UTILIZING FIRST HOP REDUNDANCY PROTOCOL TO MITIGATE THE EFFECT OF DENIAL-OF-SERVICE ATTACK

BY

KHONG JOHNSON

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF COMMUNICATION AND NETWORKING (HONS)

Faculty of Information and Communication Technology
(Perak Campus)

JANUARY 2018
REPORT STATUS DECLARATION FORM

Title: ________________________________________________________
__________________________________________________________
__________________________________________________________

Academic Session: _____________

I __________________________________________________________
(CAPITAL LETTER)

declare that I allow this Final Year Project Report to be kept in
Universiti Tunku Abdul Rahman Library subject to the regulations as follows:
1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified by,

______________________________________________  ________________________________
(Author’s signature)  (Supervisor’s signature)

Address:
______________________________________________
______________________________________________
______________________________________________
______________________________________________

Supervisor’s name

Date: _____________________  Date: _____________________
UTILIZING FIRST HOP REDUNDANCY PROTOCOL TO MITIGATE THE
EFFECT OF DENIAL-OF-SERVICE ATTACK

BY
KHONG JOHNSON

A REPORT
Submitted to
Universiti Tunku Abdul Rahman
in partial fulfillment of the requirements
for the degree of
BACHELOR OF COMMUNICATION AND NETWORKING (HONS)
Faculty of Information and Communication Technology
(Perak Campus)

JANUARY 2018
DECLARATION OF ORIGINALITY

I declare that this report entitled “Utilizing First Hop Redundancy Protocol to Mitigate the Effect of Denial-Of-Service Attack” is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature : ______________________

Name : KHONG JOHNSON________

Date : 6th APRIL 2018____________
ACKNOWLEDGEMENTS

I would like to express my sincere thanks and appreciation to my supervisors, Dr. Gan Ming Lee who has given me this bright opportunity to engage in an network security project. It is my first step to establish a career in networking and network security field. A million thanks to you.

To a very special person in my life, Chow Wen Chai, for her unconditional support during hard times. Finally, I must say thanks to my parents and my family for their love, support and continuous encouragement throughout the course.
ABSTRACT

This paper is to determine whether first hop redundancy protocol is viable to mitigate the effect of denial-of-service attack (DoS). Since DoS attack is significantly influencing the security and reliability of networks, it urged the researches to come out a proposed solution to mitigate DoS attack. However, most of the proposed solutions increase the workload of the network devices especially the routers and thus lead to network latency. For example, previous researchers suggested to put capabilities in every packet sent to be acknowledged as wanted packet by the destination host. This solution not only increase the workload of router to stamp and check the capabilities on every packet, it also derives other possible attack which is Denial-of-Capability attack. Henceforth, in this work, we would like to introduce an alternative solution to mitigate DoS attack without increasing the workload of network devices and yet efficient. The proposed solution is to use First Hop Redundancy Protocol specifically the Gateway Load Balancing Protocol (GLBP) to form a group of redundant routers. The redundant routers share one virtual IP address as the IP gateway for the hosts. One of the routers will be elected as Active Virtual Gateway (AVG) which will assign virtual MAC address to other redundant routers known as Active Virtual Forwarder (AVF). Whenever packets sent to the virtual IP gateway, AVG will answer for the ARP request for the virtual IP address from the host. Then load balancing is achieved by the AVG replying to the ARP requests with different virtual MAC addresses in round-robin basis. By doing so, the routers will not be buffer overflow and down, henceforth DoS attack could be mitigated. In this work, a simulation will be carried out before implementing GLBP to show that DoS attack can be done successfully. Later, GLBP will be implemented in a group of redundant routers and to simulate that DoS attack is successfully mitigated.
TABLE OF CONTENTS
TITLE .................................................................................................................................................. i
DECLARATION OF ORIGINALITY .................................................................................................. ii

ABSTRACT ........................................................................................................................................ iv

TABLE OF CONTENTS ................................................................................................................ v
LIST OF TABLES ........................................................................................................................ vii
LIST OF FIGURES ........................................................................................................................ viii
LIST OF ABBREVIATIONS ............................................................................................................ xiii

Chapter 1 : INTRODUCTION ........................................................................................................... 1
1.1. MOTIVATION AND PROBLEM STATEMENT ........................................................................ 1
1.2. PROJECT SCOPE .................................................................................................................. 1
1.3. PROJECT OBJECTIVES ....................................................................................................... 4
1.4. IMPACT, SIGNIFICANCE AND CONTRIBUTION ............................................................... 5
1.5. BACKGROUND INFORMATION ........................................................................................ 6
1.6. REPORT ORGANISATION .................................................................................................... 8

Chapter 2 : LITERATURE REVIEW ................................................................................................ 9
2.1 - EXISTING PROPOSED SOLUTIONS OVERVIEW ............................................................ 9
2.2 - PACKET FILTERING ......................................................................................................... 10
2.3 - CAPABILITY ..................................................................................................................... 10
2.4 - CAPTCHA MECHANISM .............................................................................................. 12
2.5 - INGRESS FILTERING ....................................................................................................... 13

Chapter 3 : PROPOSED METHOD/APPROACH ............................................................................. 15
3.1 DESIGN SPECIFICATIONS ................................................................................................. 15
3.2 EVALUATING PLAN FOR PERFORMANCE OF GLBP IN MITIGATING SYN FLOOD ATTACK .......................................................................................................................... 18
3.3 MITIGATION OF ADDITIONAL TYPE OF DoS ATTACKS ....................................................... 18
3.4 SYSTEM DESIGN / OVERVIEW .......................................................................................... 21
3.5 IMPLEMENTATION ISSUES AND CHALLENGES ............................................................... 30
3.6 COST ANALYSIS ................................................................................................................ 30
3.7 TIMELINE ............................................................................................................................ 31

Chapter 4 : TESTING RESULTS AND DISCUSSION .................................................................... 35
4.1 SYN FLOOD ATTACK ........................................................................................................... 35
4.2 PING FLOOD ATTACK ......................................................................................................... 41
4.3 ACK FLOOD ATTACK .................................................................45
4.4 Additional research results ......................................................49
4.5 DISCUSSION FOR SLOWLORIS ATTACK ..............................63

Chapter 5: CONCLUSION ................................................................66

Chapter 6: BIBLIOGRAPHY ..........................................................68

APPENDICES ..................................................................................A-1

APPENDICES A: Router Configuration with GLBP implemented ..........A-1
APPENDICES B: Configuration on PC running Apache Web Server .......B-1
APPENDICES C: Configuration on Attacker’s PC ..............................C-1
APPENDICES D: Final Year Project Biweekly Report .........................D-1
APPENDICES E: POSTER ...............................................................E-1
APPENDICES F: Example of plagiarism check summary ..................F-1
LIST OF TABLES

