National College of Ireland

Securing Home Automation against distributed denial of service attack

MSc Internship
Cybersecurity

Anurag Nitin Mhatre
Student ID: x19236042

School of Computing
National College of Ireland

Supervisor: Dr. Vanessa Ayala-Rivera

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Anurag Nitin Mhatre

Student ID: X19236042

Programme: Research in computing **Year:** 2021

Module: Internship

Supervisor: Vanessa Ayala-Rivera

Submission Due Date: …16/12/2021…….

Project Title: Securing Home Automation against distributed denial of service attack……

Word Count: ……4773…… **Page Count**……23……..…

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……Anurag Mhatre……

Date: ……15/12/21……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Securing Home Automation against distributed denial of service attack

Anurag Nitin Mhatre
X19236042

Abstract

As information technologies advance at a rapid pace, the possibility of an attack keeps growing. One of the most complicated security problems to fix is distributed denial of service (DDoS). While many existing techniques focus on DDOS attacks and their countermeasures, the most crucial component in securing home automation. Because smart home IoT devices are linked with hardware and software, IoT devices must be secured to work effectively. If an attacker gains access to a device, it can simply usurp the device's functioning and steal the information of the users. In this work, we attempt to resolve the Distributed Denial of Service (DDoS) problem against home routers and secure home IoT devices. Securing the network's main entry point (router) can reduce the number of cyberattacks. We have implemented Virtual Router Redundancy Protocol Techniques and a virtual load balancer in our approach, which can be an efficient and effective way to ameliorate DDoS attacks. As a result, the experimental setup was evaluated by implementing a Cisco packet tracer simulator, and the results show how the network's main access point (router) can be accessible. In the case of a failure, these two distinct techniques can conveniently mitigate DDoS traffic without interfering with precise traffic or causing widespread disruption to home automation.

1 Introduction

The Internet of Things (IoT) has become a slashing technology as well as an intriguing area of great interest to researchers and businesses. These IoT devices involve device connectivity as well as device ability to connect to humans. Smart home automation is important because it improves efficiency, dependability, and a secure environment. (*National Institute of Standards and Technology | NIST, 2021)* Since this device is connected to the Internet through local Wi-Fi networks, it is exposed to cyberattacks. During this epidemic, securing home automation is a major issue. The vulnerabilities are intensified by a one-of-a-kind situation in which humans utilize computer systems and other multiple devices from their home.

Every day, DoS and DDoS attacks pose a serious problem throughout the world, causing a disruption of systems and devices, resulting in a loss of availability and financial loss in business. In a distributed denial-of-service attack, the attacker floods the susceptible target with a huge number of data packets (requests) to deplete resources (whether processing or communication assets) in a short period of time, preventing authorized users from accessing it. *(Shetty, S. and Nagesh, H.R., 2014*)

Eventually, due to the pervasiveness of this type of attack, numerous detection, and prevention methods for countering these types of attacks were proposed. As a result, the question that arises here is how can home automation be secured against DDoS attacks using a load balancer and Virtual router redundancy Protocol methodology? To address this type of issue in smart homes for securing IoT devices and personal data, the operating principle of virtual redundancy protocol, as well as its technical details, have been proposed. The VRRP protocol is implemented because it ensures the sustainability of LAN host public network access. The VRRP protocol can be used in the smart home as it can change the route to another route and maintain the connectivity of the user to the internet even in case of any cyber-attack. (*Geng, Q., and Huang, X., 2018*)

This protocol employs a mechanism that combines several routers into a single virtualized router, with its own IP address. In the incidence of a DDoS attack on the main router, requests from other devices are sent to the virtual router IP. This virtual router is known as the Master router because it manages traffic aimed at certain addresses and intelligently redirects it. The master router additionally advertises to the backup router on a constant schedule. If the main router fails in any way, the backup router will no longer get any advertisements. Later, the backup router takes over as the master router and initiates operations.

As this protocol provides a great availability of network resources 24/7, implementation of this protocol can be the best use for smart home routers. The load balancer is the new router-based technique that should be implemented on the home router. Humans are adopting the work-from-home concept, and to work with full network connectivity, a virtual load balancing router should be implemented in the smart home, which can also be used in the case of a DDOS attack on a router. This paper aims to provide a detailed understanding of how intruders can target home automation and how the main entry point (router) of smart devices can be secured utilizing these two strategies. Through simulation software cisco packet tracer, a smart house with a virtual router redundancy protocol and a load balancer protocol implemented.

2 Related Work

In previous years, computer networks have played a key role in different applications, with computer networks now providing a much more crucial function. On the one hand, the network system's efficiency is unquestionable; on either hand, centralized network dependability is becoming highly relevant. A primary requirement of LAN users is to communicate with the external public network in a reliable. Kavallieratos et al., 2019 report shows the potential deployment of IoT devices which might expand attack surfaces as we advance farther in computer networks where smart IoT devices are connected.

The study in this article enables the detection of DDoS attacks on home automation. Karthikeyan, B., 2014 has disseminated a marking technique on TTL (Time-to-Live) value and MAC value inspection in this study article. This distributed denial of service of attack can be countered by compromised computers detecting the faked network packet. And the cola soft packet builder and snort intrusion detection program identify this faked packet by utilizing its TTL value. Using the ARP watch tool and the Snort Intrusion Detection tool, this tool determines the unique MAC address and IP address. Burhan, Rehman, Khan, and Kim, 2018 have demonstrated the importance of security for IoT devices in smart homes, hospitals, buildings, transportation, and cities in this study. Burhan, Rehman, Khan, and Kim, 2018 have explained in this study how the significant use of IoT devices has risen, but it has left an attacker a backdoor to break into smart homes and other facilities that are connected to it. Researchers give a brief overview of IoT (Internet of Things) layered architectures and security from the standpoint of several IoT layers.

In a past study, Chen, E.Y. and Yonezawa, A., 2005 demonstrated how IoT devices are vulnerable; in this article, the researcher demonstrated how a distributed denial-of-service attack is serious. Chen, E.Y. and Yonezawa, A., 2005 demonstrated several ways for protecting against DDoS attacks. For mitigating DDoS attacks, researchers have divided these approaches into detection, segregation, and mitigation. Because this DDoS attack can be carried out by an attacker Because there are so many users connected to the network in a smart home, high availability and dependability must be promising criteria.

