24].
- *Permutation Scanning* – This is a smart-scanning technique used to prevent worms probing the same IP address multiple times. This is achieved using a pseudo-random

permutation of IP addresses to ensure that if a device is infected via permutation scanning then that device will start scanning again from a random point in the list [25]. This prevents machines which were previously infected from being infected a second time. Furthermore, permutation scanning also helps determine when to stop the scanning by examining the progress of the current infection [24].

- *Topological Scanning* – This is an alternative to Hitlist Scanning in which the worm selects its next target based on information obtained from an already infected machine. If the worm manages to infect an application, then it has the potential to acquire a list of peers for targeting. This technique therefore does not require the attacker to produce their own list of initial targets, making this method a quicker starting option [24].
- *Local Subnet Scanning* – This technique involves an already compromised host searching for new targets within a its own subnet and trying to infect them. The primary purpose of this method is to infect as many local machines as possible within a sub-network [24].

2.2.7 Propagation & Attack

Propagation is the phase preceding the attack phase. This phase propagates the attack code to all compromised devices, this code will include info about the victim, time and duration of the attack being carried out. There are three types of propagation; Central Source, Back-Chaining and Autonomous. All three types involve the use of a worm [26] to propagate infected code, central source focusses on placing a high burden on a central server, however, this makes the attack vulnerable as it presents a single point of failure [25]. Back-chaining and autonomous are more survivable attacks, avoiding single points of failure whilst still propagating the attack successfully [25]. The attack phase is the final phase and there are countless methods and techniques which can be used to execute DDoS attacks. This project aims to select a few methodologies and study and compare the effect they have on different environments, therefore an in-depth analysis of selected attacks will come in a later section,

2.3 Effect of DDoS on Application Services

In order to effectively analyse and compare results obtained via this paper, it is important to look into previously conducted experiments and simulations to study the effect of DDoS. The primary applications to focus on will be voice, video and overall network delay. Research conducted by Bogdanoski, Shuminoski and Risteski into the SYN Flood attack presents an in-depth analysis of the effect of DDoS on the aforementioned variables [14].

2.3.1 Voice Application

Voice, video and TCP segment delay are all analysed on a small OPNET WLAN scenario. When voice applications are analysed under the effect of DDoS it is clear that the delay over time in the application increases exponentially, having a catastrophic effect on the service [14]. Voice applications under this extreme amount of delay become essentially unusable. Delay variation reaches upwards of 4.5 seconds, this would make voice communication in a network extremely difficult. Further research from Bogdanoski demonstrates the effect of a DDoS ICMP flood attack on a network voice service. Packet end-to-end delay varies massively when attacks are underway. In the presented scenario, delay must not exceed 80ms, however, under DDoS stress this is not the case [11]. Delay reaching unacceptable levels can be devastating for voice applications, especially in corporate environments relying on voice conferencing or VoIP to communicate within the company.

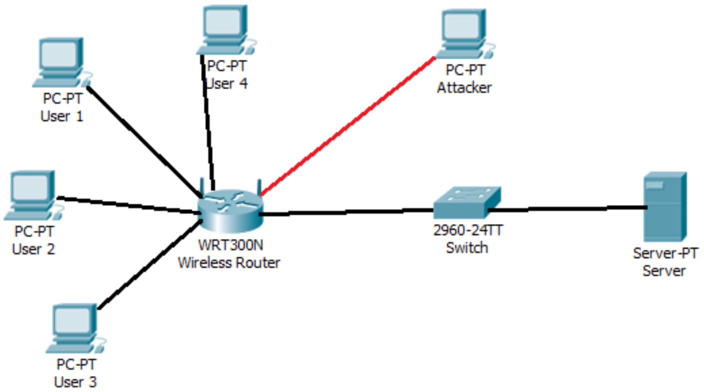


Fig 3. A diagram of a simple ICMP Flood. The attacker overloads the central router with ICMP traffic, denying the legitimate users access.

2.3.2 Video Application

Video applications are commonly used in corporations to participate in long distance conference calls or to help employees work from home. Many international corporations rely on video conferencing to conduct their daily business and DDoS can cause serious problems for this. Video applications can be almost fully stalled out by DDoS attacks. When video applications are overwhelmed by SYN flooding, the buffers fill up rapidly, causing a massive amount of traffic to be dropped [14]. This traffic dropped can cause video calls and conferences to become impossible. Massive amounts of dropped packets can result in call quality dropping to almost zero or even cutting off the calls entirely.

2.3.3 Data Applications Transmission and Delay

DDoS can cause serious delays in WLAN data transmissions. Delays in data transmissions mean that websites will fail to load or clients will be unable to communicate with each other. Research in [14] demonstrates that under the strain of the SYN Flood attack there is almost 3 seconds of delay in the network. This end-to-end delay within a network can slow down corporate operations, costing valuable time and money for the company.

2.4 Impact of Distributed Denial of Service on Corporate Environments

The growth of the internet as well as e-commerce industries makes Distributed Denial of Service a dangerous and evolving menace. The wave of DDoS attacks carried out in the early 2000s are prominent example of the catastrophic effect DDoS can have on unprotected web services. Yahoo, CNN, Amazon, E*Trade and other high-profile e-commerce trading websites were made unavailable for lengthy periods of time as a result of the attacks [27]. An article in *Technology News* from the time notes that these attacks cost corporate victims millions of dollars and shook the e-commerce industry. Furthermore, in this same article, David Kennedy of the ICSA (an internet security provider) raised concerns that many networks were being constructed to attain maximum speed and efficiency whilst neglecting security altogether [28]. This research highlights the devastating effect Distributed Denial of Service can have on corporate environments, costing even the largest companies time and money. However, there are still recent and relevant examples of DDoS affecting e-commerce giants like Amazon's AWS. In October of this year AWS' DNS systems were slammed by a prolonged DDoS attack, taking down numerous AWS services in the process. The attack lasted a total of 6 hours, causing serious problems for AWS reliant services [29].

2.4.1 Smokescreening

It is vital that corporate environments have tough enough security measures in place to deal with any additional threats which DDoS brings along with it. When other types of cyberattack tag along with DDoS it is referred to as 'Smokescreening', this is because the DDoS attack provides a 'smokescreen' to misdirect technicians whilst the intruder plants spyware, breaks into the network or leaks company data [30] [31]. In a survey carried out by Kaspersky Lab and B2B International, 74% of companies reported that DDoS attacks would be accompanied by other IT issues on that same day. Of these companies, 45% reported malware issues, 32% reported network intrusions and a further 26% reported data leaks [30]. These are all major issues for corporations as they potentially hold sensitive customer information (bank details, addresses etc.) or have important files stored on their networks which they do not want others having access to and DDoS 'Smokescreening' provides attackers with a window of opportunity to cause unprecedented disruption.

3.0 Methodology

3.1 Research Methodology

This project aims to analyse the effect various DDoS attacks have on corporate WLAN environments. To achieve the best results this simulation project will employ the CISCO PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimise) methodology. This is unique to networking projects and follows a very strict flow, therefore providing the most benefit to a network project [32]. Each PPDIOO stage is summarised as follows:

- ➢ Prepare: Establish topology requirements and create a concept of the network to identify beneficial/relevant technologies.
- ➢ Plan: Identify network requirements within defined scope and based on what is necessary (in this case a close to real life recreation of a corporate topology), the planning phase for this project will focus on network size and base performance.
- ➢ Design: Detail specifics regarding the network before implementing e.g. security, performance and technical requirements. For this project network design will focus on the performance of the network and analysis of statistics which can be used to determine performance.
- ➢ Implement: Create the network whilst minimising points of failure and avoiding any potential vulnerabilities.
- ➢ Operate: Network health is maintained, and any errors identified are corrected. This phase is vital to the project as it allows analysis of performance statistics.
- ➢ Optimise: Manage the network and continue to improve it, this will allow network performance to be monitored and show where it drops under the stress of DDoS.

This project involves building a simulation model and should address numerous issues. According to Uros Breskvar and Miroljub Kljajic in [33] a simulation project should have six stages. The stages are as follows:

1. Plan
2. Define the System
3. Build a Model
4. Experiment
5. Analyse Results
6. Report Results

These stages will be considered when analysing the results obtained from the topologies generated. The outcome of this simulation will be to acquire enough data so that the effect of DDoS attacks on corporate WLAN environments can be effectively analysed. This project chose to use simulation methodology as it had the clearest advantages in this case. Simulation methodology allows various questions to be answered simultaneously thanks to the iterative nature of simulation as well as how easy it is to duplicate and change scenarios. Furthermore, the use of Riverbed Academic Edition makes the process zero cost and makes analysis of countless scenarios readily possible. However, the project must be cautious when undertaking this approach as it will be easy for the scope to grow out of control if not monitored carefully. The timescale of this project must be kept in mind as although there are endless possibilities with simulation there is not enough time here to cover them all. Finally, simulation allows for a great amount of data to be collected and compiled from various scenarios which will allow a more accurate and detailed conclusion to be drawn. The use of simulation methodology was chosen over development and experimental methodologies for various reasons. Development methodologies do not suit this project as they are based around customers and personal interactions whereas this topic is focused more on tools and processes. Furthermore, the development methodologies involve adapting to continuous change, which is not present with this project as it is based on static simulation designs. Experimental methodologies do not suit this project as they are extremely time consuming. More importantly, ethical and legal issues come into play with experimental methodologies as it is then taking the DDoS out of a simulated environment and into a real one, thus ensuring that it is kept controlled and contained could present issues.

3.2 Refined Objectives

3.2.1 Developed a base testbed topology in OPNET and duplicated this to create appropriate scenarios

For this project, three network topologies were be created; one with few attackers, one with a decent amount of attackers and one with a large number of attackers. These networks are configured appropriately and are fully connected and provide an output which can be analysed effectively. A base scenario has been created which will be used for comparison to help determine the full effect DDoS flooding has on corporate WLAN environments. Based on literature review research, topologies will be constructed as follows:

Reduced Attackers		Medium Attackers		Large Attackers	
Clients	5	Clients	5	Clients	5

Infected	10	Infected	40	Infected	60
Sim Time (s)	840	Sim Time (s)	840	Sim Time (s)	840

3.2.2 Conducted simulations and gathered network performance statistics

OPNET has been used to simulate various DDoS attacks on each network topology. The attacks were carried out iteratively. This is to ensure that stats acquired from the attack runs are as accurate as possible. Statistics which were be analysed to determine the effect of DDoS were be;

- Throughput
- CPU Utilisation %
- Response Times

These statistics were chosen as they help accurately identify the stages of the attack as they take place and they show the detrimental effect of DDoS on the corporate environments as it is expected that when under stress the CPU utilisation percentages and response times will peak.

3.2.3 Compared data collected from each scenario

Each scenario has been compared in terms of network performance as described above to determine which of the scenarios underwent the largest drop in overall performance when under the effect of DDoS flooding. Determining the effect each attack had on the various sizes of network will allow for a more thorough and accurate conclusion to be presented.

3.2.4 Presented a conclusion based on comparison and analysis of data

After comparison, data has been grouped together and compared for a complete analysis. The output attained will definitively show which topology suffered the most from the effects of the DDoS floods. This allowed a conclusion to be drawn based on data which helped identify which of the scenarios took the largest performance hit when it comes to the effects of DDoS flooding.

3.2.5 Hypothesis

For the scenarios to be presented in this project, it is expected that all three scenarios will present major issues for any corporate network. The first scenario is expected to cause the least disruption due to the low amount of infections and clients; the second scenario is expected to cause high disruption due to the ratio of infected:healthy devices present. This scenario should present significant delays and increases in CPU usage. The final scenario should prove the most detrimental causing serious delays in response time and maxing out CPU utilisation. This scenario should prove the most problematic as it has the highest ratio of infected:healthy devices presented across all scenarios.