Table Number | Title | Page
--- | --- | ---
Table 3-1: Table for the network configuration with GLBP implemented | 17
Table 3-2: Table for cost analysis | 30
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure Number</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1-1</td>
<td>Network topology for first simulation</td>
<td>2</td>
</tr>
<tr>
<td>Figure 1-2</td>
<td>Network topology for second simulation</td>
<td>3</td>
</tr>
<tr>
<td>Figure 1-3</td>
<td>GLBP operation (Gan, 2017).</td>
<td>7</td>
</tr>
<tr>
<td>Figure 2-1</td>
<td>Process of adding capability into packet in TVA network (Yang, Wetherall and Anderson, 2005)</td>
<td>11</td>
</tr>
<tr>
<td>Figure 2-2</td>
<td>Login page with CAPTCHA verification included (Elias, 2009)</td>
<td>13</td>
</tr>
<tr>
<td>Figure 2-3</td>
<td>CATPCHA verification before accessing to login page (Know Your Meme, n.d.)</td>
<td>13</td>
</tr>
<tr>
<td>Figure 3-1</td>
<td>Network topology for first simulation</td>
<td>15</td>
</tr>
<tr>
<td>Figure 3-2</td>
<td>Network topology for second simulation</td>
<td>17</td>
</tr>
<tr>
<td>Figure 3-3</td>
<td>Flowchart for SYN flood attack before GLBP</td>
<td>21</td>
</tr>
<tr>
<td>Figure 3-4</td>
<td>Network built for first simulation in Practical Lab</td>
<td>22</td>
</tr>
<tr>
<td>Figure 3-5</td>
<td>Flowchart for SYN flood attack after GLBP</td>
<td>23</td>
</tr>
<tr>
<td>Figure 3-6</td>
<td>Flowchart for SYN flood attack before GLBP</td>
<td>24</td>
</tr>
<tr>
<td>Figure 3-7</td>
<td>Flowchart for PING flood attack after GLBP</td>
<td>25</td>
</tr>
<tr>
<td>Figure 3-8</td>
<td>Flowchart for ACK flood attack before GLBP</td>
<td>26</td>
</tr>
<tr>
<td>Figure 3-9</td>
<td>Flowchart for ACK flood attack after GLBP</td>
<td>26</td>
</tr>
<tr>
<td>Figure 3-10</td>
<td>Flow chart for launching Slowloris attack</td>
<td>27</td>
</tr>
<tr>
<td>Figure 3-11</td>
<td>Flowchart of varying the packets sent interval before GLBP</td>
<td>28</td>
</tr>
<tr>
<td>Figure 3-12</td>
<td>Flowchart of varying the packets sent interval after GLBP</td>
<td>29</td>
</tr>
<tr>
<td>Figure 3-13</td>
<td>Gantt chart for current semester</td>
<td>32</td>
</tr>
<tr>
<td>Figure 3-14</td>
<td>Gantt chart for future semester</td>
<td>34</td>
</tr>
<tr>
<td>Figure 4-1</td>
<td>Page Load Time for first tab is 289ms (SYN flood)</td>
<td>35</td>
</tr>
<tr>
<td>Figure 4-2</td>
<td>Page Load Time for second tab is 120ms (SYN flood)</td>
<td>35</td>
</tr>
<tr>
<td>Figure 4-3</td>
<td>Page Load Time for third tab is 117ms (SYN flood)</td>
<td>35</td>
</tr>
<tr>
<td>Figure 4-4</td>
<td>Page Load Time for forth tab is 97ms (SYN flood)</td>
<td>35</td>
</tr>
<tr>
<td>Figure 4-5</td>
<td>Page Load Time for fifth tab is 106ms (SYN flood)</td>
<td>35</td>
</tr>
<tr>
<td>Figure 4-6</td>
<td>Page Load Time for first tab after SYN flood attack is 10.65s</td>
<td>36</td>
</tr>
<tr>
<td>Figure 4-7</td>
<td>Page Load Time for second tab after SYN flood attack is 29.21s</td>
<td>36</td>
</tr>
<tr>
<td>Figure 4-8</td>
<td>Page Load Time for third tab after SYN flood attack is 28.02s</td>
<td>36</td>
</tr>
<tr>
<td>Figure 4-9</td>
<td>Page Load Time for forth tab after SYN flood attack is 27.45s</td>
<td>36</td>
</tr>
</tbody>
</table>
Figure 4-10: Page Load Time for fifth tab after SYN flood attack is 26.73s ..........37
Figure 4-11: Ping reply time before and after SYN flood attack..........................38
Figure 4-12: Page Load Time for first tab after mitigation of SYN flood attack is
1.14s .........................................................................................................................39
Figure 4-13: Page Load Time for second tab after mitigation of SYN flood attack is
1.18s .........................................................................................................................39
Figure 4-14: Page Load Time for third tab after mitigation of SYN flood attack is
185ms .....................................................................................................................39
Figure 4-15: Page Load Time for forth tab after mitigation of SYN flood attack is
172ms .....................................................................................................................39
Figure 4-16: Page Load Time for fifth tab after mitigation of SYN flood attack is
181ms .....................................................................................................................40
Figure 4-17: Page load time of first tab before mitigation of PING flood attack is
510ms ....................................................................................................................41
Figure 4-18: Page load time of 2nd tab before mitigation of PING flood attack is
3244ms ...................................................................................................................41
Figure 4-19: Page load time of 3rd tab before mitigation of PING flood attack is
508ms ....................................................................................................................42
Figure 4-20: Page load time of 4th tab before mitigation of PING flood attack is
3222ms ...................................................................................................................42
Figure 4-21: Page load time of 5th tab before mitigation of PING flood attack is
478ms ....................................................................................................................42
Figure 4-22: Page load time of 1st tab after mitigation of PING flood attack is 188ms
.................................................................................................................................43
Figure 4-23: Page load time of 2nd tab after mitigation of PING flood attack is 176ms
.................................................................................................................................43
Figure 4-24: Page load time of 3rd tab after mitigation of PING flood attack is 166ms
.................................................................................................................................43
Figure 4-25: Page load time of 4th tab after mitigation of PING flood attack is 204ms
.................................................................................................................................44
Figure 4-26: Page load time of 5th tab after mitigation of PING flood attack is 196ms
.................................................................................................................................44
Figure 4-27: Page load time before mitigation of ACK flood attack for 1st tab is 600ms ................................................................. 45
Figure 4-28: Page load time before mitigation of ACK flood attack for 2nd tab is 1950ms ................................................................. 45
Figure 4-29: Page load time before mitigation of ACK flood attack for 3rd tab is 1306ms ................................................................. 46
Figure 4-30: Page load time before mitigation of ACK flood attack for 4th tab is 2736ms ................................................................. 46
Figure 4-31: Page load time before mitigation of ACK flood attack for 5th tab is 6198ms ................................................................. 46
Figure 4-32: Page load time after mitigation of ACK flood attack for 1st tab is 180ms ................................................................. 47
Figure 4-33: Page load time after mitigation of ACK flood attack for 2nd tab is 188ms ................................................................. 47
Figure 4-34: Page load time after mitigation of ACK flood attack for 3rd tab is 178ms ................................................................. 48
Figure 4-35: Page load time after mitigation of ACK flood attack for 4th tab is 204ms ................................................................. 48
Figure 4-36: Page load time after mitigation of ACK flood attack for 5th tab is 172ms ................................................................. 48
Figure 4-37: Page load time when u1 as packets interval in SYN flood attack (Before GLBP) ................................................................. 49
Figure 4-38: Page load time when u10 as packets interval in SYN flood attack (Before GLBP) ................................................................. 50
Figure 4-39: Page load time when u100 as packets interval in SYN flood attack (Before GLBP) ................................................................. 50
Figure 4-40: Page load time when u1000 as packets interval in SYN flood attack (Before GLBP) ................................................................. 50
Figure 4-41: Page load time when u10000 as packets interval in SYN flood attack (Before GLBP) ................................................................. 51
Figure 4-42: Page load time when u100000 as packets interval in SYN flood attack (Before GLBP) ................................................................. 51