To mitigate this issue, Lee, C., Kim, S., and Ryu, H., 2019 demonstrated in this work how effective virtual router redundancy protocol (VRRP) approaches may be employed for smart homes in the event of a DDoS attack. It also demonstrates the benefit of deploying the VRRP protocol, which reduces connectivity breakdown.

Additional techniques demonstrated by Bhagat, N.H., 2011 provides a detailed overview of how the virtual router redundancy protocol can be implemented for enterprise networks to achieve high availability. The researcher compares the hot standby router protocol to the virtual router redundancy protocol and explains why VRRP is better at preserving redundancy than HSRP. The researcher included the workings of both protocols in their diagram, as well as difficulties and principles for maintaining efficient redundancy.

Previous work by Pai-Hsiang Hsiao, A. Hwang, H. T., 2021 has also demonstrated how virtual balancing may be achieved on a wireless access network. Using this method, a smart home router may be protected and strengthened against distributed denial of service attacks. The researcher proposes the 'load-balanced tree' load-balancing technique, which is used to improve routing and avoids per-destination and per-flow state for quality of service (QOS) reservation. These approaches can be applied to smart home routers to combat distributed denial of service attacks.

3 Research Methodology

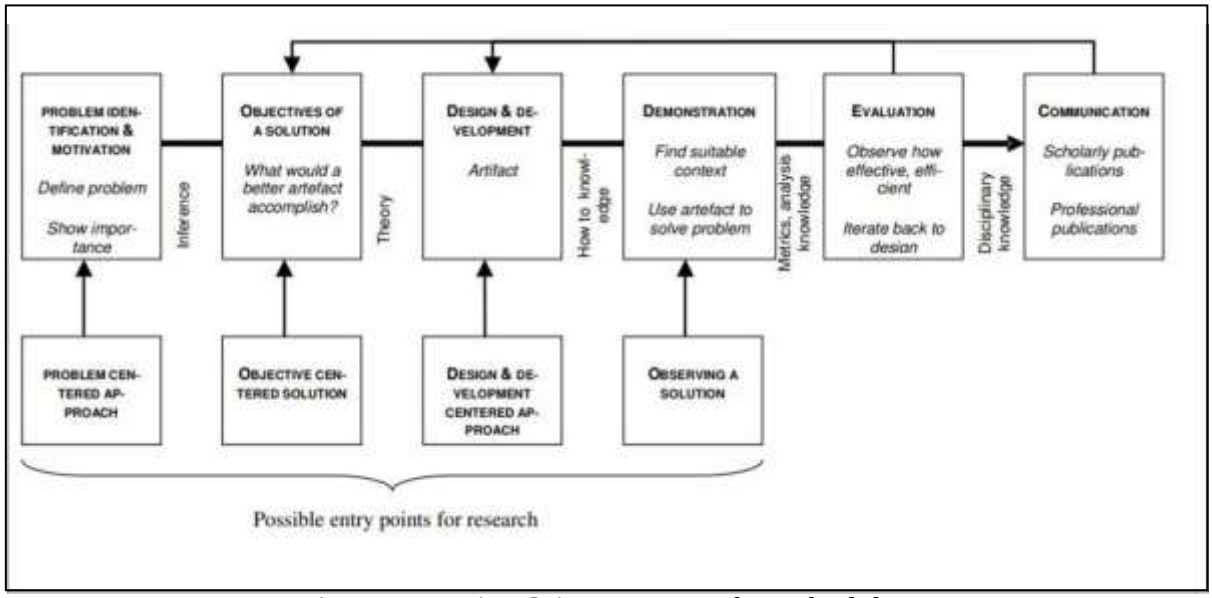

Figure 1: Design Science Research Methodology

The Methodology we used in this paper is the Design Science research methodology *Hukkanen, M. and Idini, A., 2019.* It consists of six stages (as illustrate in figure 1.)

1. *Assessment and purpose of problems* - The first step in research methodology is to identify the research problem, which is then justified with a research question and a solution value. This research question problem can be useful in developing illusionary solutions that can be used to solve a permanent problem as well as original problem intricacies. Because this problem solution is applicable in the real world, it can be used to combat any cyber-attacks on smart home automation. The goal of this research problem would provide a stronger insight of the solution to the research question through a functional depth's execution.

2. *Aim of the proposal* - According to previous related research questions and conclusions, the desirability of various research was determined by estimating the accuracy of the solution. This stage provides a firm understanding of the objective which should be logically derived from the problem definition. Knowledge on the actual situation of issues and current remedies, as well as their effectiveness, are essential resources for this.

3. *Development of the proposal*. - At this stage of design and development, the main focus was on creating an artifactual solution for the smart home network. Using different simulators to test different network diagrams, methods and create the actual implementation of the research problem solution. This stage involves deciding the functional requirement and structures of the artifact, as well as creating the precise artifact which can clearly be comprehended by other researchers.

4. *Demonstration of the proposal* - This stage presents a genuine portrayal of the research problem and how we minimize the problem by attempting to illustrate the usefulness of the artifact in solving the problem. The above presentation necessitates a comprehensive understanding of how the artifact has been applied to solve the problem.

5. *Appraisal of the proposal* - This stage explains how the demonstrated solution of the artifact provides the actual result. The required knowledge to showcase in the demonstration such as relevant metrics and analysis techniques. At this stage explains the actual demonstration of the artifact the researcher can develop new questions related to a research problem. At the completion of the stage, the researcher can decide whether to return to step 3 and make better changes in terms of the efficacy of the artifact.

6. *Communication of the proposal* – The key goal here was to convey the research challenge and demonstrate how essential it is to other academics, professionals, and other communities. The other researcher created and showed a different machine learning technique for mitigating DDOS attacks. The proposal's major goal was to convey how smart home routers may be effective when employing these protocols.

4 Design Specification

The design specification and process flow of our proposed methodology have been discussed and presented in detail in this section. The process flow diagram below describes the actions taken during the assessment to achieve the purpose model objective of combating distributed denial of service attacks and securing IoT devices in smart homes. The ideology is built around two key methodologies: virtual router redundancy protocol and virtual load balancer. VRRP protocol is a virtual router that is used as a backup router to maintain the normal flow of network connectivity to the main router in case of DDoS attack, and load balancer can manage the network flow of incoming traffic, in case of a DDOS attack, both methodologies may be efficiently used to massively reduce the DDoS attack.