4.0 Execution

4.1 Summary of Project Implementation

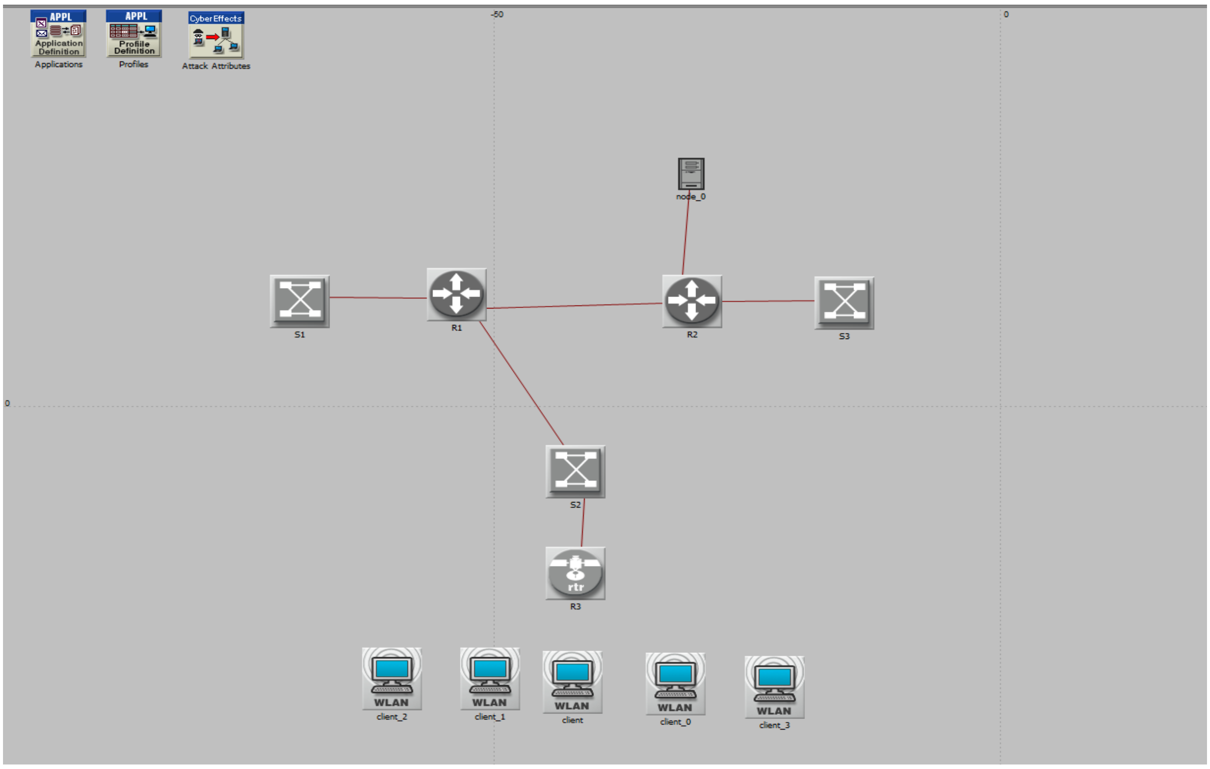
The development of test scenarios for use in this project was carried out using Riverbed Modeller Academic Edition. This software was chosen over other software packages due to the wide range of features and ability to test varying DDoS scenarios with ease. OPNET Modeller allowed for setup of a comprehensive base scenario which could then be modified in accordance with previously set objectives to see how different scenarios were affected by DDoS when factors such as number of clients and number of affected clients were changed.

The OPNET object palette provides a "Cyber-Effects" node tree which allows the creation of an Attribute Definition package where a DDoS attack and specific phases of a DDoS attack can be mapped out and triggered accordingly. The Attribute Definition within OPNET was used to create a profile to simulate a DDoS attack. This profile consists of two phases labelled "Phase 1" and "Phase 2" respectively. The first phase will trigger [redacted] which will cause the attacking device to infect connected devices over a period of 600 seconds and then confirm this. This phase will always execute upon running the simulation. This phase will be marked as complete if [redacted] is successful. The second phase triggers once the previous phase has been marked as completed. The second phase will flood the IP address 192.102.100.1 with false traffic from the infected nodes causing a severe delay/shutdown.

The two aforementioned phases are made possible via the use of [redacted] within the Attribute Definition. The first [redacted] created for use is [redacted] infect any reachable Cyber Effects device for an unlimited duration. The second [redacted] generates a 12,000 bit packet every 0.01 seconds and floods it towards the 192.102.100.1 IP address. This IP address is the target server which is hosting services for the clients.

As mentioned within the objectives section, three simulations have been created. The first simulation consists of one attacker, ten infected nodes and five Wireless Clients attempting to access HTTP files from a server. The second simulation consists of one attacker, forty infected nodes and fifteen wireless clients. The final simulation consists of fifty infected nodes and fifteen wireless clients. These simulations will be run simultaneously and used to gather data pertaining to the effect of DDoS on the network performance.

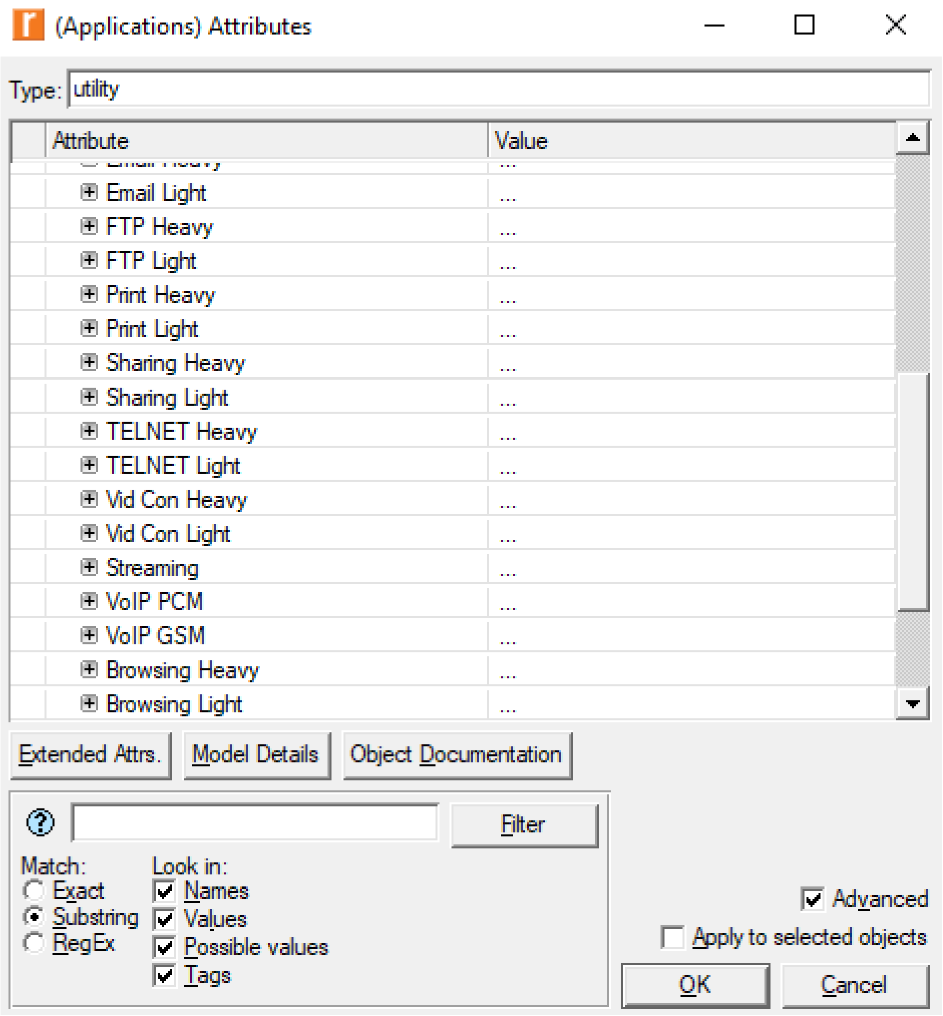
4.1.1 Device Setup and Topology



The above topology is the base topology used for this simulation, consisting of ten Cyber Effects Workstation nodes with an Infection Rate of 100%. These are connected via Ethernet switches and routers to “Node_7” which is the target server. The attacking machine “node_23” is directly connected to a gateway router allowing for access to the server and machines to infect. The application configuration being used is Default and a profile is set up and applied to each of the Wireless Clients allowing them to access HTTP resources on the server with Heavy Load.

This topology is modified a further two times in order to present various scenarios with more infected devices and more clients to see if there is any noticeable change in performance in the network when more clients or infected machines are added. Further topologies will be shown and discussed in a later section.

4.1.2 Application, Profile and Cyber Effects Configurations



(Applications) Attributes

Type: utility

Attribute	Value
⊞ Email Heavy	...
⊞ Email Light	...
⊞ FTP Heavy	...
⊞ FTP Light	...
⊞ Print Heavy	...
⊞ Print Light	...
⊞ Sharing Heavy	...
⊞ Sharing Light	...
⊞ TELNET Heavy	...
⊞ TELNET Light	...
⊞ Vid Con Heavy	...
⊞ Vid Con Light	...
⊞ Streaming	...
⊞ VoIP PCM	...
⊞ VoIP GSM	...
⊞ Browsing Heavy	...
⊞ Browsing Light	...