BCN (Hons) Communication and Networking
Faculty of Information and Communication Technology (Perak Campus), UTAR
Figure 4-43: Graph of page load time with SYN flood packets interval varies (Before GLBP) .........................................................................................................................52
Figure 4-44: Total packets sent with varying packets interval set .........................53
Figure 4-45: Page load time when u1 as packets interval in SYN flood attack (After GLBP) .........................................................................................................................54
Figure 4-46: Page load time when u10 as packets interval in SYN flood attack (After GLBP) .........................................................................................................................54
Figure 4-47: Page load time when u100 as packets interval in SYN flood attack (After GLBP) .........................................................................................................................54
Figure 4-48: Page load time when u1000 as packets interval in SYN flood attack (After GLBP) .........................................................................................................................55
Figure 4-49: Page load time when u10000 as packets interval in SYN flood attack (After GLBP) .........................................................................................................................55
Figure 4-50: Page load time when u100000 as packets interval in SYN flood attack (After GLBP) .........................................................................................................................55
Figure 4-51: Graph of page load time with SYN flood packets interval varies (After GLBP) .........................................................................................................................56
Figure 4-52: Graph of page load time with SYN flood packets interval varies (Before and After GLBP) .........................................................................................................................56
Figure 4-53: Page load time when u1 as packets interval in PING flood attack (Before GLBP) .........................................................................................................................57
Figure 4-54: Page load time when u10 as packets interval in PING flood attack (Before GLBP) .........................................................................................................................57
Figure 4-55: Page load time when u100 as packets interval in PING flood attack (Before GLBP) .........................................................................................................................58
Figure 4-56: Page load time when u1000 as packets interval in PING flood attack (Before GLBP) .........................................................................................................................58
Figure 4-57: Page load time when u10000 as packets interval in PING flood attack (Before GLBP) .........................................................................................................................58
Figure 4-58: Page load time when u100000 as packets interval in PING flood attack (Before GLBP) .........................................................................................................................59
Figure 4-59: Graph of page load time with PING flood packets interval varies (Before GLBP) .........................................................................................................................59
Figure 4-60: Page load time when u1 as packets interval in PING flood attack (After GLBP) .................................................................................................................................................. 60
Figure 4-61: Page load time when u10 as packets interval in PING flood attack (After GLBP) .................................................................................................................................................. 60
Figure 4-62: Page load time when u100 as packets interval in PING flood attack (After GLBP) .................................................................................................................................................. 60
Figure 4-63: Page load time when u1000 as packets interval in PING flood attack (After GLBP) .................................................................................................................................................. 61
Figure 4-64: Page load time when u10000 as packets interval in PING flood attack (After GLBP) .................................................................................................................................................. 61
Figure 4-65: Page load time when u100000 as packets interval in PING flood attack (After GLBP) .................................................................................................................................................. 61
Figure 4-66: Graph of page load time with PING flood packets interval varies (After GLBP) .................................................................................................................................................. 62
Figure 4-67: Graph of page load time with SYN flood packets interval varies (Before and After GLBP) .................................................................................................................................................. 62
Figure 4-68: HTTP GET header .................................................................................................................................................................................................................................................................................................................................................. 63
Figure 4-69: Slowloris -GET .................................................................................................................................................................................................................................................................................................................................................. 63
Figure 4-70: Slowloris – GET .................................................................................................................................................................................................................................................................................................................................................. 64
Figure 4-71: GLBP failed to mitigate Slowloris attack .................................................................................................................................................................................................................................................................................................................................................. 64
**LIST OF ABBREVIATIONS**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLBP</td>
<td>Gateway Load Balancing Protocol</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial-of-Service</td>
</tr>
<tr>
<td>DoC</td>
<td>Denial-of-Capability</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality-of-Service</td>
</tr>
<tr>
<td>SYN</td>
<td>Synchronize</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
</tbody>
</table>
1.1. MOTIVATION AND PROBLEM STATEMENT

Denial of service (DoS) is a cyber-attack where attacker attempts to prevent legitimate users from accessing information or services by intentionally excessive using of the resources to an extent that they are not available to the legitimate users. As the impact of abrupt growth of advance technologies, DoS attack has become an appalling threat to the reliability of the Internet. According to the research done by Moore, Voelker and Savage (2006, p.1), they found 12,805 DoS attacks over 500 different organisations which are ranging from Amazon, Hotmail to small foreign ISP within 3 weeks period. Moreover, a very serious DoS attack had happened on 21 October 2002 where 7 out of 13 DNS roots servers in the world went down completely and 2 of them were unfavourably ruined (McGuire, 2003). From the examples mentioned above, it is undeniable that DoS attack is one of the most serious security breaches that causes tremendous negative effects across many fields. Although there are many researchers proposed solutions to mitigate DoS attack, their proposed solutions is not comprehensive and even increase network latency. Therefore, this project would like to provide an alternative to mitigate the effect of DoS attack without increasing network latency.

1.2. PROJECT SCOPE

At the end of this project, the deliverable will be simulation results. Based on the simulation result obtained, the intention is to prove that by implementing GLBP, impact of DoS attack could be alleviated.

To do so, first, a simulation will be conducted before implementing GLBP to show that DoS attack can be successfully launched and cause the legitimate users not able to access the web services. The figure 1-1 below shows the network topology being setup:
Assume that the interface of PC running Apache web server will be congested once it received 5000 packets and above. In the first simulation, there will be an attacker sending SYN packets continuously to the PC running Apache web server. Since the PC’s interface will receive more than 5000 packets after some time, so theoretically the interface will be congested. Should the legitimate user want to access to web services, he/she will not be able to do so as the link or path to the PC running web server is congested. This would be the anticipated simulation result obtained before implementing GLBP.

In the second simulation, GLBP will be enabled in a group of redundant routers. Then, TCP load balancing will be also configured to allow further load sharing between two mirror servers. This is an improvement from the Proposal report, as it is to avoid the server to become bottleneck of DoS attack. The figure 1-2 below shows the network topology for this second simulation:
For this round, when the attacker sending huge amount of SYN packets towards the PC running Apache web server, the packets are load balanced among the redundant routers, thus the links or path to the PC running Apache web server will not be easily congested. Then the packets will be further load balanced among the mirror servers when being forwarded to the destination. Since the links are not congested, legitimate user is still able to access web service.

By implementing GLBP, it is expected that effect of DoS attack could be mitigated. Should DoS attack still able to take down the routers, then modification or improvement on the GLBP might be done to ensure that it can mitigate DoS attack at the end.

Figure 1-2: Network topology for second simulation
CHAPTER 1: INTRODUCTION

1.3. PROJECT OBJECTIVES

There are 3 main objectives for this project. First, the main objective is to study whether DoS attack could be alleviated by implementing GLBP in redundant routers. Second, to prove that GLBP would be an alternative to mitigate various type of DoS attack using different attacking tools at the same time with lesser network latency as compared with others proposed solutions. Last, to show that GLBP is a more comprehensive and yet effective ways to mitigate DoS attack with leading to any side-effects. Each of the objective is explained further below.

The principal objective for this project is to determine whether the effect of DoS attack could be alleviated by implementing GLBP in redundant routers. Theoretically, GLBP could reduce the impact of DoS attack as its characteristic of load balancing will minimize the probability to congest a link. However, since this is a brand-new idea, there is no researcher has done that before, so this proposed solution is still under investigation. Henceforth, practical experiment or simulation will be conducted in this project to prove that DoS attack could be mitigated by GLBP.

Moreover, the second objective is to prove that by implementing GLBP, it would mitigate various type of DoS attack with less network latency. As compare with the previous solutions proposed by the researchers, such as packet filtering at router (Mahajan et. al., 2002), putting capabilities in data packets (Yang, Wetherall and Anderson, 2005), CAPTCHA mechanism (Mehra et al., 2011) and ingress filtering, all of them would increase the workload of network devices. For instance, routers need to check the filtering rules whenever received the packets to filter out unwanted packets. If the method of putting capabilities in the packets is used, then the routers need to stamp the capabilities on every single packet. These two examples proved that they are increasing the workload of the routers and lead to network latency. In some of the companies, network latency might lead to serious problem and it is not tolerable. Therefore, it is important to prove that by implementing GLBP to mitigate DoS attack, it would not further increase the network latency and it is actually a better alternative than other proposed solution. Furthermore, some of the previous proposed solutions especially CAPTCHA mechanism could only mitigate one type of DoS attack, in this case, SYN flood would be the attack. As CAPTCHA mechanism is indirectly reduce the TCP connections to the web server before the client enter the correct CAPTCHA. However, by implementing GLBP, various type of DoS attacks could be mitigated even
CHAPTER 1: INTRODUCTION

with various attacking tools like hping3 SYN flood, hping3 PING flood and Slowloris attack.

Additionally, the third objective is to prove that utilizing GLBP to mitigate DoS attack would be more comprehensive than previous works. For some of the previous works, especially using capabilities to recognize wanted packets by destination host, it leads to another threat so called Denial-of-Capability (DoC). This is because an illegitimate user might flood the link by keep on sending request for capability establishment to destination host and finally it causes DoC attack. So, this project is also to prove that GLBP will not derive other threats.

1.4. IMPACT, SIGNIFICANCE AND CONTRIBUTION

Nowadays, the number of Internet users from all over the world is large to an extent that is beyond the imagination. Just within 10 years of duration, the Internet users in world population had increased approximately by 32.8% from 16.7% in year 2006 until year 2016 (Internetworldstats, 2017). Many important transaction are done over Internet and huge number of private information is stored and transmitted over Internet as well. Therefore, network reliability and network efficiency are very essential factors for Internet users to have better and secure Internet experiences.

This project which suggest implementing GLBP to mitigate DoS attack not only provide an alternative in terms of network security, it also promises Quality-of-Services (QoS) as it has less network latency compared with other proposed solutions. As a normal Internet user, he/she could feel relieved as the private information is protected over the Internet. By mitigating DoS attack, Internet users could enjoy accessing Internet without any constraint and worry.