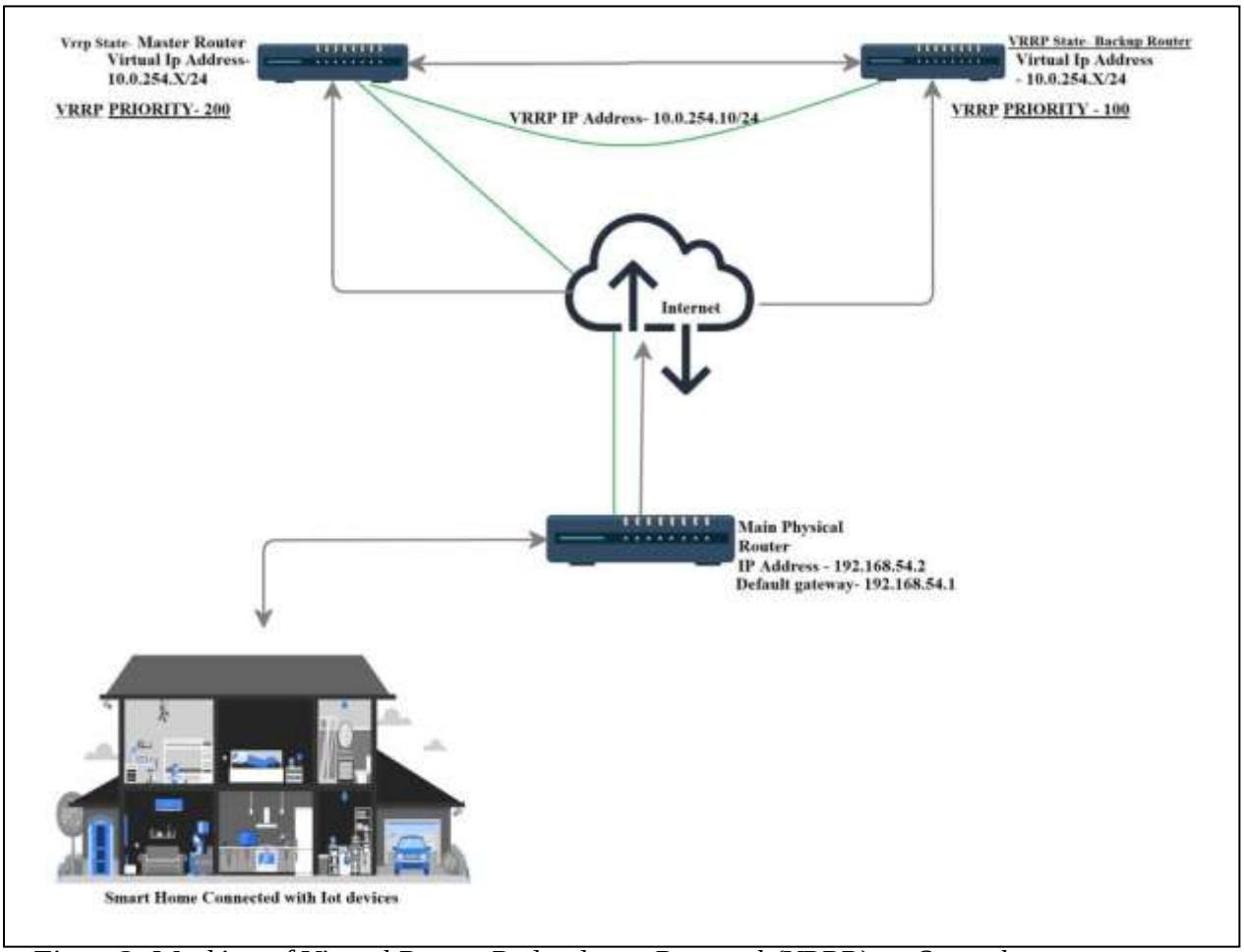

Figure2: Working of Virtual Router Redundancy Protocol (VRRP) on Smart home router.

Virtual Router Redundancy protocol: In our model which is an open standard protocol. The VRRP protocol dynamically assigns responsibilities to a virtual in the Local Area Network. Considering the design specification in our purpose model as shown in the figure the main router is the main connectivity of smart home automation. In case of Distributed denial of service attack on the main router. The Implemented VRRP protocol directly elects another virtual router with the highest priority as Master Router. VRRP is used for dynamic failover to ensure that another virtual router is available. This is implemented by assigning an IP address to a virtual router that serves as the default router. The main router can only be assigned to forward traffic to a designated virtual router. (If the main router is forwarding traffic to a designated virtual router, then that virtual router serves as the master router.) If the preferred backup Router started forwarding traffic for a virtual router, it means it has been replaced from backup to Master router.

1. *Main Router (owner):* The physical router is the main router, and it must be setup using the virtual router redundancy protocol. On the VLAN, the virtual router should be setup with a real IP address. Ultimately, the main router prioritizes the virtual routers as Master Router and Backup Router, assigning high and low priority to routers.

2. *Master Router*: The main router automatically assigns one master router to the network (in any VLAN). If the main router fails to connect due to a network failure, the Master Router (Highest Priority) will immediately connect to the network.

3. *Backup Router*: If the main router and master router fail to offer connectivity, there must always be a backup router to support them. The backup router has a default priority of 100, which determines the precedence of the backup router to operate as a master router in the event of an emergency.

1. Virtual Load Balancer

The load balancer is used as an element of the Multi-layered Security approach. The primary feature is to set up a virtual load balancer on a local area network (LAN) to provide high availability. The main principle of load balancers is to distribute the workload over different servers in order to avoid overloading the system, optimize the process and improve durability. The report demonstrates how a virtual load balancer may be used to keep smart home routers connected and accessible. The load balancer is a built-in GNS3 protocol that may be used to boost resilience by rerouting real-time traffic from one router to another. Distributed denial of service can be mitigated by installing a load balancer, which reduces the attack surface on the primary physical router in a smart home. Implementing a Load balancer on virtual routers can distribute the workload on backup routers.