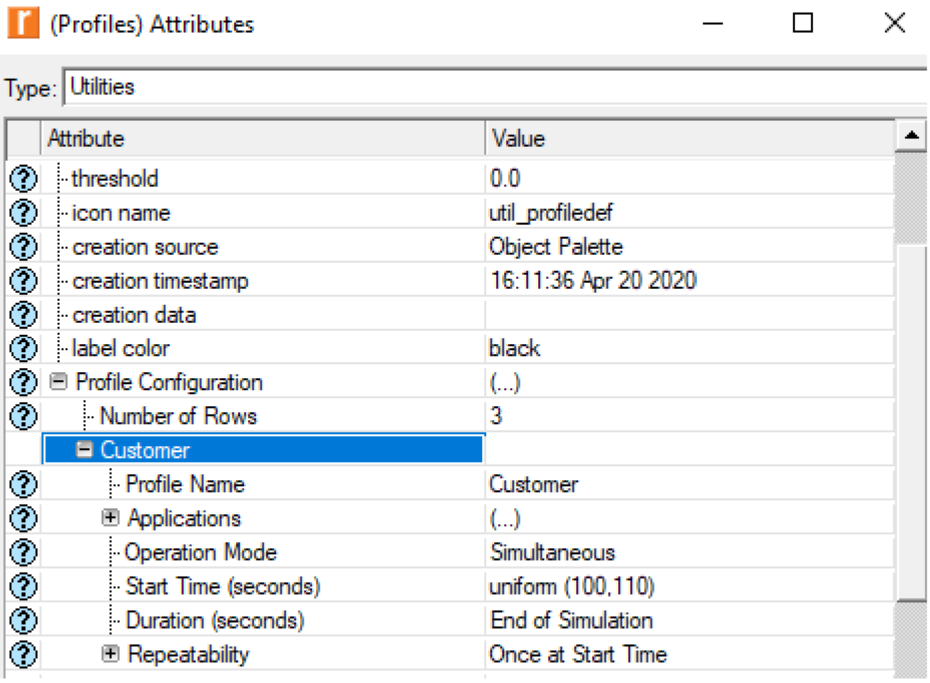
Match: ○ Exact ● Substring ○ RegEx

Look in: ☑ Names ☑ Values ☑ Possible values ☑ Tags

☑ Advanced

□ Apply to selected objects

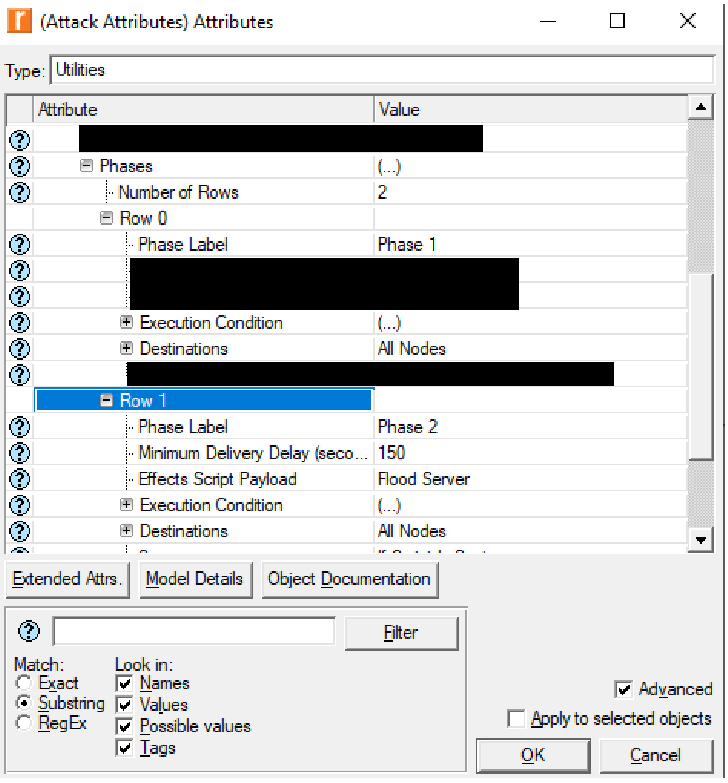
Shown above is the Application Attribute configuration used for each scenario in the project. Attribute configurations are simply set to the OPNET base values with Heavy Browsing and Light Browsing holding the default attribute values and so on. For scenarios in this project the Heavy Browsing application is used primarily.


(Profiles) Attributes

Type: Utilities

Attribute	Value
threshold	0.0
icon name	util_profiledef
creation source	Object Palette
creation timestamp	16:11:36 Apr 20 2020
creation data	
label color	black
⊟ Profile Configuration	(...)
Number of Rows	3
⊟ Customer	
Profile Name	Customer
⊞ Applications	(...)
Operation Mode	Simultaneous
Start Time (seconds)	uniform (100,110)
Duration (seconds)	End of Simulation
⊞ Repeatability	Once at Start Time

Following on from Application configurations the above displays the Profile settings for this project. The Customer profile is applied to each client device in the simulation. This profile triggers each client to send HTTP requests, traffic starts in the simulation between 100 and 110 seconds in and lasts until the end of the simulation. This traffic is sent to the target server which supports the Heavy Browsing application allowing the clients access to that resource. The base topology will be used to acquire normalised running statistics when the network is not under the pressure of a DDoS attack. Following on from this the Cyber Effects application is configured as follows:


(Attack Attributes) Attributes

Type: Utilities

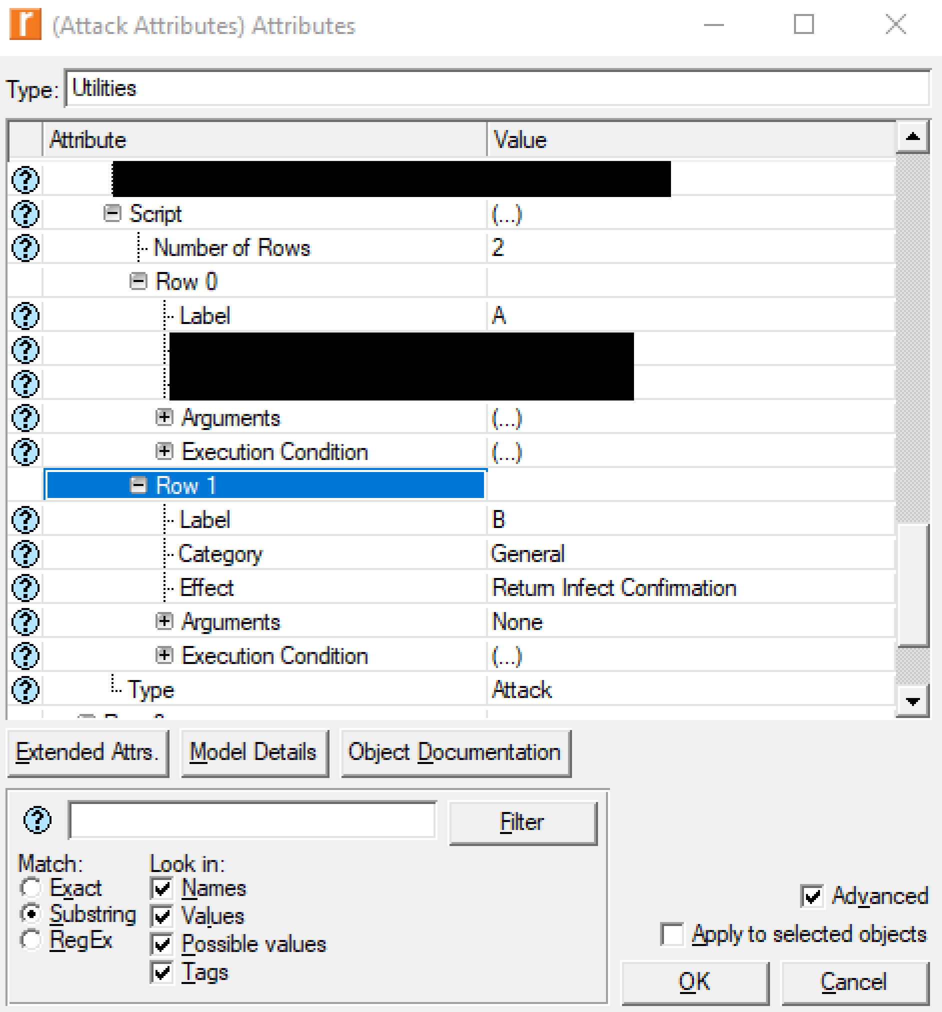
Attribute	Value
[redacted]	
⊟ Phases	(...)
Number of Rows	2
⊟ Row 0	
Phase Label	Phase 1
[redacted]	[redacted]
⊞ Execution Condition	(...)
⊞ Destinations	All Nodes
[redacted]	[redacted]
⊟ Row 1	
Phase Label	Phase 2
Minimum Delivery Delay (seco...	150
Effects Script Payload	Flood Server
⊞ Execution Condition	(...)
⊞ Destinations	All Nodes

Match:
○ Exact
● Substring
○ RegEx

Look in:
☑ Names
☑ Values
☑ Possible values
☑ Tags

☑ Advanced
□ Apply to selected objects

The DDoS attack is configured to execute in two phases. The first phase of attack is instant and triggers the infection of devices the attacker has access to. The devices which are to be infected have an infection rate of 90% in these scenarios, the infection rate is set close to 100% to see the full effect of a DDoS attack on network infrastructure. Once this phase is marked as successful the second phase will trigger. Phase 2 triggers the script created to flood the server with trafic. Once this phase triggers 12,000 bit packets will be sent to the server from clients with a 0.01 interarrival time for a duration of 150 seconds, thus denying access to the server and massively slowing response times. This attack is carried out using [redacted]. The first [redacted] an infite duration as soon as the first phase triggers. The second script is used to flood the server with traffic as discussde previously and triggers upon successful execution of the first phase. The third script is used to confirm the infection of targeted devices.



(Attack Attributes) Attributes

Type: Utilities

Attribute	Value
[redacted]	
⊟ Script	(...)
Number of Rows	2
⊟ Row 0	
Label	A
[redacted]	
⊞ Arguments	(...)
⊞ Execution Condition	(...)
⊟ Row 1	
Label	B
Category	General
Effect	Return Infect Confirmation
⊞ Arguments	None
⊞ Execution Condition	(...)
Type	Attack

Match: ○ Exact ● Substring ○ RegEx

Look in: ☑ Names ☑ Values ☑ Possible values ☑ Tags

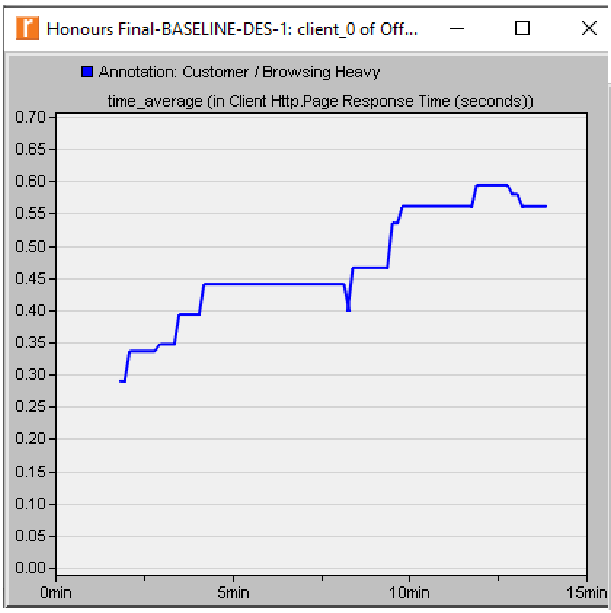
☑ Advanced

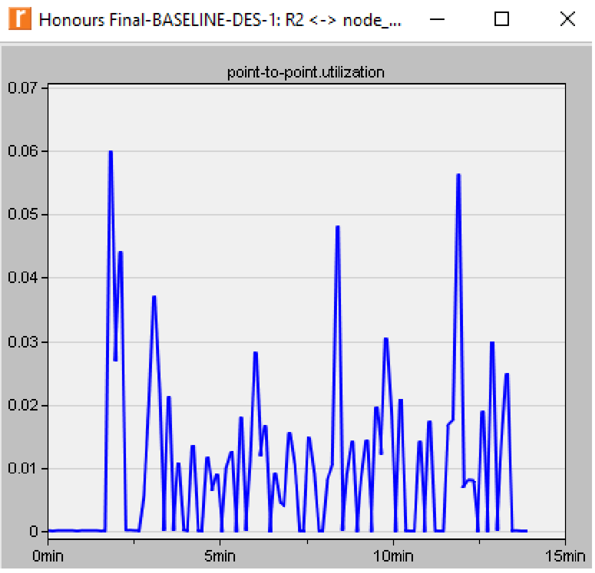
□ Apply to selected objects

The third script is shown above and consists of two parts labelled “A” and “B” respectively. Part “A” infects devices connected whilst part “B” returns confirmation of infection to the attacking machine. This script confirms devices have been infected to ensure that the attack can go ahead successfully in Phase 2.