For companies that much utilize Internet as their main core of operation, it is needless for them to worry about leakage of clients’ information which in turn leads to loss of reputation. Besides, if DoS attack is successfully launched to the targeted company, even the services are down for few minutes, it could cause an organisation especially an e-commerce organisation losing huge amount of money. However, if the companies use the proposed solution in this project, not only DoS attack could be mitigated, the companies also can save a lot of expenditure in purchasing, implementing or maintaining network security devices like Intrusion Detection System or Intrusion Prevention System, Firewall, antivirus software and etc.
1.5. BACKGROUND INFORMATION

The dominant technology deployed in this project would be “Gateway Load Balancing Protocol” (GLBP). Using the load balancing feature among the GLBP group members, the flood of unwanted packets can be evenly distributed among the GLBP group members and thus alleviating the problem of buffer overflow in targeted network device or interface.

GLBP combines several routers to become a single GLBP virtual router group. This group of routers share a single virtual IP address that will be configured as the default gateway of the IP hosts. Once GLBP configuration is done on every member of GLBP group, they communicate with each other through hello messages sent every 3 seconds to the multicast address 224.0.0.102 and from that, one of the member’s gateway will be elected to be Active Virtual Gateway (AVG) for that group. The other routers will be remained as redundant routers until the AVG failed. These redundant routers play a role as an Active Virtual Forwarder (AVF).

AVG election is done by exchanging the hello packets among the GLBP group members and examining the priority field in the hello packets. The one with highest GLBP priority value will be elected to become AVG whereas the rest of the GLBP members would become AVFs that would assume the responsibility of AVG once the AVG has down. Should the priority values of the GLBP group members are same, then member with highest physical IP address will be elected to become the AVG. This is how the AVG election is done and GLBP group is formed.

AVG will first assign a virtual MAC address to each of the member of GLBP group including itself. This implies that, there is only one virtual IP address being shared among the member of GLBP group, but each of the member could have their own virtual MAC address. On the other hand, AVFs are responsible to forward packets that are sent to its virtual MAC address assigned to that gateway by the AVG.

When a client send an ARP request for the gateway IP address, the AVG will send ARP reply to the client which consists of information about virtual MAC address of one of the AVFs. Later if the client want to send any data, it will first forward the data to the AVF with virtual MAC address assigned by AVG. Same process applied to the second client but this time AVG will return the next virtual MAC address available to forward packets in the ARP reply to the second client (Gan, 2017). Figure 1-3 below shows the GLBP operation:
Basically, there are 3 GLBP operations which are weighted load-balancing algorithm, host-dependent load-balancing algorithm and round-robin load-balancing algorithm. In this project, round-robin load-balancing algorithm is chose as main GLBP operation. This algorithm allows all GLBP members’ MAC addresses take turns being included in ARP reply for the default gateway IP address of particular client (Gan, 2017).

Figure 1-3: GLBP operation (Gan, 2017).
CHAPTER 1: INTRODUCTION

With the technology mentioned above, the main objective and the sub-objectives are achieved as GLBP do not add extra tasks to the network devices for example to routers to analyse the packets and filter the packets unwanted as in the existing proposed solutions. GLBP do not apply packet filtering feature, it is just a predefined protocol for first hop redundancy but its load balancing feature could be utilized to mitigate effect of DoS attack. Not only that, since no packet filtering is involved, it would not affect or block the legitimate traffic to the destination host.

1.6 REPORT ORGANISATION

The contents of the report are organized as following. Chapter 2 will discuss about the proposed solutions from other researchers and determine their respective advantages and disadvantages. From that, comparison is made between the others’ proposed solutions with the solution focused in this project. Chapter 3 is to show the design specification of the proposed solution in the aspect of network topology built, the devices and the attacking tools used. The attacking plan is show as following:

1) Before and after launching SYN flood attack – compare average page load time
2) SYN flood attack after mitigation – compare average page load time before and after mitigation of SYN flood
3) PING flood attack before and after mitigation - compare average page load time before and after mitigation of PING flood
4) TCP ACK flood attack before and after mitigation – compare average page load time before and after mitigation of ACK flood
5) Slowloris attack
6) SYN flood attack with varying packets interval before and after mitigation – compare graphs plotted
7) PING flood attack with varying packets interval before and after mitigation – compare graphs plotted

In chapter 3 as well, flowchart will be included to have systematic testing flow. Implementation issues, cost analysis and timeline are presented within this chapter too. Moreover, chapter 4 will mainly show the results for each testing with screenshot provided and calculations done. A discussion section is included for Slowloris attack. Lastly, conclusion will be made based on the testing results and objectives of the project.
2.1 - EXISTING PROPOSED SOLUTIONS OVERVIEW

Denial of service attack (DoS) is performed with the intention to prevent legitimate user from accessing a particular service. As the technologies advancement grows by leap and bounds, there are more sophisticated ways to execute cyber-attacks, but yet DoS attack is still one of the cyber-attacks that is most frequently execute. This is due to the fact that it is simple to be executed and yet can achieve the purpose of taking down a service.

The impact brought by DoS attack had led to a raft of proposed solutions. According to the existing researches, the suggested ways to mitigate DoS attack are packet filtering at router (Mahajan et. al., 2002), putting capabilities in data packets (Yang, Wetherall and Anderson, 2005), CAPTCHA mechanism (Mehra et al., 2011) and ingress filtering to prevent packets with spoofed IP source address (Ferguson and Senie, 2017). The proposed solutions do mitigate DoS attack successfully but not effectively. All of the mechanisms above are extra layer of security to mitigate DoS attack. They added extra tasks to the network devices especially the router to help achieving the purpose rather than just routing task. This is one of the weaknesses of those solutions as they increase the workload of the routers. Instead, in this paper, an existing protocol so called “Gateway Load Balancing Protocol” (GLBP) is used to mitigate DoS attack. It is a protocol that secures data traffic from a down router, while allowing packet load sharing between a groups of redundant routers (Cisco, n.d.). With the load balancing feature available in GLBP, flooding packets can be evenly distributed among the redundant routers and thus avoiding DoS attack.
2.2 - PACKET FILTERING

Firstly, early research in the area of DoS sought to install signature based packet filtering at routers by defining and configuring a set of rules. These rules could be limiting the source or destination IP address, type of services like ICMP, HTTP and so on or rate of receiving the packets. When routers received the packets, they will check and match with the rules defined, if any of the rules is matched, then the routers will drop the packets, else forward the packets appropriately. This solution is good in the sense that it could solve the insidious side of the Internet that is the receivers do not have control over resources consumed on their behalf: a receiver can receive a repetitive stream of packets notwithstanding of they are not desired. Nevertheless, packet filtering like pushback (Mahajan et. al., 2002) might possible to block some of the traffic from legitimate users as there is not clear cut to distinguish between attackers’ traffic and legitimate users’ traffic. This happened as the attackers could create packets with contents of their choosing. In this paper, attempt not to block the legitimate users’ traffic could be done by not implementing packet filtering at the routers.

2.3 - CAPABILITY

Secondly, some researchers had advocated putting a capability in every data packets that is to be checked by the routers to verify that a packet is a wanted packet by the destination and giving them preferential service. In Traffic Validation Architecture (TVA) (Yang, Wetherall and Anderson, 2005), a sender will first send a request to destination for capability before sending packets. The destination host grants the capability to the sender and the requested capability is stamped on the packets before sending out by the sender. Then, routers received the packets must identify capability without trusting the hosts foremost. Last, if the communication is done, destination host no longer want to receive any packets from the sender, the capability will be expired. Figure below shows how the capability being added into packets in TVA:
The advantage of this capability is that a destination host will not lose connectivity due to a flood of unwanted packets. All the unwanted packets (without the capability stamped) will be discarded by the routers before they reach a congested link during capability verification. Only wanted and trusted packets (with capability stamped) are received. Thus, DoS attack is mitigated. Nonetheless, a malicious user might still take down another host by flooding requests to the destination for the capability establishment. This in turn causes Denial of Capability (DoC) attack (Fu, 2011, p.1). In this paper, the proposed solution to mitigate DoS attack will eliminate capability feature. This is because GLBP will load sharing the packets no matter they are wanted or unwanted among the redundant routers to alleviate the effect of DoS attack. Therefore, it is needless to distinguish wanted packets and unwanted packets.
CHAPTER 2: LITERATURE REVIEW