2. Load balancer Design Fundamental

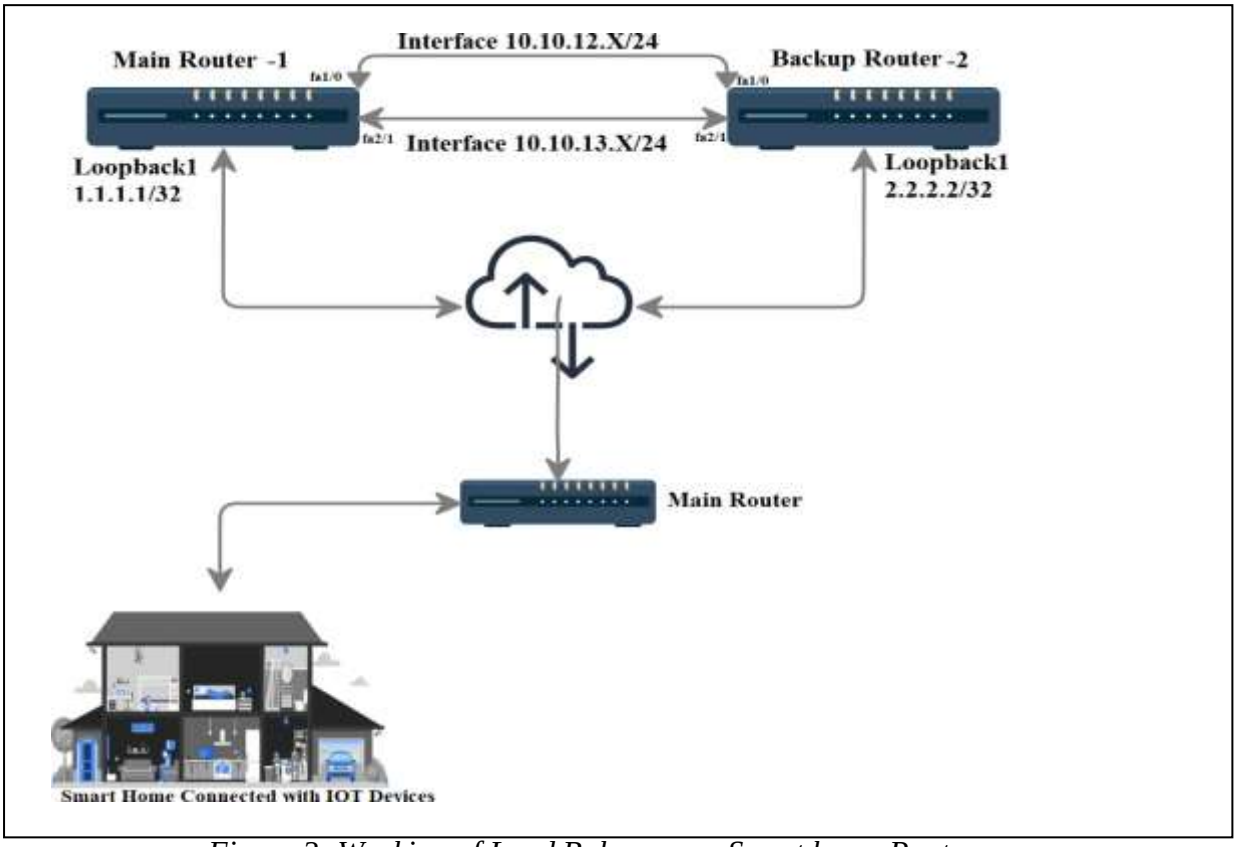

Figure 3: Working of Load Balancer on Smart home Router.

As shown in the figure below, a connected physical router in a smart home has a protocol implemented that is a virtual Router redundancy protocol and a load balancer. A load balancer has been deployed on the virtual router to balance workload on virtual routers. In the eventuality of a DDOS attack, the physical router instantly connects to the virtual router through the virtual router redundancy protocol, which serves as the backup routers. To distribute the workload on the virtual router Load balancer add a resiliency by rerouting live traffic from router to other. Load balancer enables the minimization of node

failures, reduce the attack surface and the reduction of exhaustion resources and overloading networks.

CISCO Express Forwarding (CEF)

The major feature employed in gns3 for load balancing is Cisco Express Forwarding (CEF). The major components of CEF are known as forwarding information bases (FIB). This FIB is used to build numerous routing protocols, each of which contains only the next-hop address for a specific IP-route. CEF primarily focuses on traffic load balancing across multiple outbound routes. Implementing CEF in Gns3 For load balancing, two schemes may be implemented. *(Bhardwaj et al., 2021)*

1. Per-Destination Load-balancing

This technique is adequate for a large number (Source - Destination) sessions. This load balance is also used for individual sessions (Source - Destination)over multiple paths.

2. Per-Packet Load balancing.

This technique is used the round-robin method to process the traffic distribution in which the router sends one packet to the destination over the first path, and to the same destination, it uses the second path, and so on.

This technique is Per-packet load balancing which uses equal utilization of paths that can avoid path congestion.

- Using two techniques, security measures may be created while also ensuringthat critical areas of security are considered.

Smart home automation Store users detailed information, using this methodologies main Physical router can be secured from DDOs attack, and IoT devices connected to the smart home can be secured. Through which we can provide confidentiality to users' data. In a DDoS attack on smart home automation, the user information stored in IoT devices cannot be tampered with, implementation of these two methodologies can always provide connectivity and Security which reduce the chances of tampering of user's data which provides Integrity to the user. The user should be able to access the network and IoT devices 24/7. Implementing Methodology's on the home router can work effectively, efficiently to enable high availability to users by operating as virtual standby routers.

5 Implementation

This Section of report explains the implementation of the two Methodologies used in securing home automation to mitigate from distributed denial of service attack. The methods were implemented using Graphical Network Simulator-3 **[GNS3]**, which is a visual simulation application that allows users to create alternative topologies and simulate real computer networks. The application offers many features and a command line interface for simulating the configuration of Cisco routers and switches.

This section explain implementation of two methodologies on Gns3 in two phases.