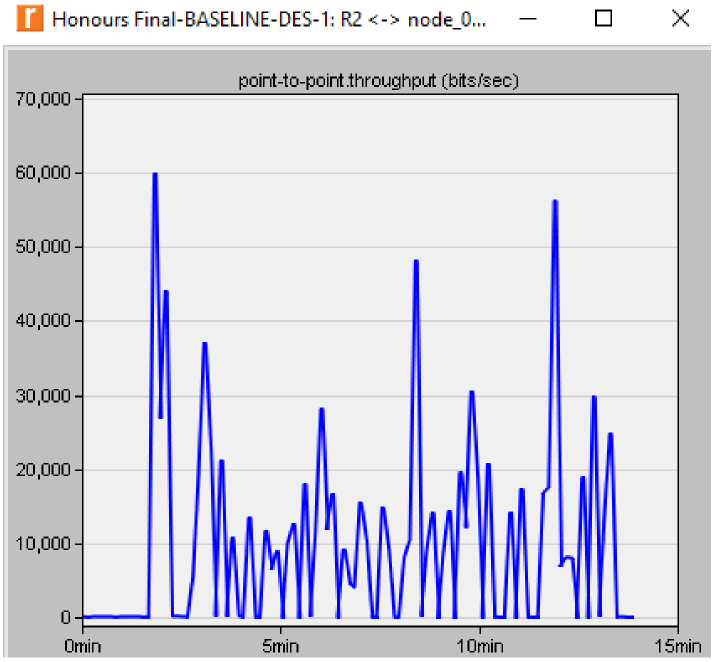
5.0 Evaluation and Discussion

5.1.1 Base Topology Results



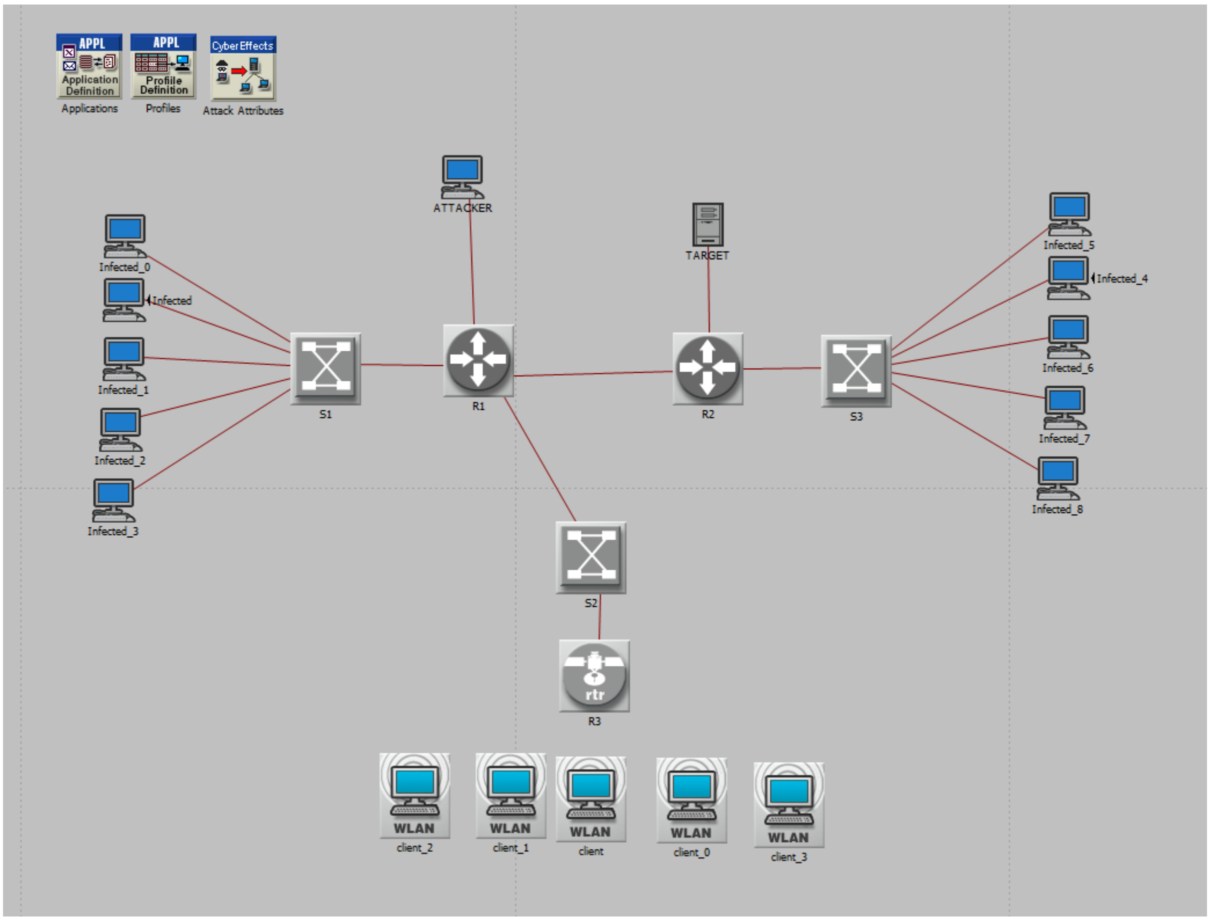


The base simulation scenario was run over a total of 840 seconds to acquire base values for statistics like CPU utilisation, page response time and throughput on the targeted server. The above graphs demonstrate that while under normal operating conditions, the server has a peak CPU utilisation percentage of roughly 0.06% and the client’s response time from the server ranges from 0.30 to 0.60 seconds. Furthermore, the throughput maxes out at sixty thousand bits per second while the network is under no stress.

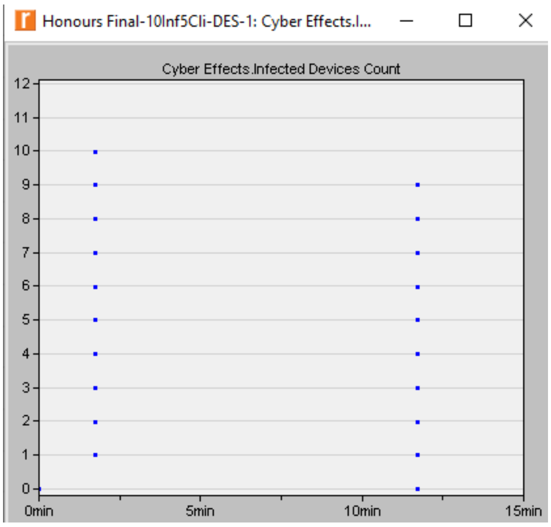


These results will be used in comparison with the upcoming scenarios to determine the detrimental effects of a DDoS attack on the network.

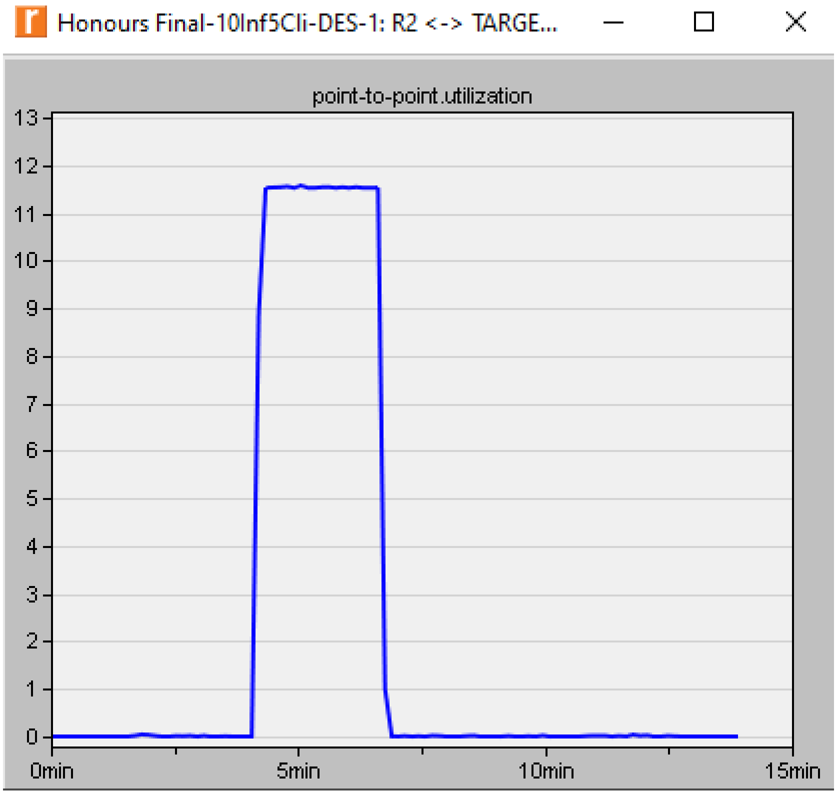
5.1.2 Scenario 1 Results



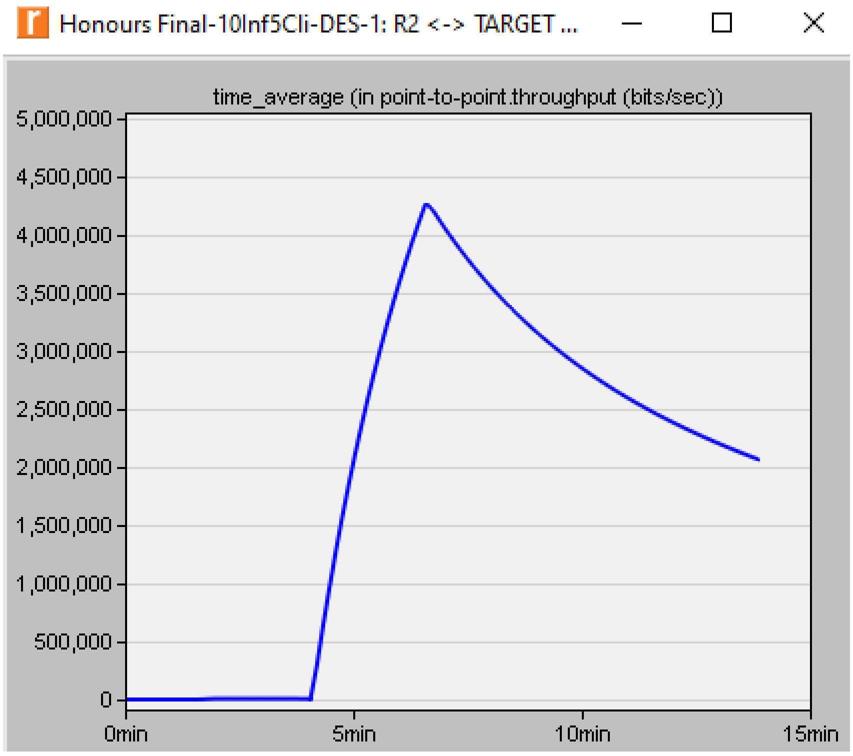
This is the first scenario presented in determining the effects of DDoS on corporate WLAN environments. This scenario incorporates ten infected machines, one attacker and five clients running the Customer profile. In this scenario each infected machine has a 90% infection probability and the target is the server.