2.4 - CAPTCHA MECHANISM

Aside from that, there is another approach to mitigate DoS attack, which is by CATPCHA mechanism. CATPCHA mechanism is used to identify human-generated web traffic and distinguish it from robot-generated traffic. With that information, policies can be implemented such as limiting the number of fake request sent. In most of the website, CAPTCHA is verified at the first login attempt or after few failed logins. Overhead is needed to send username, password and CAPTCHA together over the Internet to the server for authentication purpose. Every single login request consume the resource or capacity (buffer) of the server as the size of the request is large. Due to that, attackers could take advantage of this method. Henceforth, Mehra suggested that the CAPTCHA should be verified before accessing to the login page. By doing so, the process of re-verifying user credentials on each fake request is reduced to only CAPTCHA verification (Mehra et al., 2011). This is due to the fact that only human can read and understand the CAPTCHA but robots are not able to decipher the CAPTCHA, thus they are not allowed to access the login page. It could be said without the fear of contradiction that this solution successfully limits the attackers to use botnets to execute DoS attack. Unfortunately, DoS attack is not only limited to login request any other type of packets could make the server’s buffer overflow. CAPTCHA mechanism only limited the size of every login request but what if the attackers successfully login the website and submit other type of request like make payment request to the server, the attackers still can create a lots of make payment requests to flood the server. Hence, it is not a comprehensive way to mitigate DoS attack. In this paper, the suggested solution do not encounter such problem as redundant routers with GLBP-enabled will load balance any kind of requests among them so that the requests would not overflow a host’s buffer. Figures below show CAPTCHA is verified in the login page and CAPTCHA is verified before accessing to login page:
CHAPTER 2: LITERATURE REVIEW

Figure 2-2: Login page with CAPTCHA verification included (Elias, 2009)

Figure 2-3: CATPCHA verification before accessing to login page (Know Your Meme, n.d.)

2.5 - INGRESS FILTERING

Previous research found that ingress filtering is feasible to mitigate DoS attack as well. Ingress filtering is a technique used to ensure that incoming packets are actually from the networks from which they claim to originate. This prevents the spoofing of IP addresses in DoS attack by defining rules on point of entry routers that limit source addresses to a known range. The router will first check the source IP field of IP packets it received, and dropped packets if the packets don't have an IP address in known range (Ferguson and Senie, 2017). This solution could mitigate DoS attack not in a comprehensive way. This is due to the light of the fact that when an end host is multi-homed which means it is connected to more than one networks, then the attackers from unknown network can choose to send out the packet via the network that is known by the ingress-filtering-enabled-router(What is INGRESS FILTERING? What does INGRESS FILTERING mean? INGRESS FILTERING meaning & explanation, 2017). With that the attacker can bypass the ingress filtering. Hence, in this paper, to avoid
CHAPTER 2: LITERATURE REVIEW

this security breach, the proposed solution would not consider to include ingress filtering.

In summary, the existing proposed DoS attack mitigation have their respective advantages and it is undeniable that they can solve DoS problem but unfortunately not in a comprehensive and efficient way. Most of the proposed solution added extra tasks to the routers to examine the packets which in fact, increased the workload of the routers and might cause network latency. In this paper, the proposed solution could provide a simpler, more comprehensive and yet effective approach to mitigate DoS attack which implementing the existing protocol so called “Gateway Load Balancing Protocol”. Further restriction is given to the solution so that it might be pragmatically deployed in today’s technology.
CHAPTER 3: PROPOSED METHOD/APPROACH

Chapter 3: PROPOSED METHOD/APPROACH

3.1 DESIGN SPECIFICATIONS

This project has two main simulations and three additional researches. The first simulation is to simulate that DoS attack could successfully be launched to the PC running with Apache web server without implementing GLBP. The network topology is setup as shown below:

![Network topology for first simulation](image)

**Figure 3-1: Network topology for first simulation**

The devices needed to build the network topology for the first simulation are 2 PCs, 2 Ethernet switches and 1 Cisco router. The attacker’s PC is running Kali Linux whereas the PC with Apache web server is running on Windows 10. To link the devices together, forming a Local Area Network (LAN), 4 straight-through cables are needed. Software so called “Putty” is needed in order to telnet into the router for configuration. After all, DoS attack specifically SYN flood will be launched from the attacker’s PC towards the targeted PC running Apache web server. To do so, a command-line oriented TCP/IP packet generator must be installed on attacker’s PC (blackMORE Ops, 2015). In the command prompt, type the command “`apt-get install hping3`” in bid to install hping3. Then the command to launched DoS attack is

```
hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source IP_PC_with_Apache_webserver
```

*Note: Please replace “IP_PC_with_Apache_webserver” above to IP address of the targeted PC.*
CHAPTER 3: PROPOSED METHOD/APPROACH

Explanation of the command is as follow:

- **hping3** – Application binary’s name
- **-c 10000** – Number of packets to be sent to target
- **-d 120** – Size of every packet to be sent
- **-S** – SYN flood is specified here
- **-w 64** – windows TCP size which default value is 64
- **-p 80** – destination port number (i.e. 80 for HTTP)
- **--flood** – sending packet in flood mode without showing incoming replies
- **--rand-source** – using random IP addresses to sent the SYN packets
- **IP_PC_with_Apache_webserver** – victim’s IP address

Plugin will be installed on the web browser from the legitimate users’ PC to record the average page load time before and after launching the SYN flood attack. It is suggested to use “Page Load Time” plugin for Chrome and “Page Speed Monitor” plugin for Firefox Mozilla.

In the next simulation which is the main objective of this project – to study whether by implementing GLBP could alleviate DoS attack. GLBP is implemented in a group of redundant routers. First and foremost, network topology was built as shown in figure below:
In this second simulation will implement GLBP in two redundant Cisco routers. One PCs will run the Apache web server. Then two Ethernet switches are needed as well. The attacker which running Kali Linux OS will again perform SYN flood attack towards the IP address of the web server. The configuration is as shown in table below:

<table>
<thead>
<tr>
<th>Gateway for hosts in network 192.168.0.0/24:</th>
<th>Virtual IP address of redundant routers- 192.168.254</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway for hosts in network 192.168.2.0/24:</td>
<td>Virtual IP address of redundant routers- 192.168.2.254</td>
</tr>
<tr>
<td>IP address of attacker:</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td>IP address of legitimate user:</td>
<td>192.168.1.2/24</td>
</tr>
<tr>
<td>IP address of PC running Apache web server:</td>
<td>192.168.2.1/24</td>
</tr>
<tr>
<td>Actual IP address of interface fa0/1 of router 1:</td>
<td>192.168.1.222/24</td>
</tr>
<tr>
<td>Actual IP address of interface fa0/1 of router 2:</td>
<td>192.168.1.233/24</td>
</tr>
<tr>
<td>Actual IP address of interface fa0/0 of router 1:</td>
<td>192.168.2.222/24</td>
</tr>
<tr>
<td>Actual IP address of interface fa0/0 of router 2:</td>
<td>192.168.2.233/24</td>
</tr>
</tbody>
</table>

Table 3-1: Table for the network configuration with GLBP implemented

After SYN flood attack, average page load time will be recorded too.
3.2 EVALUATING PLAN FOR PERFORMANCE OF GLBP IN MITIGATING SYN FLOOD ATTACK

The system performance metric chosen is the page load time. The longer the page load time indicates the greater the effect of DoS attack. To verify that after the SYN flood attack, the resource in web server is overconsumed and the page load time becomes longer, plugin must be installed on the web browser as mentioned before. In the first simulation, the page load time before launching SYN flood attack and the page load time after launching SYN flood attack is compared to compute the difference between two situations (i.e. before and after SYN flood attack).

\[
\text{Difference} = |\text{Page Load Time}_{\text{after-syn}} - \text{Page Load Time}_{\text{before-syn}}|
\]

If the difference is in positive number and is very large then it indicates that DoS attack is successfully launched and detected, else if it is negative number or is not significant, then it indicates that DoS attack is not launched successfully. It is necessary to modify the GLBP parameter so that the attack can be launched successfully to take down the web server.