I. First phases explain the Required stimulator, IOS files, virtual machine Appliance file.
II. Second phase explain primarily focus on connecting GNS3 with KaliLinux

Phase 1:

Smart home automation was implemented on the Gns3 stimulator, which allows for real-time network stimulation. Using Gns3 stimulator different router, switch's, virtual PC stimulator are used as shown in Table no 4. (*VPCS Configuration and Operation, 2021)* (*cisco-ios-images-for-dynamips/. 2021)*

SR No.	***Networking Devices***	***Description***	***IDLE-PC Value***
1.	C3602	C3602 is a cisco Router ISO image which support 8 maximum Ethernet ports and 32 Fast-ethernet Ports and 8 serial ports.	Idle -PC value: 0x6050b114
2.	C7206	C7206 has a different design	Idle-PC Value:

		which support 1 fast-ethernet port, 6 port adapters.	0x606dc520
3.	C3725	C3725 is cisco Router IOS image which support 2 Fast-Ethernet Interface, 6 serial ports.	Idle-PC value: 0x602467a4
4.	Ethernet Switch [Managed Switch]	The ethernet switch is part of Dynagen package which is used GNS3 to emulate router.	***Objective:*** Managed switch is used in LAN which can be useful to integrate several IOT devices.
5.	VPCS (Virtual PC Stimulators)	VPCS is a light-load PC stimulator which is used gns3 to check the connectivity between two different systems.2	***Objective:*** kali Linux is used in-order to demonstrate DDOs attack on smart home Physical router.

Table 4: Router and Switches used in our experiment

Phase 2:

Following the initial phase of connecting the router and switch, the link between the IOT devices and physical router is implemented. The second phase shows how to integrate GNS3 with Kali Linux. This implementation demonstrates a Distributed Denial of Service (DDoS) attack on a physical router and how quickly an attacker may disconnect all IoT devices in a smart home.

1. Kali Linux integration with GNS3 is supported in GNS3 VM version 2.2.27 by manually importing virtual machines.
2. Because GNS3-VM offers a variety of options for deploying a machine through virtual-box or VMware.
3. Because Virtual-Box is installed on the host operating system, GNS3 instantly enables the user with the option to identify the loaded machine on GNS3.
4. After merging the virtual machine with GNS3, it appears as a virtual PC stimulator (VPCS).

As illustrated in the state diagram in figure 5, the virtual router redundancy protocol and load balancer are deployed as backup virtual routers to support the primary physical router. The state diagram depicts the operating concept of the protocol deployed on the Main Router to secure network access to which IoT devices are linked. If the primary router fails during a distributed denial of service attack, the deployed VRRP protocol is automatically enabled. Even if the Virtual backup Router (VRRP) is overburdened by network traffic, the Load balancer between the two virtual routers evenly distributes the workload, reducing the attack surface of distributed denial of service attacks.

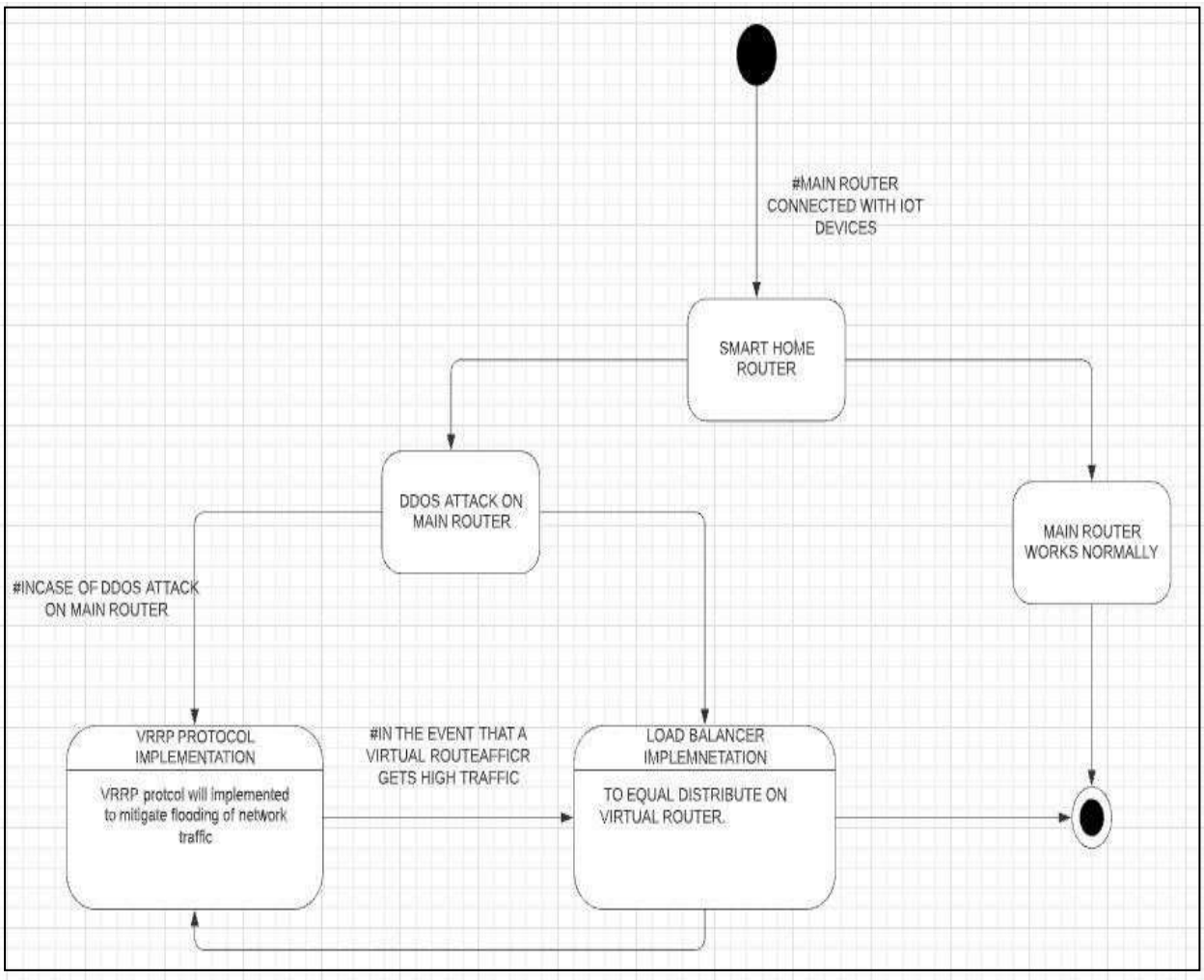

Figure5: State diagram depicts working model of Two methodology.

6 Evaluation

GNS3 stimulator was installed and integrated with Kali Linux to test the functionality of network topology. GNS3 was installed on the host system (Windows 10) and Kali Linux was installed on a virtual machine. The main goal was to carry out the DDOS attack on the GNS3 stimulator (router) in order to illustrate the attack and how it might impact the main Physical router. The network between the topologies has been configured for this topology.