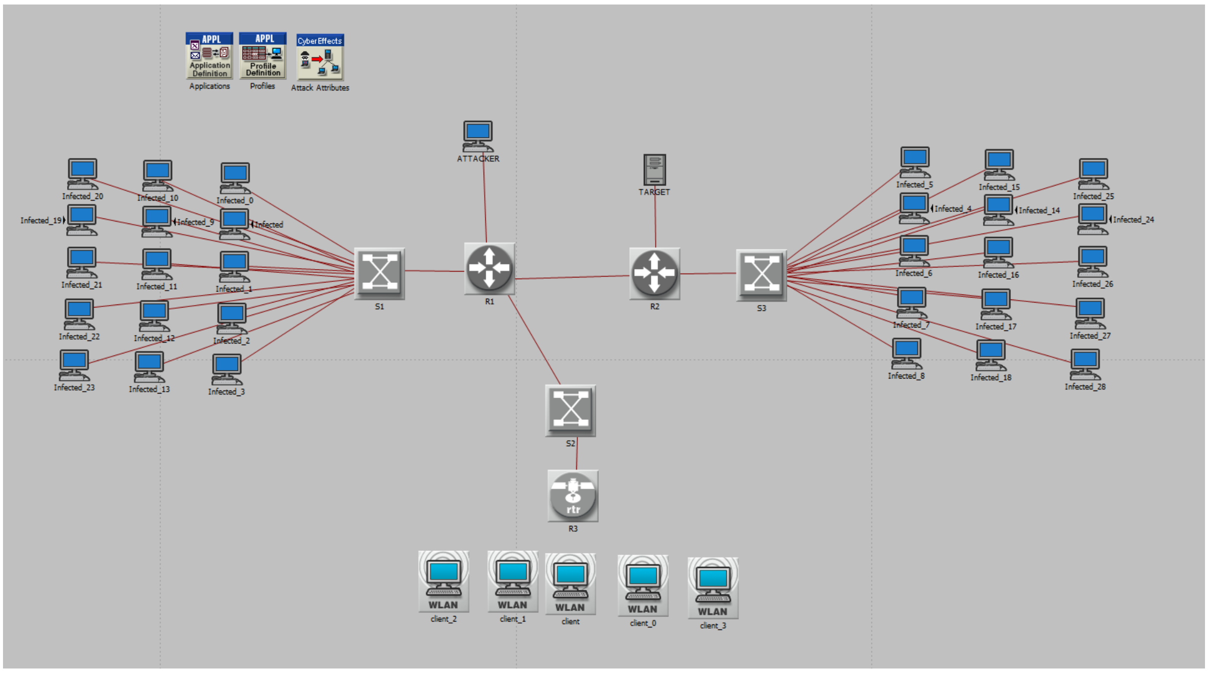
The graph above demonstrates the first notable statistic, number of devices which have been infected. The first spike in this graph shows each of the 10 devices being infected at the start mark of one hundred seconds. The second spike on the graph is the end of the DDoS simulation where the infected devices are released one by one. This graph is solely to demonstrate that in this simulation there are ten infected devices present. The first statistic evaluated in this scenario will be the CPU utilisation percentage which looks as follows.



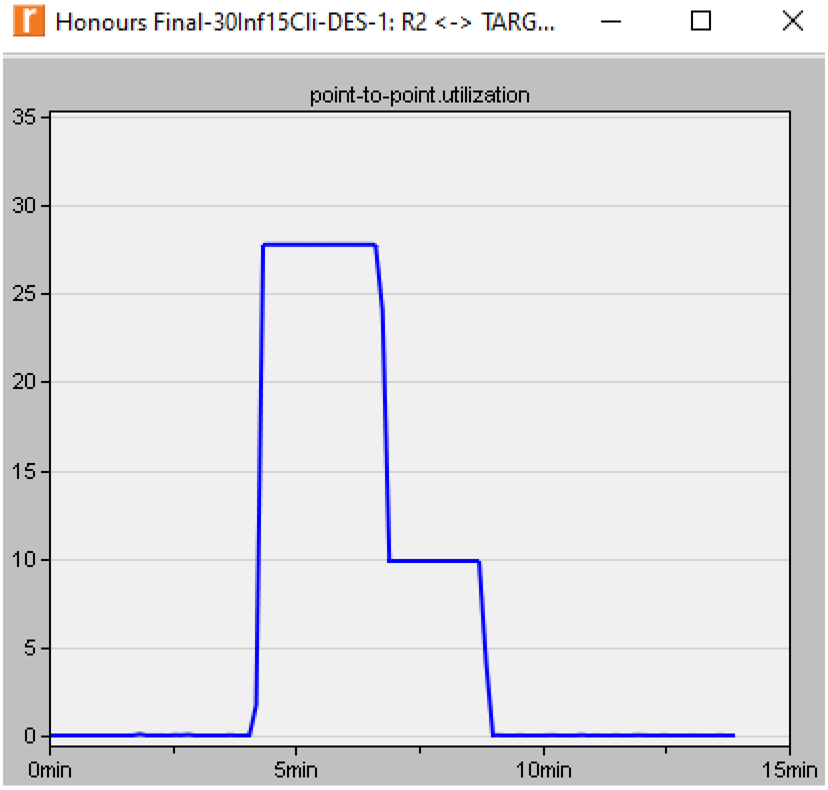
This graph tracks the CPU utilisation percentage between the server and the router. Under the stress of DDoS via ten infected machines in this scenario the CPU utilisation peaks at 11.5% roughly and holds for around five minutes, this is a significant jump in CPU usage as pre-four minutes the CPU usage can be seen to be close to zero before a massive leap to 11% when the DDoS attack commences. A leap in CPU usage like this can significantly slow down a server and consume a lot of resources. Following on from this the throughput of the server can be tracked under the stress of ten infected clients. The graph below shows the server throughput reaching a peak of four and a half million bits per second almost when the DDoS starts, signifying a massive amount of traffic flooding through the server.



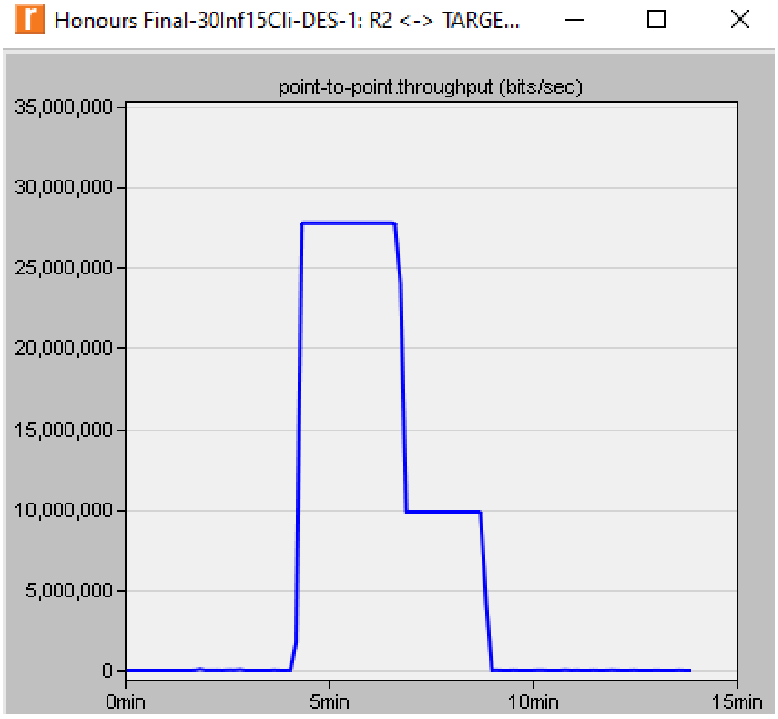
5.1.3 Scenario 2 Results



The above demonstrates the topology used in the second scenario of this simulation, this scenario consists of five clients and thirty infected machines. Once again, the first graph to be inspected here is the CPU utilisation graph which demonstrates a very high CPU usage over a longer period than previously.

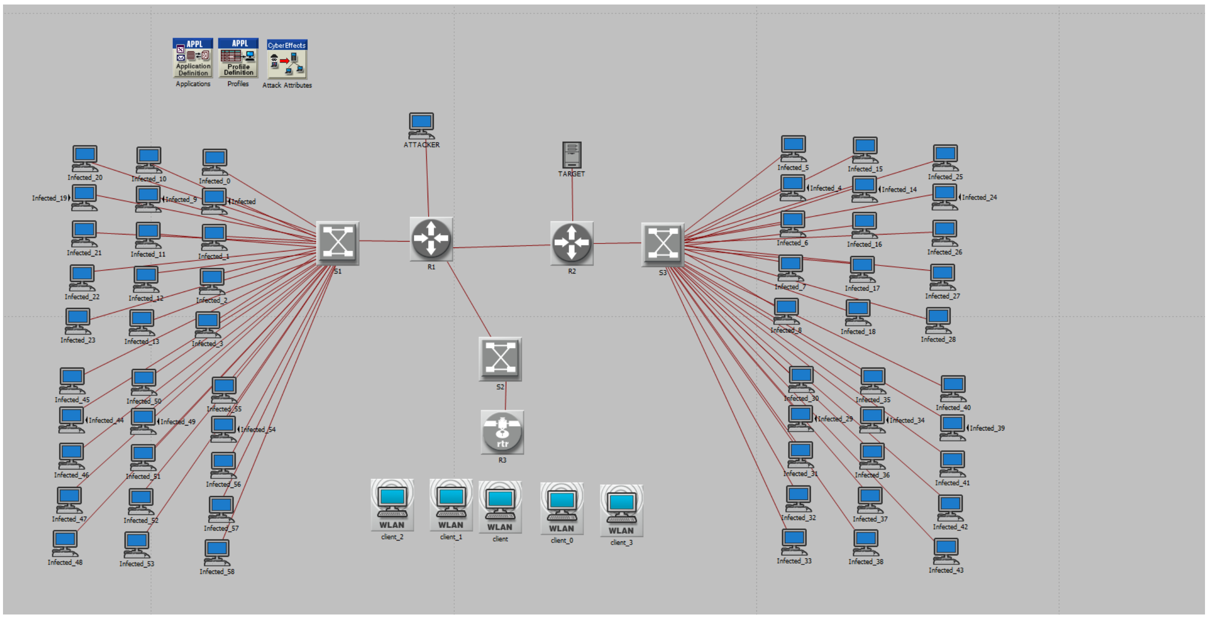


The graph shown displays the CPU utilisation reaching a max of almost thirty percent during the DDoS attack, slowing to ten percent at around halfway into the attack. This CPU load is a massive increase in comparison to the base test which was run previously. A CPU load this high can lead to massive decreases in response times and sever overloads in some occasions. A DDoS attack of this magnitude against such a small number of clients has potential to be completely devastating. Moving on from this to the throughput for the server in this scenario;

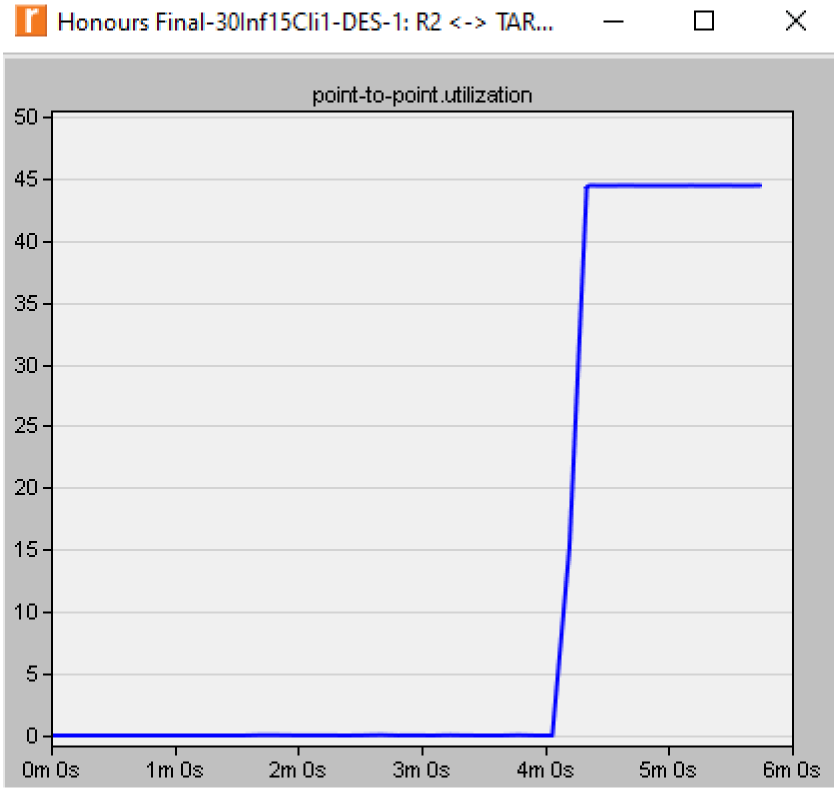


This graph shows the max throughput at close to thirty million bits per second. This shows that a massive amount of traffic is successfully passing through this server and accessing resources, this correlates with the previous CPU utilisation graph which takes the same shape roughly. This shows that the server CPU utilisation spikes out as the most amount of data passes through it, causing it to use a much higher than usual amount of CPU to be able to handle the data which is flowing through it.