In the second simulation, the page load time after implementing GLBP during SYN flood attack is launched will be recorded too. Ultimately, the average page load time from both before and after mitigation of SYN flood attack will be compared. If the result after mitigation is shorter than the result from before mitigation, it proves that GLBP can mitigate the effect of SYN flood attack successfully.

3.3 MITIGATION OF ADDITIONAL TYPE OF DoS ATTACKS

To further proving the second objective which is GLBP could mitigate different type of DoS attack, another attacks will be launched which are PING flood attack, TCP ACK flood and Slowloris. For PING flood attack, the network topology will be same as before and after mitigation of SYN flood attack just that the target will not be the IP address of web server any longer but the gateway IP address. Firstly, the attack will have constant variable of attacking duration which lasts 15s. The attacking command (run in Kali Linux terminal) is:

```
hping3 --icmp --flood gateway_IP_Address
```

*Note: Please replace “gateway_IP_Address” above to gateway IP address of the attacking network. In this case, it is 192.168.1.254.
CHAPTER 3: PROPOSED METHOD/APPROACH

Explanation of the command is as follow:

- hping3 – Application binary’s name
- --icmp – to send ICMP echo request packets
- --flood – sending packets as fast as possible without showing incoming replies
- gateway_IP_Address – gateway IP address of the attacking network.

Repeat the attack for 5 times to get the average page load time before and after implementing GLBP.

$$\text{Difference} = |\text{Page Load Time}_{\text{after-GLBP-ping}} - \text{Page Load Time}_{\text{before-GLBP-ping}}|$$

If the mitigation by GLBP is successful, then the difference should have negative value as the page load time after implementing GLBP will be smaller than that of before implementing GLBP.

To launch ACK flood attack, just modify the command to the following:

```
hping3 -d 120 -A -w 64 -p 80 --flood --rand-source IP_PC_with_Apache_webserver
```

“-A” here indicates ACK flood attack. Repeat the attack for 5 times to get the average page load time before and after mitigation of ACK flood attack.

$$\text{Difference} = |\text{Page Load Time}_{\text{after-GLBP-ACK}} - \text{Page Load Time}_{\text{before-GLBP-ACK}}|$$

Similarly, if the mitigation by GLBP is successful, then the difference should have negative value as the page load time after implementing GLBP will be smaller than that of before implementing GLBP.

Another attack would be carry out is Slowloris, to determine whether GLBP could mitigate this attack. The plan to test is that the number of connections will be increased from 1000 until 10000 with 1000 of increment. Later, it is determine at how many connections will cause the mitigation to be failed.

Last but not least, it is also important to observe the impact of DoS attack when the rate of packets sent is increased. For SYN flood and PING flood attack, the packets interval will gradually increase from interval of 1µs, 10µs, 100µs, 1000µs, 10000µs and 100000µs. Each of the packet rate will last for 10s and to collect the corresponding page load time. Graphs will be plotted to compare page load time before and after implementing GLBP. The command for SYN flood attack with varying packets interval is:

```
hping3 -d 120 -S -w 64 -p 80 -i u10000 --rand-source IP_PC_with_Apache_webserver
```
CHAPTER 3: PROPOSED METHOD/APPROACH

Where the –c 10000 is removed so that as many packets sent as possible but not limited to 10000 SYN packet. Furthermore, -i here is to define the packets sent interval and u10000 indicates there will be 10SYN packets sent out per second (Sanfilippo, n.d.). In this case, the packets sent interval will change from 1µs, 10µs, 100µs, 1000µs, 10000µs and 100000µs. Each different packets interval will last for 10s of attacking duration. Whereas the command for PING flood attack with varying packets interval is:

```
hping3 --icmp --i u10000 gateway_IP_Address
```

Similar to the SYN flood attack above, the packets interval will varies from 1µs, 10µs, 100µs, 1000µs, 10000µs and 100000µs.
CHAPTER 3: PROPOSED METHOD/APPROACH

3.4 SYSTEM DESIGN / OVERVIEW

There is a set of standard work flow when carrying out the first simulation as shown in Figure 3-3 above. This is to ensure that the working process is systematic and traceable when there are some problems encountered. The first step will be building up the network topology. The figure below shows the network topology setup in the practical lab.

Figure 3-3: Flowchart for SYN flood attack before GLBP
CHAPTER 3: PROPOSED METHOD/APPROACH

Figure 3-4: Network built for first simulation in Practical Lab

After network topology is done building, it is necessary to check the connectivity of every device or interface in the LAN. To do so, every device must execute ping command to test for the connectivity, for example “ping 192.168.1.1”. If there is one host is unreachable, network topology must be rebuilt or reconfigured especially the IP addresses and IP gateways. If there is no problem for the connectivity, the next step will be accessing the website by using web browser from attacker’s PC before launching DoS attack. If the website could not be accessed, configurations must be reviewed. Else, if the website is successfully accessed, then the average page load time must be recorded by opening the website repeatedly for 5 times. To record the page load time, adds-on or plugin must be installed on the web browser.

The following step will be launching SYN flood attack towards PC running Apache web server. After launching DoS attack which is SYN flood attack, from the attacker’s PC, access to the website again. If the website can be accessed as normal before SYN flood attack is launched, then it is necessary to modify the hping3 command or change to another DoS attack command. Otherwise, the average page load time is recorded by opening the same webpage repeatedly for 5 times. The last step would be comparing the difference between the page load time before and after the SYN flood attack.
The flow chart for the SYN flood attack after GLBP will be almost the same as the SYN flood attack before mitigation. The major differences are that network topology will be distinct. Consequently, after LAN is built up, the next step will be implementing GLBP in the redundant routers. The average page load time before launching SYN flood attack is needless in this simulation but the average page load time after launching SYN flood attack is still necessary. Ultimately, compare the average page load time after launching SYN flood attack in the second simulation with that of the first simulation. If the result from second simulation is shorter than that of first simulation, it implies that GLBP does can mitigate DoS attack. Otherwise, modify the GLBP parameter and re-implement the modified GLBP in the redundant routers.
In order to proving that by implementing GLBP, PING flood attack also could be mitigate, firstly, set up the network exactly same as the network topology in SYN flood attack (before GLBP implemented). This round, collect the page load time of website in 5 times after PING flood attack is launched. Calculate the average page load time when PING flood is launching.
Later on, launch again the PING flood attack but this round GLBP is implemented in redundant routers. Access to the website in 5 times and record the page load time for each time. Calculate the average page load time after GLBP is implemented. Then, compare the average page load time before and after implementing GLBP for PING flood attack. If the difference is negative value, it shows that mitigating PING flood attack is successfully done by implementing GLBP. Otherwise, revise the GLBP parameter and start over the attack until mitigation successes.

Figure 3-7: Flowchart for PING flood attack after GLBP
CHAPTER 3: PROPOSED METHOD/APPROACH

Figure 3-8: Flowchart for ACK flood attack before GLBP
Average page load time is recorded before mitigation of ACK flood attack.

Figure 3-9: Flowchart for ACK flood attack after GLBP
Average page load time after mitigation of ACK flood attack is recorded and compared with that of before mitigation.
Figure 3-10: Flow chart for launching Slowloris attack

Figure above showed the way to launch Slowloris attack. Since after the Slowloris attack, the website will not able to be loaded, it is not possible to calculate the average page load time. Thus, if before mitigation, the website cannot be accessed and after mitigation, the website can be accessed, then it actually indicates that mitigation of Slowloris attack is successful by implementing GLBP. Furthermore, the number of packets sent will be manipulated to further determine the threshold whereby the proposed solution is no longer effective. The range of number of connections is from 1000 to 10000 with each round runs for 10s of attacking duration.
Figure 3-11: Flowchart of varying the packets sent interval before GLBP

To show that when packet sent interval is shorter, the impact of DoS attack will be more serious and the page load time will be longer, the SYN and PING flood attack are repeated with packets interval 1µs, 10µs, 100µs, 1000µs, 10000µs and 100000µs. Record the corresponding page load time and plot a graph.
After implementing GLBP, it is the time to prove that the mitigation is succeed. Thus, record the corresponding page load time when packets sent interval varies from 1µs to 100000µs. The graphs of before and after mitigation with varying packets sent interval are plotted and compared.
CHAPTER 3: PROPOSED METHOD/APPROACH

3.5 IMPLEMENTATION ISSUES AND CHALLENGES

It is undeniable that the major challenge in this first simulation is to find the most suitable and workable command to launch DoS attack. Some of the commands available on the websites are not workable in Kali Linux.