6.1 Experiment 1: Testing Environment Setup

In order to stimulate the network traffic, 3-router was set up for the VRRP testing environment. Routers A, B, C are the Main physical router, a Master router, backup router respectively. Router A, B, and C were already configured with VRRP protocol. Sending ICMP traffic from Router A to B to check the connection between the routers.

1. The router with the highest priority is set as the master router and the lowest priority router is set as the backup router. Set the highest priority router (200), as indicated in the image below, as theMaster router.
2. The router with the lowest priority (100) is designated as the backup router.
3. If Master router fails Backup router Goes in Initial stage as shown in figure.

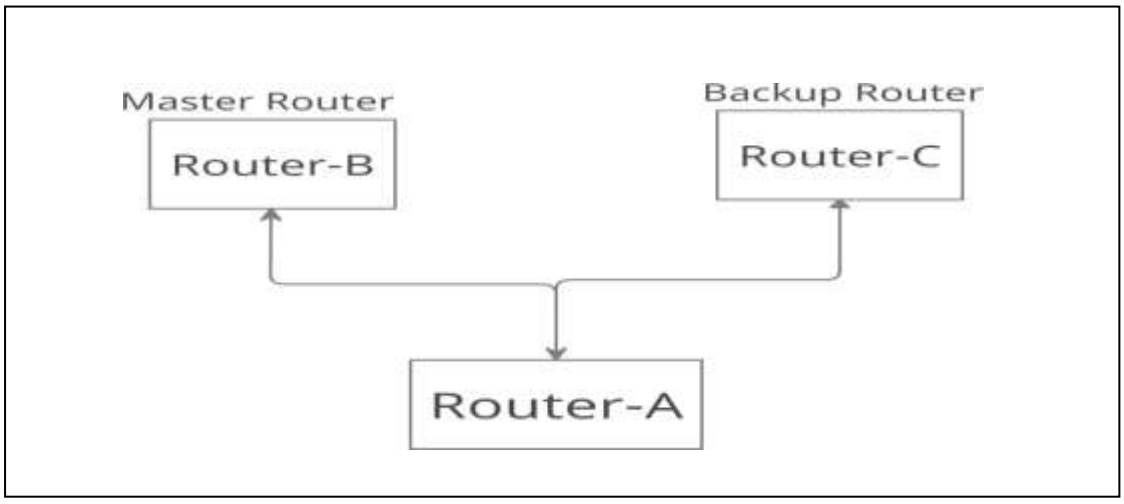

Figure 6: Illustration of VRRP Test environment

4. Master Router is configured with VRRP Protocol, with priority 200. Whenthe master router is configured, the VRRP status shown in figure 7. This

diagram depicts Master Router information, with emphasis on its configuredstate, Virtual IP address, Advertisement Interval, and Authentication.

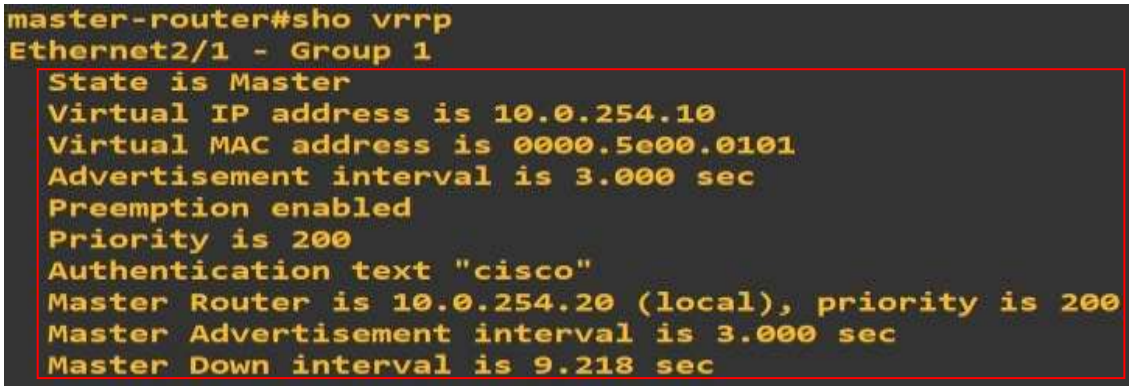

Figure 7: Configuration of VRRP Status in GNS3.

5. Backup Router configuration with VRRP Protocol, Setting up priority 100. When the Backup router is configured, the VRRP status is shown in figure 8. This diagram depicts Backup Router information, with emphasis on its configured state, Virtual IP address, Advertisement Interval, and Authentication.

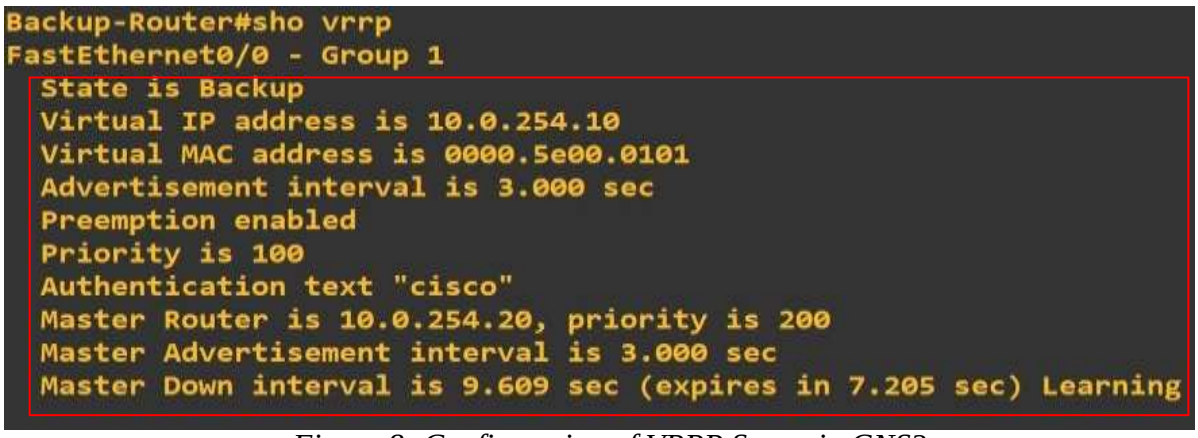

Figure 8: Configuration of VRRP Status in GNS3

6.2 Experiment 2: Testing Load balancer on virtual router when VRRP master router fails

We check Load balancer protocol testing on virtual router once the master router fails, to have the backup for virtual backup routers the load balancing techniques can be used. The load balancer can distribute the real-time traffic and network failover chances for the main physical router reduces. In the case of DDOs attack on the Main physical router the implemented VRRP protocol will be working as a supporting virtual router redundancy protocol and Load balancing techniques is implemented. (Load balancing GRE tunneled multicast traffic, 2021)

As to check the working principle of the load balancing algorithm we have created a table of interface tunneling of incoming traffics which is demultiplexed to the appropriate tunnel.