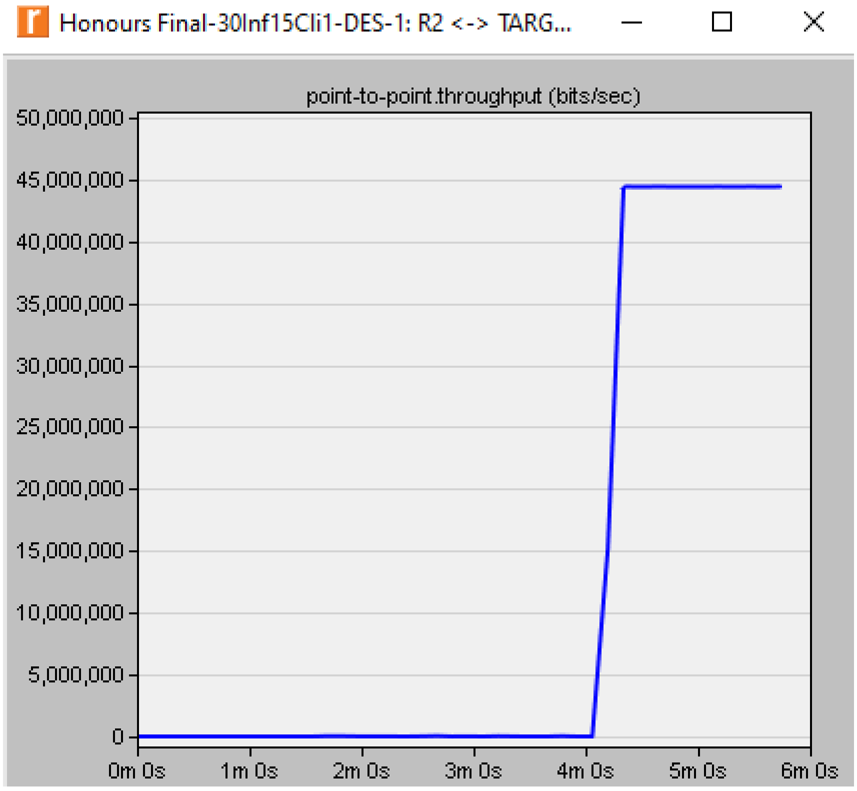
5.1.4 Scenario 3 Results



The third and final scenario used in this simulation involves sixty total infected devices and five client machines. This scenario pressures the network to the extremes. As before, the first graph to be inspected is the CPU usage graph which displays the following:



The server CPU utilisation in this scenario caps out at forty five percent utilisation, more than both previous scenarios due to the massive amount of infected clients sending traffic, the CPU utilisation becomes so high that the server crashes out entirely at six minutes into the simulation, making the network effectively useless. Further reinforcing the effect this amount of infected machines has on a network of this size is the throughput statistics which are as follows:



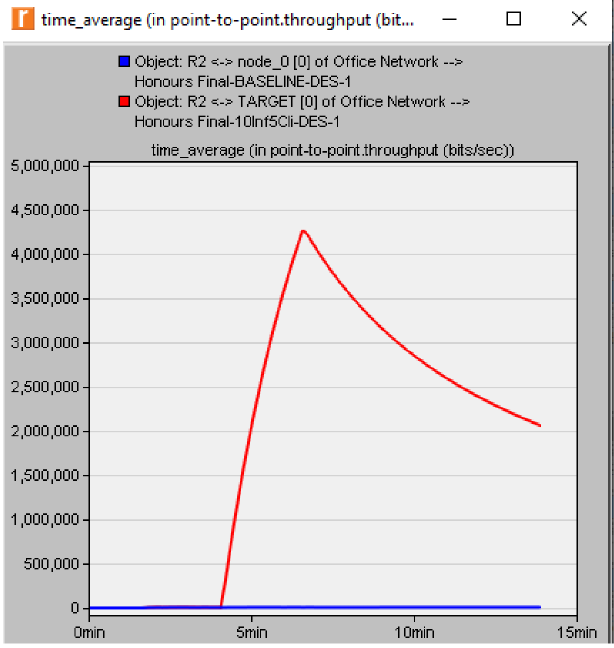
Once again, this graph lines up nicely with the CPU utilisation graph, showing that as utilisation caps out and the server crashes, throughput reaches a max of forty-five million bits per second. This huge amount of traffic flowing through the server causes CPU usage to almost reach fifty percent and slows down response times and server function massively.

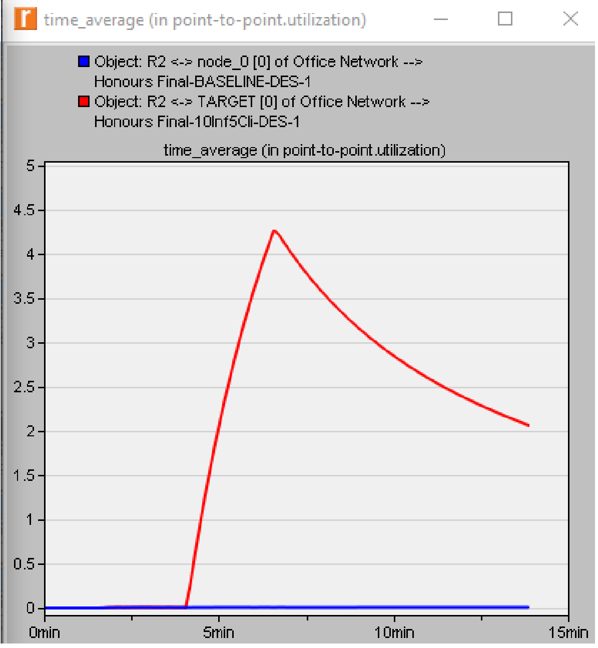
5.1.5 Ethical and Professional Issues

As this project was carried out using a simulation package and completed without the involvement of others there are few ethical issues involved. The nature of this project pertains to Distributed Denial of Service and how it is carried out. Outside of a simulated environment DDoS flooding is illegal. Using knowledge attained throughout this project for malicious purposes falls under the Computer Misuse Act. The knowledge gained throughout the duration of this project has been used purely for educational purposes and should not be taken outwith a simulated environment under any circumstance. Software used throughout this project was obtained under an educational license. In the context of this project, the use of DDoS outside the realm of simulation can cause significant harm to a company or individual and therefore should be strictly restricted to simulated environments, it is for this reason that simulation was chosen to conduct this project.

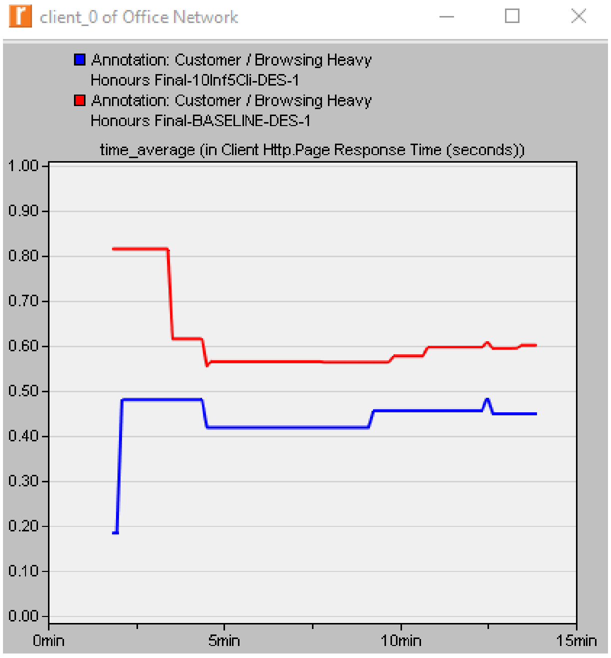
5.2 Comparisons Between Scenarios and Base Topology

5.2.1 Scenario 1 vs Base





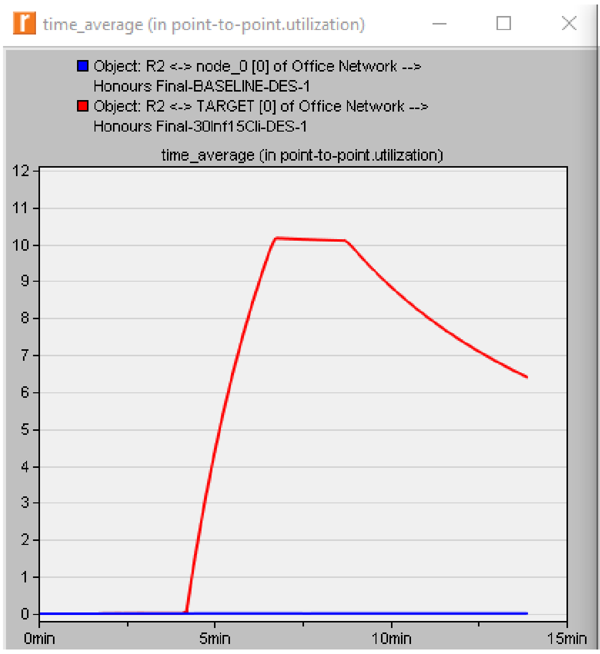
The above graphs demonstrate a direct comparison between the first DDoS scenario and the Base topology constructed. The blue line represents the base topology and the red line represents the DDoS scenario. The graph on the left shows the massive leap in throughput bits per second in relation to the base topology. The graph on the right shows the leap in CPU utilisation during the DDoS attack compared to the base topology. The leap in throughput traffic indicates that the second phase of the attack has executed, and the infected devices have begun flooding traffic. The peaks occur at the same point in time as when the server is flooded, both the number of packets flowing through it and the CPU utilisation percentages spike.