Later on, when the most likely workable command had been found, it needs some times to understand what the meaning of the options in the command are. Deciding the number of packets to send, size of packet to send and the rate to send the packets will be the crucial factors to determine the success or failure of the DoS attack. It is time consuming to try every commands found and available and to further understand about the commands. Manipulating the packets sent interval, attacking duration to collect the corresponding page load time is also tedious.

3.6 COST ANALYSIS

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Service</th>
<th>Price (MYR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate – 100E (Asashi, 2017)</td>
<td>Packet Filtering/Ingress Filtering</td>
<td>11310.00</td>
</tr>
<tr>
<td>Cisco Router 1841 (x2) (itprice, 2018)</td>
<td>GLBP</td>
<td>6558.00</td>
</tr>
</tbody>
</table>

Table 3-2: Table for cost analysis
3.7 TIMELINE

This project will be divided into two parts which are the first simulation simulating the DoS attack before implementing GLBP and second simulation simulating the DoS attack after implementing GLBP.

In previous semester, the first simulation which is demonstrating DoS attack before implementing GLBP will be carried out. The first week of this semester, application for the time slot using the practical lab will be submitted to the lab instructor. Next two weeks will be building up the network topology and to ensure connectivity for every device and interface in the LAN. Start from week 4 and onwards, time will be taken to find the workable DoS attack command to launch DoS attack via trial and error. This will take around 1.5 weeks because it is important to understand the options in the command and manipulate the options to ensure DoS attack is successfully launched. Week 6 onwards, the average page load time will be computed before and after the DoS attack. Graph will be plotted. It is estimated that the draft report would be submitted to the supervisor to check for the content on week 9. Further enhancement would be carried out from week 10 to week 11 and lastly full report will be submitted by before week 13. The schedule is illustrated in the Gantt chart below.
Figure 3-13: Gantt chart for current semester
CHAPTER 3: PROPOSED METHOD/APPROACH

In this semester, second simulation which is demonstrating mitigation of DoS attack after implementing GLBP is carried out. The first will be booking the timeslot for conducting the simulation in practical lab. Second week to third week will be building up the network topology, setup Apache web server, check for connectivity and implementing GLBP. The forth week is going to launch DoS attack and modify the GLBP parameters until DoS attack is mitigated by GLBP. The next week will be collecting results from the simulation especially the average page load time and plot the graph. Second Final Year Project draft report will be started from week 7 to week 9 and submit to the supervisor to check the content level. Further improvement will be carried out along week 10 to week 12. The schedule is illustrated in the Gantt chart below on the next page.
Figure 3-14: Gantt chart for future semester
4.1 SYN FLOOD ATTACK

To verify that DoS attack is launched successfully in the first simulation, page load time before and after the attack is recorded. Figure below show the page load time of the website hosted by the Apache web server before DoS attack. To get the average, 5 tabs were opened and access to the website respectively.

Figure 4-1: Page Load Time for first tab is 289ms (SYN flood)

Figure 4-2: Page Load Time for second tab is 120ms (SYN flood)

Figure 4-3: Page Load Time for third tab is 117ms (SYN flood)

Figure 4-4: Page Load Time for forth tab is 97ms (SYN flood)

Figure 4-5: Page Load Time for fifth tab is 106ms (SYN flood)
CHAPTER 4: TESTING RESULTS

From figure 4-1 to figure 4-5 the page load time are 289ms, 120ms, 117ms, 97ms, and 106ms respectively. The average of the page load time before DoS attack is:

\[
\text{Average page load time} = \frac{289 + 120 + 117 + 97 + 106}{5} \\
= \frac{729}{5} \\
= 145.8\text{ms} \\
= 0.1458\text{s}
\]

However, after the DoS attack launched, the page get longer time to be displayed. The page load time for the respective five tabs to display the page is as shown in the figure below.

Figure 4-6: Page Load Time for first tab after SYN flood attack is 10.65s

Figure 4-7: Page Load Time for second tab after SYN flood attack is 29.21s

Figure 4-8: Page Load Time for third tab after SYN flood attack is 28.02s

Figure 4-9: Page Load Time for forth tab after SYN flood attack is 27.45s
CHAPTER 4: TESTING RESULTS

Figure 4-10: Page Load Time for fifth tab after SYN flood attack is 26.73s

The average of the page load time after DoS attack is:

\[
\text{Average page load time (after-SYN)} = \frac{10.65 + 29.21 + 28.02 + 27.45 + 26.73}{5} \\
= \frac{122.06}{5} \\
= 24.41 \text{s}
\]

To compute the difference between the page load time before and after DoS attack, here is the step:

\[
\text{Difference} = |\text{Average Page Load Time (after-SYN)} - \text{Average Page Load Time (before-SYN)}| \\
= |24.41 - 0.1458| \\
= 24.26 \text{s}
\]

The difference page load time before and after DoS attack is 24.26s which is positive, indicating that page loads is 24.26s longer than that of after DoS attack. Besides, the page load time \( (\text{after-SYN}) \) is 16742.1 times slower than average page load time \( (\text{before-SYN}) \) which is very large difference between them.

Moreover, it is also advisable to examine on the ping reply time for the user to ping the PC running Apache web server before and after DoS attack. The figure below shows that the command to launch SYN flood attack and the time for user to ping PC with Apache web server before and after the attack being launched.
CHAPTER 4: TESTING RESULTS

Let’s take 5 ping replies time and compute the average of ping reply time before and after DoS attack to the PC running Apache web server. The working steps are as following:

\[
\text{Average ping reply time(before)} = \frac{0.781 + 0.937 + 0.937 + 0.930 + 0.833}{5} = 0.884 \text{ ms}
\]

\[
\text{Average ping reply time(after)} = \frac{4.90 + 5.02 + 4.32 + 3.72 + 4.04}{5} = 4.400 \text{ ms}
\]

Difference = |Average ping reply time(after) – Average ping reply time(before)|

= |4.400 ms – 0.884 ms|

= 3.516 ms

Ratio of Average ping reply time(after) to Average ping reply time(before)

\[
= \frac{4.400}{0.884} = 497.74
\]

From the calculation, it is obvious that the average ping reply time after SYN flood attack is much higher than that of average ping reply time before SYN flood attack by the difference (before modulus) of 3.516ms. Besides, the average ping reply time (after) is around 497.74 slower than average ping reply time(before) which is also considered a huge gap between them.
CHAPTER 4: TESTING RESULTS

Since the difference is positive number and it is considered very large difference, thus it could be said without the fear of contradiction that SYN attack is launched successfully on the PC running Apache web server.

After mitigation of SYN flood attack by implementing GLBP, the corresponding average page load time had been obtained:

Figure 4-12: Page Load Time for first tab after mitigation of SYN flood attack is 1.14s

Figure 4-13: Page Load Time for second tab after mitigation of SYN flood attack is 1.18s

Figure 4-14: Page Load Time for third tab after mitigation of SYN flood attack is 185ms

Figure 4-15: Page Load Time for forth tab after mitigation of SYN flood attack is 172ms
CHAPTER 4: TESTING RESULTS

Figure 4-16: Page Load Time for fifth tab after mitigation of SYN flood attack is 181ms

The average of the page load time after mitigation of SYN flood attack is:

\[
\text{Average page load time}_{\text{(after-SYN)}} = \frac{(1.14+1.18+0.185+0.172+0.181)}{5} = 0.572s
\]

The difference between the average page load time before and after mitigation of SYN flood attack is:

\[
\text{Difference} = \left | \frac{\text{Average Page Load Time}_{\text{(after-GLBP-SYN)}} - \text{Average Page Load Time}_{\text{(before-GLBP-SYN)}}}{\text{Average Page Load Time}_{\text{(before-GLBP-SYN)}}} \right |
\]

\[
= \left | \frac{0.572 - 24.41}{24.41} \right | = 23.84s
\]

The difference (before modulus) page load time before and after mitigation of SYN flood attack by implementing GLBP is -23.84s which is negative. It implies that after implementing GLBP to mitigate SYN flood attack, the page load time is 23.84s much faster before mitigation. Besides, the average page load time \(\text{after-GLBP-SYN} \) is 2.34 times relatively shorter than that of before mitigation. Thus, it could be said without the fear of contradiction that, mitigation of SYN flood attack is successful by implementing GLBP.
4.2 PING FLOOD ATTACK