Tunnel 1: When we transmit an ICMP packet from Master router to Backup router, we examine that it takes IP route ethernet 1/0 to loopback1.

	Master Router-1	**Backup Router-2**
Tunnel	Interface 1	Interface 2
IP Address	10.10.12.1	2.2.2.2/24
Tunnel Source IP	ethernet 1/0	Loopback1
Load balancing Mode	CEF	CEF

Tunnel 2: Additionally, when send packets from Master router, we examine that it takes IP route ethernet 2/0 to loopback1

	Master Router-1	**Backup Router-2**
Tunnel Interface	Tunnel 1	Tunnel 2
IP Address	10.10.13.1/24	2.2.2.2/24
Tunnel Source IP	ethernet 2/0	Loopback1

Load balancing Mode	CEF	CEF

Tunnel3: At last, we send ICMP packet, we examine that again it takes IP route ethernet 1/0 to loopback1

	Master Router-1	**Backup Router-2**
Tunnel Interface	Tunnel 1	Tunnel 2
IP Address	1.1.1.1/32	2.2.2.2/32
Tunnel Source IP	Loopback1	Loopback1
Load balancing Mode	CEF	CEF

6.3 Experiment 3: Additional Cyberattack on Smart home Automation**.**

DDos attacks on smart home automation can bring entire networks offline. The distributed denial of service (DDoS) attack may be conducted using open-source software such as slow-Loris, HPING3, or Orbit Ion Cannon (LOCI), which are free software that can be used by the normal user or hacker to test the attack on our network. We focused on DDos attacks in our model and suggested a mitigation approach for smart routers. The adopted methodology may be effective in mitigating additional cyber threats on smart home automation.

- Additional cyber-attacks that can be on smart home automation to make the devices vulnerable are discussed in this case study. We provide a graph that depicts the period of cyber-attacks from 2012 to 2020 that may have an impact on smart home automation. Cyber-attacks on smart homes target two primary sources: networks and IoT devices, intending to exploit users' information in smart homes.

- DDOs attack volume has increased tremendously over the last year, as measured in Gbps. In comparison to 2014, the amount of DDoS attacks grew in 2015, and this trend is expected to continue through 2020.

- There is an increase in the frequency of online platforms that provide a service-botnets that are capable of launching distributed denial of service attacks. The increasing number of botnets enables for higher quantities of network traffic to be generated and make a attack. *(Peraković, Periša and Cvitić, 2015)*

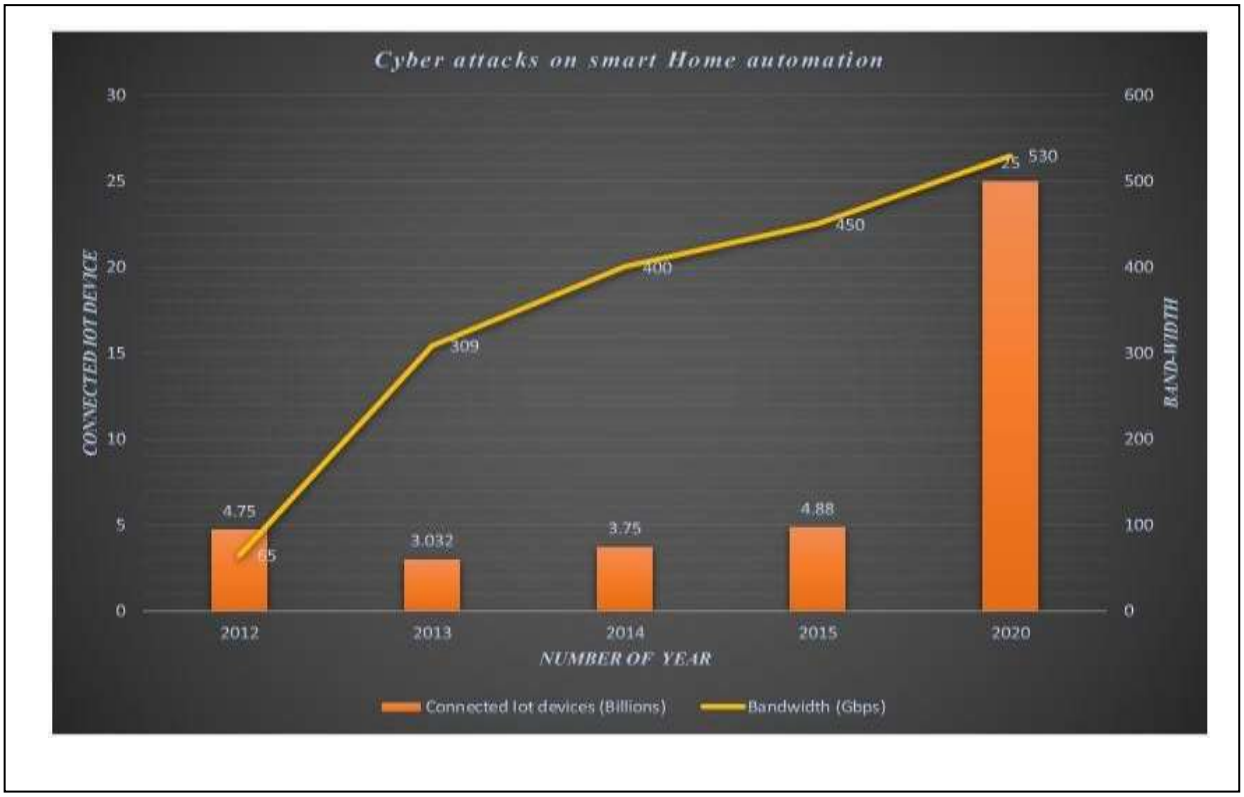

Figure 9: The ratio of increase in cyberattacks on Smart Home Automation. (Peraković, Periša and Cvitić, 2015)

6.4 Discussion

Based on the analysis of the abovementioned case study procedure, the designed integrated methodology should be deployed on smart home routers to secure against distributed denial of service attacks. The testing process result demonstrates that the Physical router can function well while mitigating DDOs and other cyber-attacks. According to the above case study, the virtual router redundancy protocol is a useful protocol that users may utilize. Despite the second case study, virtual load balancing strategies to decrease the attack surface of DDOs attacks should be a viable option for distributing the load

across the routers. This technique will be useful in critical analysis to make routers stronger and smarter.