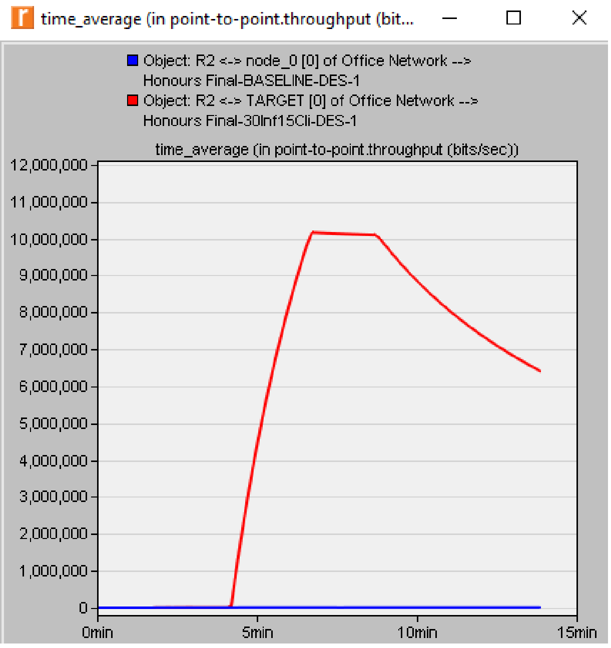


This graph displays the difference in response times for this scenario. The difference is notable; however, it is not an extreme difference, differing from the base topology by around 0.10

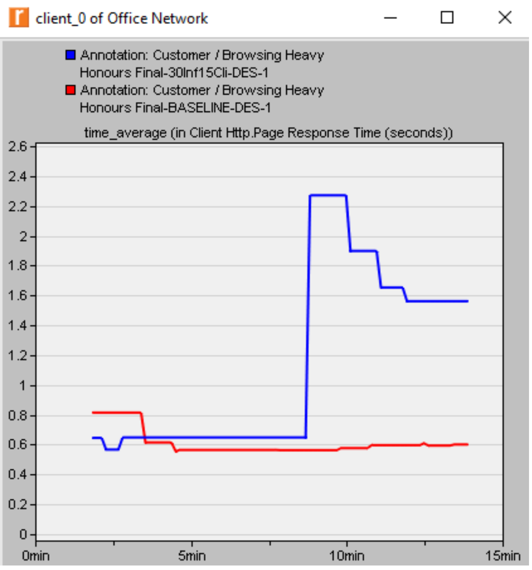
seconds. This scenario would likely not have an extremely detrimental effect on the network due to the small number of attackers and the size of the network.

5.2.2 Scenario 2 vs Base


time_average (in point-to-point.utilization)
🟦 Object: R2 <-> node_0 [0] of Office Network --> Honours Final-BASELINE-DES-1
🟥 Object: R2 <-> TARGET [0] of Office Network --> Honours Final-30Inf15Cli-DES-1
time_average (in point-to-point.utilization)
12
11
10
9
8
7
6
5
4
3
2
1
0
0min
5min
10min
15min

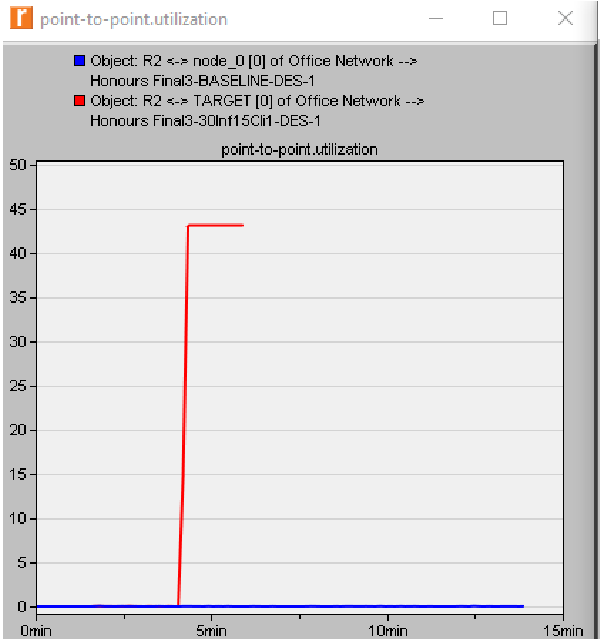

time_average (in point-to-point.throughput (bit...
🟦 Object: R2 <-> node_0 [0] of Office Network --> Honours Final-BASELINE-DES-1
🟥 Object: R2 <-> TARGET [0] of Office Network --> Honours Final-30Inf15Cli-DES-1
time_average (in point-to-point.throughput (bits/sec))
12,000,000
11,000,000
10,000,000
9,000,000
8,000,000
7,000,000
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
0min
5min
10min
15min

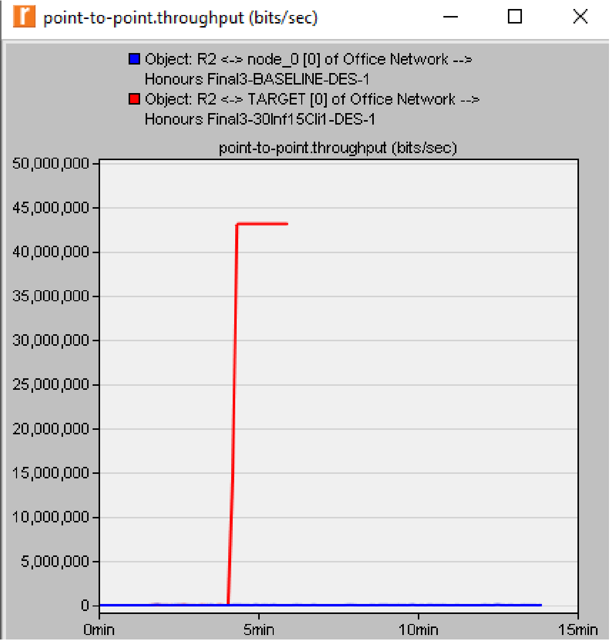
This scenario adopts a much larger number of attackers, thirty. Under the stress of thirty attackers the differences are immediately noticeable. CPU utilisation begins to skyrocket at five minutes and never comes back down to its base value. In this scenario the CPU utilisation peaks at double what it reached in the first scenario. Ten percent CPU utilisation compared to a normal level of less than one percent has a noticeably detrimental effect on the network response time and the server performance. Again, the peaks look similar as alongside the CPU utilisation spiking, the throughput maxes out at ten million bits per second showing where the second phase of the attack begins.


client_0 of Office Network
🟦 Annotation: Customer / Browsing Heavy Honours Final-30Inf15Cli-DES-1
🟥 Annotation: Customer / Browsing Heavy Honours Final-BASELINE-DES-1
time_average (in Client Http.Page Response Time (seconds))
2.6
2.4
2.2
2
1.8
1.6
1.4
1.2
1
0.8
0.6
0.4
0.2
0
0min
5min
10min
15min

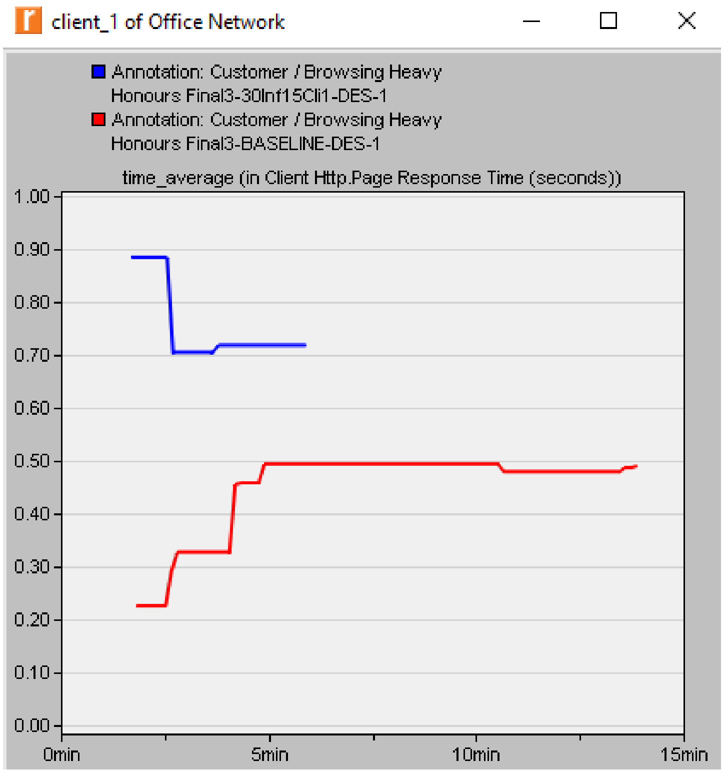
This graph compares the client page response time between the base scenario and the DDoS scenario. This time the differences in response times are significant. Once the server has been overloaded with traffic from the infected clients the response time spikes to over two seconds up from the base level of under one. This spike in response time can be detrimental to corporations running their services from online, delayed response times like this can easily turn away potential customers. The average response time does improve slightly over time as the effects of the attack wear off, but it still levels out at around one and a half seconds, over a second longer than the response time when under no stress.

5.2.3 Scenario 3 vs Base





In this final scenario there are a maximum of sixty infected machines flooding the server simultaneously. The massive amount of traffic this generates is demonstrated on the right-hand side graph which shows the throughput to peak out at forty-two million bits per second. This is the largest amount of traffic generated across all the simulated scenarios and causes the server to stop responding entirely. On the left the CPU percentage utilisation can be seen which caps out just below forty-five percent. Compared to the base scenario which has around one percent utilisation this is an absolutely massive amount of CPU utilisation and causes definite issues for the network including the server becoming unresponsive.



The final graph to be analysed here shows the response time from the server in blue under the stress of DDoS and in red at a base level. The response time from the server completely vanishes as the second phase of the attack executes as this causes the server to fail. For clients, this means they are no longer able to access any web resources which they would otherwise have had access to. This is especially crippling for corporate environments due to the potential downtime caused. The results of these effects across scenarios will be discussed further in conclusions.

6.0 Conclusions

6.1.1 Scenario 1 and Effects

The first scenario consisted simply of ten infected machines flooding a server hosting five clients. The clients were accessing a web resource made available by a corporation which could be collecting information, selling services/products online etc. When the DDoS takes effect the server response time spikes from a roughly 0.40 second average to a 0.55 second average. In this case the difference in response times will not particularly be noticeable for customers attempting to access any web resources therefore in terms of response time there is no noticeable affect or detriment in this scenario in terms of response time. CPU utilisation in this scenario peaks from around one percent to up to four and a half percent, whilst this is a significant spike considering the base average is around one percent, it is not enough of a leap to cause harm to the network as a whole. This leap in utilisation will likely be noticed by anyone monitoring the network but is not significant enough to cause any serious harm or delays in the network. Finally, throughput climbs to around four million bits per second from the base level of sixty thousand bits per second. This influx of traffic will definitely be noticed by those monitoring the network and will likely provide enough warning to nullify the minor effects of the attack. Overall, this scenario has no severe effects on the network as a whole and presents little to no threats.

6.1.2 Scenario 2 and Effects

The second scenario takes a significant leap in infected machines, utilising thirty devices flooding a server hosting five clients. In this scenario, when the second phase of the attack is executed the server response time peaks at roughly 2.3 seconds. In comparison, the base level for this scenario is around 0.6 seconds. This leap in response time will definitely be noticeable by clients using web resources provided by the corporation. Delays in web loading times can deter clients looking to make use of a company's resources, in modern times speed is vital to most operations and customers will gravitate towards the fastest, most efficient service. Corporations who prove vulnerable to DDoS attacks such as this will suffer in response times across the network. High response times result in lost customers, lost time, and therefore lost money. Furthermore, this scenario doubles the CPU utilisation percentage from the last, peaking at ten percent. This is a significant increase from the usual (roughly one percent), this increase in CPU load is part of the reason for the delay in response times and can cause issues for the server itself. As the throughput increases, so does the amount of CPU required to handle the traffic. CPU utilisation in this scenario never falls below five percent once the attack commences. Again, the traffic can be seen in the throughput which reaches over ten million bits per second under the stress of this attack. Overall, this attack would definitely be detrimental to a corporate network. Delay in response time and peaks in CPU utilisation would cause issues with customers being unable to access network resources and with the server being potentially incapable of keeping up with incoming requests from the massive influx of traffic. If this attack were to last longer than the allocated simulation time for this project it would likely have a devastating effect on the reputation and cashflow of a given corporation.