As a result, this report is suitable for real-world deployment. The paper also includes a step-by-step strategy for integrating two methodologies that can contribute to home automation security. The most promising prospect is to create Cybersecurity from each and every perspective in order to secure individuals' personal information, as well as methods to construct smart home router a defender to counteract any cyberattacks.

7 Conclusion and Future Work

As an IoT device, it is used in smart homes to improve the quality of life by linking smart devices that can automate everything around us. There is also a considerable chance of attackers gaining access to this device. The fundamental difficulty with this IoT device is its poor processing power, which cannot deal with oversaturated internet access traffic and so presents a weakness for attackers. This study uses two ways to mitigate distributed denial of service attacks in smart home automation. Because smart home automation is prone to DDOs, keeping personal information is incredibly dangerous. However, being the main network entry point, it must be secured. However, in the event of a network outage or a DDoS attack, smart home automation may be compromised. As a result, we require a mitigation approach to fight against DDOs attacks. As a result, we developed a Mitigation approach that can be deployed in smart home routers. Integrating VRRP protocol and load balancing method DDos can be minimized, since we deploy a virtual backup router to the primary physical router. In all conditions, users should have access to network which will provide connectivity and availability. However, because there is a significant probability of traffic for overloading the router in a DDos situation, the virtual router should have a load balancing approach by which deployed virtual router can efficiently share traffic workload and Distributed denial of attack may be minimized. There is a situation in which a smart house is connected to IoT devices, and the main physical router is attacked by DDoS using the Hping3 tool in Kali Linux. According to the research, the main physical router is overloaded by bogus traffic generated by the attacker. The primary physical router is automatically shut down, and a virtual backup router is set up.

Virtual router redundancy protocol and load balancer can be enhanced in the future by employing numerous ways using these two methodologies that can be used to counteract additional cyberattacks. Load balancing hashing algorithm and Round-Robin are two load balancing strategies that can be used to provide good load distribution on a local area network.

References

- Kavallieratos, G., Chowdhury, N., Katsikas, S., Gkioulos, V. and Wolthusen, S., 2019. Threat analysis for smart homes. *Future Internet*, *11*(10), p.207.'
- Karthikeyan, B., 2014. Detecting and Isolating Distributed Denial of Service Attack in Smart Grid Systems. *Diss. National Institute of Technology Rourkela*.
- Burhan, M., Rehman, R.A., Khan, B. and Kim, B.S., 2018. IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors*, *18*(9), p.2796.
- Chen, E.Y. and Yonezawa, A., 2005, January. Practical techniques for defending against DDoS attacks. In *The 3rd ACS/IEEE International Conference onComputer Systems and Applications, 2005.* (p. 72). IEEE.
- Lee, C., Kim, S. and Ryu, H., 2019. FDVRRP: Router implementation for fast detection and high availability in network failure cases. *ETRI Journal*, *41*(4), pp.473-482.
- Bhagat, N.H., 2011. Virtual Router Redundancy Protocol-A Best Open Standard Protocol in Maintaining Redundancy. In *International Conference on Web Services Computing (ICWSC). Palo Alto, CA, USA September* (pp. 18-21).
- Hsiao, Pai-Hsiang, Adon Hwang, H. T. Kung, and Dario Vlah. "Load-balancing routing for wireless access networks." In *Proceedings IEEE INFOCOM 2001. Conference on computer communications. Twentieth annual joint conference of the IEEE computer and communications society (Cat. No. 01CH37213)*, vol. 2, pp. 986-995. IEEE, 2001.
- Kirsebom, O.S., Jones, S., Strömberg, D.F., Martínez-Pinedo, G., Langanke, K., Röpke, F.K., Brown, B.A., Eronen, T., Fynbo, H.O.U., Hukkanen, M. and Idini, A., 2019. This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details. *PHYSICAL REVIEW LETTERS Phys Rev Lett*, *123*, p.262701.
- Bhardwaj, R., Bhardwaj, R., Bhardwaj, R., Bhardwaj, R., Bhardwaj, R., Bhardwaj, R. and Bhardwaj, R., 2021. *LOAD BALANCING – PER PACKET AND PER DESTINATION - IP With Ease*. [online] IP With Ease. Available at: <https://ipwithease.com/load-balancing-per-packet-and-per-destination/> [Accessed 14 December 2021].

- N-Study. 2021. *VPCS Configuration and Operation*. [online] Available at: <https://www.n-study.com/en/how-to-use-gns3/vpcs/> [Accessed 14 December 2021].
- cisco-ios-images-for-dynamips/. 2021. [online] Available at: <https://docs.gns3.com/docs/emulators/cisco-ios-images-for-dynamips/> [Accessed 7 December 2021].
- Geng, Q. and Huang, X., 2018. VRRP Load Balance Technology Simulation Practice Based on GNS3. In *MATEC Web of Conferences* (Vol. 228, p. 03012). EDP Sciences.
- Pavithra, K.C., Shetty, S. and Nagesh, H.R., 2014. A Comprehensive Study on Distributed Denial of Service Attacks and Defense Mechanisms. *International Journal of Computer Applications*, *975*, p.8887.
- NIST. 2021. *National Institute of Standards and Technology | NIST*. [online] Available at: <https://www.nist.gov/> [Accessed 14 December 2021].
- Peraković, D., Periša, M. and Cvitić, I., 2015. Analysis of the IoT impact on volume of DDoS attacks. *XXXIII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju–PosTel*, *2015*, pp.295-304.
- CCIE, the beginning!. 2021. *Load balancing GRE tunneled multicast traffic*. [online] Available at: <https://cciethebeginning.wordpress.com/2010/07/26/load-balancing-gre-tunneled-multicast-traffic-3/> [Accessed 14 December 2021].