6.1.3 Scenario 3 and Effects

This scenario simulates sixty total infected devices flooding a single server hosting five clients. In this final scenario, the second phase of the attack executes, and the server immediately spikes to a massive forty-five percent CPU utilisation, at this point the server becomes fully unresponsive and the simulation ends. As the server reaches this utilisation peak the throughput maxes out at forty-five million bits per second travelling through the server. This percentage of CPU utilisation for a server can be catastrophic, especially if the environment in which it is housed is not correctly established. Small companies may not have correctly configured or constructed server rooms and the temperatures at which a server running at this percentage of CPU use would operate could cause physical damage. Besides this, the server becoming completely unresponsive for a duration can absolutely wreck a business, without an operational server the company will be unable to host web resources or provide any explanation to customers as to why their services have failed. The amount of downtime caused by this can cause a company to lose a significant amount of income and can also drive customers away if they know a company is vulnerable. Server response times in this scenario level out at 0.70 seconds for the second phase of the attack before vanishing entirely when the server goes down. Depending on the context of the hosted service this can cause any number of issues such as cancelled transactions, lost work, lost information etc.

6.1.4 Final Conclusions

Based on the three scenarios presented, it is apparent that DDoS traffic flooding is an effective way at crippling a wireless corporate environment. The hypotheses presented previously in this project proved to be partially correct. Whilst all attacks did present an output which showed to have some effect on network performance, the first scenario had no particular detrimental effect on the network. This scenario presented negligible effects on response time and CPU utilisation. DDoS floods are, of course, less than ideal but in the first scenario presented there were no meaningful issues caused by the attack occurring. In this case, mitigating the attack would be as simple as ignoring it due to the short duration (fifteen minutes) being simulated here. However, were the attack to last longer the effects would potentially become more severe over time and this is an issue which would be interesting to investigate at a later date. The second scenario performed as expected, putting pressure on the network with a high infected:healthy ratio had a significant and noticeable impact on response times from the server. This scenario presented a meaningful increase in response time delay as well as CPU percentage utilisation. Response times were delayed up to two seconds and utilisation reached ten percent. Delays this long in the modern era can push away potential customers, not only this but if customers become aware than a corporation is vulnerable to cyber attacks like DDoS it is highly likely that they will lose interest. Finally, the third scenario presented sixty infected machines and caused the server to crash fully, which was a greater detrimental effect than expected when hypothesising. The server losing full functionality after reaching a peak of forty-five percent presents major issues for the corporation hosting services or selling products online. The server losing full functionality poses serious issues for any corporation. Customers losing access to the server and hosted web resources can mean loss of vital data, errors with transactions or simply inability to access a desired web page.

Overall, the impact DDoS has on corporate environments is major. Regardless of the effect on performance metrics, a company being afflicted by a DDoS attack immediately is at risk of losing reputation, income, and loyal customers. Customers and clients who become aware that a corporation they previously trusted has been made vulnerable via DDoS are likely to abandon said organisation, particularly if they were entrusting sensitive information to said organisation. Furthermore, as mentioned previously, these attacks have the potential to be screens for other, more malicious attacks. The potential DDoS has to open up a network to more dangerous attacks is boundless and the effect it can have on a company in terms of reputation can be devastating. In terms of performance metrics, the first attack proved rather negligible but the second and third scenario attacks caused serious issues within the small network which was created. Either of these scenario attacks, if carried out for long periods, could cause massive disruption, and provide easy cover for other attackers. Even if the attacks are not screening the effect, they have on response time and CPU load alone is enough to cause any corporate network serious issues. This project had the goal of identifying the effect DDoS has on corporate WLAN networks via the use of the OPNET simulation package and succeeded in identifying the effect of DDoS using performance metrics obtained from scenarios constructed within the OPNET simulation package designed for this purpose.

7.0 Further Work

This project concluded as expected, proving that DDoS flooding has the potential to have devastating effects on corporate WLAN environments, particularly when the ratio of infected:healthy devices is skewed heavily in the favour of infected. There were, however, limitations in carrying out this project. Primarily, the timescale of the project meant that a greater scope could not be fully explored. In a future scenario with more time available, it would be ideal to explore the full effect of DDoS floods on significantly larger networks and have the simulations carried out over much larger time periods than fifteen minutes. Further work could be carried out continuing to use OPNET simulation package but constructing larger, more complex environments. These environments could then be placed under the stress of DDoS floods and more variables could be tested. Variables that could be tested in future scenarios include number of clients, number of attacking machines, number of servers hosting services, the type of service being hosted. The testing of these variables would allow for a more comprehensive conclusion when it comes to the impact DDoS has. Furthermore, future work could encompass the mitigation and prevention of attacks. [redacted]. Understanding the effect of each type of attack on various networks would allow for a deeper understanding of how to prevent each attack and therefore allow the mitigation and prevention responses to be tested within OPNET as well as the attack mechanisms.

References

[1] I. A. Shourbaji, “An Overview of Wireless Local Area Networks (WLAN),” *International Journal of Computer Science and Information Security,* vol. 11, no. 2, p. 46, 2013.

[2] H. Saini, K. D. Sharma, P. Dadheech and T. C. Panda, “Enhanced 4-way Handshake Process in IEEE802.11i with Cookies,” *International Journal of Information and Network Security,* vol. 2, no. 3, pp. 229-234, 2013.

[3] P. H. Latha and R. Vasantha, “SAKGP: Secure Authentication Key Generation Protocol in WLAN,” *International Journal of Computer Applications,* vol. 96, no. 7, pp. 25-33, 2014.

[4] V. Visoottiviseth, A. Trunganont and S. Siwamogsatham, “Cross-layer based adaptive wireless traffic control for per-flow and per-station fairness,” *EURASIP Journal on Wireless Communications and Networking,* vol. 2011, no. 97, pp. 1-26, 2011.

[5] J. Thomas, “purple,” 27 May 2014. [Online]. Available: https://purple.ai/blogs/history-wifi/. [Accessed 9 April 2019].

[6] J. S. Park and D. Dicoi, “WLAN Security: Current and Future,” *IEEE Internet Computing,* vol. 7, no. 5, pp. 60-65, 2003.

[7] K. J. Negus and A. Petrick, “History of Wireless Local Area Networks (WLANs) in the Unlicensed Bands,” *Info: The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media,* vol. 11, no. 5, pp. 36-56, 2009.

[8] G. Badishi, A. Herzberg and I. Keidar, “Keeping Denial-of-Service Attackers in the Dark,” *IEEE Transactions on Dependable and Secure Computing,* vol. 4, no. 3, pp. 191-199, 2007.

[9] R. J. Gordon, “DDoS Attack Simulation to Validate the Effectiveness of Common and Emerging Threats,” *Journal of Information Warfare,* vol. 16, no. 1, pp. 49-63, 2017.

[10] N. A. Suryawanshi and S. R. Todmal, “DDoS Attacks Detection of Application Layer for Web Services using Information based Metrics,” *International Journal of Computer Applications,* vol. 117, no. 9, pp. 22-30, 2015.

[11] M. Bogdanoski and A. Risteski, “Wireless Network Behavior Under ICMP Ping Flood DoS Attack and Mitigation Techniques,” *International Journal of Communication Networks and Information Security,* vol. 3, no. 1, pp. 17-24, 2011.

[12] X. Geng, Y. Huang and A. B. Whinston, “Defending Wireless Infrastructure Against the Challenge of DDoS Attacks,” *Mobile Networks and Applications,* vol. 7, no. 3, pp. 213-223, 2002.

[13] O. K. Enigbokan and N. Ajayi, “Managing Cybercrimes Through the Implementation of Security Measures,” *Journal of Information Warfare,* vol. 16, no. 1, pp. 112-129, 2017.

[14] M. Bogdanoski, T. Shuminoski and A. Risteski, “Analysis of the SYN Flood DoS Attack,” *International Journal of Computer Network and Information Security,* vol. 5, no. 8, pp. 1-11, 2013.

[15] D. Mahajan and M. Sachdeva, “DDoS Attack Prevention and Mitigation Techniques - A Review,” *International Journal of Education and Computer Science,* vol. 67, no. 19, pp. 65-71, 2014.

[16] S. Swetapadma and M. Pandey, “Distributed Denial of Service Attacks: A Review,” *International Journal of Modern Education and Computer Science,* vol. 6, no. 1, pp. 65-71, 2014.

[17] N. Hoque, D. K. Bhattacharyya and J. K. Kalita, “Botnet in DDoS Attacks: Trends and Challenges,” *IEEE Communications Surveys & Tutorials,* vol. 17, no. 4, pp. 2242-2270, 2015.

[18] J. Kim and S. J. Shin, “Design and Implementation of DDoS Testbed Using Virtual Botnets,” *International Information Institute (Tokyo),* vol. 19, no. 5, pp. 1517-1524, 2016.

[19] E. Alomari, S. Vlanickam, B. B. Gupta and R. Alfaris, “Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art,” *International Journal of Computer Applications,* vol. 49, no. 7, pp. 24-32, 2012.

[20] V. Mosorov, A. Kosowski, R. Kolodiy and Z. Kharkhalis, “Data Traffic Modeling During Global Cyberattacks,” *International Journal of Computer Network and Information Security,* vol. 7, no. 11, pp. 20-36, 2015.

[21] K. Saravanan, R. Asokan and K. Venkatachalam, “Neuro- Fuzzy Based Clustering of Distributed Denial of Service (DDoS) Attack Detection Mechanism,” *International Information Institute (Tokyo),* vol. 16, no. 11, pp. 8137-8144, 2013.

[22] M. Malekzadeh, A. Moghis and A. Shahrokh, “Amplification-based Attack Models for Discontinuance of Conventional Network Transmissions,” *International Journal of Information Engineering and Electronic Business,* vol. 7, no. 6, pp. 15-22, 2015.

[23] A. Bonguet and B. Bellaiche, “A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing,” *Future Internet,* vol. 9, no. 3, pp. 5-6, 2017.

[24] T. Mahjabin, Y. Xiao, G. Sun and W. Jiang, “A survey of distributed denial-of-service attack, prevention and mitigation techniques,” *International Journal of Distributed Sensor Networks,* vol. 13, no. 12, pp. 2-33, 2017.

[25] J. Mirkovic and P. Reiher, “A Taxonomy of DDoS Attack and DDoS Defence Mechanisms,” *ACM SIGCOMM Comp Com,* vol. 34, no. 2, pp. 39-53, 2004.

[26] S. H. Sellke, N. B. Shroff and S. Bagchi, “Modeling and Automated Containment of Worms,” *IEEE Transactions on Dependable and Secure Computing,* vol. 5, no. 2, pp. 71-80, 2008.

[27] J. Xu and L. Wooyong, “Sustaining Availability of Web Services under Distributed Denial of Service Attacks,” *IEEE Transactions On Computers,* vol. 52, no. 2, pp. 195-208, 2003.

[28] L. Garber, “Denial-of-service attacks rip the internet,” *Institute of Electrical and Electronics Engineers,* vol. 33, no. 4, pp. 12-17, 2000.

[29] A. Keumars, *AWS servers hit by sustained DDoS attack,* London: IT Pro, 2019.

[30] PCQuest, Worse Than it Seems: DDoS Attacks Often Coincide with Other Threats, Gurgaon: Athena Information Solutions Pvt. Ltd., 2015.

[31] Dataquest, Stay Ahead of Emerging Threats, Gurgaon: Athena Information Solutions Pvt. Ltd., 2017.

[32] B. Sivasubramanian, E. Frahim and R. Froom, “PPDIOO Lifecycle Approach to Network Design and Implementation,” in *Analysing the Cisco Enterprise Campus Architecture*, Cisco Press, 2010.

[33] U. Breskvar and M. Kjajic, “How to Perform a Simulation Project - An Example of Scheduling with Genetic Algorithms and Visual Event Simulation Model,” *Scientific Papers,* vol. 38, no. 9, pp. 499-507, 2005.