The results of PING flood attack before mitigation are showed as the figures below:

Figure 4-17: Page load time of first tab before mitigation of PING flood attack is 510ms

Figure 4-18: Page load time of 2nd tab before mitigation of PING flood attack is 3244ms
CHAPTER 4: TESTING RESULTS

Figure 4-19: Page load time of 3rd tab before mitigation of PING flood attack is 508ms

Figure 4-20: Page load time of 4th tab before mitigation of PING flood attack is 3222ms

Figure 4-21: Page load time of 5th tab before mitigation of PING flood attack is 478ms

The average page load time before mitigation of PING flood attack is:

\[
\text{Average page load time} = \frac{0.510 + 3.244 + 0.508 + 3.222 + 0.478}{5}
\]
CHAPTER 4: TESTING RESULTS

=7.962/5
=1.592s

Subsequently, GLBP is implemented to mitigate PING flood attack and the figures below show the page load time after mitigation:

Figure 4-22: Page load time of 1st tab after mitigation of PING flood attack is 188ms

Figure 4-23: Page load time of 2nd tab after mitigation of PING flood attack is 176ms

Figure 4-24: Page load time of 3rd tab after mitigation of PING flood attack is 166ms
CHAPTER 4: TESTING RESULTS

Figure 4-25: Page load time of 4th tab after mitigation of PING flood attack is 204ms

Figure 4-26: Page load time of 5th tab after mitigation of PING flood attack is 196ms

The average page load time after mitigation of PING flood attack is:

\[
\text{Average page load time}_{\text{(after-GLBP-PING)}} = \frac{(0.188 + 0.176 + 0.166 + 0.204 + 0.196)}{5} = \frac{0.93}{5} = 0.186 \text{s}
\]

The difference between the average page load time before and after mitigation of PING flood attack is:

\[
\text{Difference} = |\text{Average Page Load Time}_{\text{(after-GLBP-PING)}} - \text{Average Page Load Time}_{\text{(before-GLBP-PING)}}| \\
= |0.186 - 1.592| \\
= 1.406 \\
= 1.406 \text{s}
\]

The ratio of page load time after mitigation of PING flood attack to average page load time before mitigation of PING flood attack is:

\[
\text{Ratio} = \frac{(0.186/1.592)}{\text{Average Page Load Time}_{\text{(before-GLBP-PING)}}} = 11.68 \#
\]
CHAPTER 4: TESTING RESULTS

The difference (before modulus) page load time before and after mitigation of PING flood attack by implementing GLBP is -1.406s which is negative. It implies that after implementing GLBP to mitigate PING flood attack, the page load time is 1.406s faster than before mitigation. Besides, average page load time\textsubscript{(after-GLBP-PING)} is 11.68 times shorter than average page load time\textsubscript{(before-GLBP-PING)}. Thus, it could be said without the fear of contradiction that, mitigation of PING flood attack is successful by implementing GLBP.

4.3 ACK FLOOD ATTACK

Figures below are the page load time before mitigation of ACK flood attack:

Figure 4-27: Page load time before mitigation of ACK flood attack for 1\textsuperscript{st} tab is 600ms

Figure 4-28: Page load time before mitigation of ACK flood attack for 2\textsuperscript{nd} tab is 1950ms
CHAPTER 4: TESTING RESULTS

Figure 4-29: Page load time before mitigation of ACK flood attack for 3\textsuperscript{rd} tab is 1306ms

Figure 4-30: Page load time before mitigation of ACK flood attack for 4\textsuperscript{th} tab is 2736ms

Figure 4-31: Page load time before mitigation of ACK flood attack for 5\textsuperscript{th} tab is 6198ms
CHAPTER 4: TESTING RESULTS

The average page load time before mitigation of ACK flood is:

\[
\text{Average page load time (before-GLBP-ACK)} = \frac{(0.6+1.95+1.306+2.736+6.198)}{5} \\
= \frac{12.79}{5} \\
= 2.558 \text{s}
\]

Subsequent figures are the page load time collected after mitigation of ACK flood attack:

Figure 4-32: Page load time after mitigation of ACK flood attack for 1st tab is 180ms

Figure 4-33: Page load time after mitigation of ACK flood attack for 2nd tab is 188ms
CHAPTER 4: TESTING RESULTS

Figure 4-34: Page load time after mitigation of ACK flood attack for 3rd tab is 178ms

Figure 4-35: Page load time after mitigation of ACK flood attack for 4th tab is 204ms

Figure 4-36: Page load time after mitigation of ACK flood attack for 5th tab is 172ms

Average page load time after mitigation of ACK flood is:
CHAPTER 4: TESTING RESULTS

Average page load time \(_{(after-GLBP-ACK)}\) = \(\frac{(0.180+0.188+0.178+0.204+60.172)}{5}\)

\[= 0.922/5\]

\[= 0.1844s\]

Difference between average page load time before and after mitigation of ACK flood attack is:

\[\text{Difference} = |\text{Average Page Load Time\( (after-GLBP-ACK)\)} - \text{Average Page Load Time\( (before-GLBP-ACK)\)}|\]

\[= |0.1844s - 2.558s|\]

\[= |2.3736|\]

\[= 2.3736s\]

Ratio of Page Load Time\( (after-GLBP-ACK)\) to Average Page Load Time\( (before-GLBP-ACK)\)

\[= \frac{0.1844}{2.558}\]

\[= 7.21\]

In short, mitigation of ACK flood attack I successfully as the average page load time after mitigation is shorter than that of before mitigation. The negative value in the difference (before modulus) best describe that mitigation is successful by implementing GLBP. The average page load time after mitigation is 2.3736s and 7.21 times faster than that of before mitigation.

4.4 Additional research results

Figures below are the corresponding page load time with different packet interval.

![Figure 4-37: Page load time when u1 as packets interval in SYN flood attack (Before GLBP)](image)

In short, mitigation of ACK flood attack I successfully as the average page load time after mitigation is shorter than that of before mitigation. The negative value in the difference (before modulus) best describe that mitigation is successful by implementing GLBP. The average page load time after mitigation is 2.3736s and 7.21 times faster than that of before mitigation.
CHAPTER 4: TESTING RESULTS

Figure 4-38: Page load time when u10 as packets interval in SYN flood attack (Before GLBP)

Figure 4-39: Page load time when u100 as packets interval in SYN flood attack (Before GLBP)

Figure 4-40: Page load time when u1000 as packets interval in SYN flood attack (Before GLBP)
CHAPTER 4: TESTING RESULTS

Figure 4-41: Page load time when u10000 as packets interval in SYN flood attack (Before GLBP)

Figure 4-42: Page load time when u100000 as packets interval in SYN flood attack (Before GLBP)

To prove that the page load time will increase when the packets sent interval decreases, the graph for SYN and PING flood attack (before implementing GLBP) is plotted based on the page load time collected above:
CHAPTER 4: TESTING RESULTS

Figure 4-43: Graph of page load time with SYN flood packets interval varies (Before GLBP)

From the graph above, it can be said that when the packets interval decreases, the page load time is longer. This is due to the reason that more SYN packets are sent within short interval, hence the web server’s resource will be consumed faster and more difficult to process next request.
The reason why there is a huge increase in page load time when packets interval decreases from 1000μs to 100μs is because the amount of packets sent had increased tremendously to 75639 from 9718. As specified in the attacking command each of the packets have data size of 120 byte with 40 byte of headers, total will have 12102240 bytes (65639 x 160). Henceforth, Apache web server’s resource had been occupied by these much bytes of requests. But when packets interval is 1000μs, the web server still able to cater 9718 of request packets, thus the website can be retrieved as fast as normal situation. From here, it is determined that the best packets interval to launch SYN flood attack with each packet size of 120 bytes is 100μs.

Subsequently, after mitigation of SYN flood attack, the graph is plotted together with that before mitigation to make comparison. The figures below is the page load time after mitigation:
CHAPTER 4: TESTING RESULTS

Figure 4-45: Page load time when u1 as packets interval in SYN flood attack (After GLBP)

Figure 4-46: Page load time when u10 as packets interval in SYN flood attack (After GLBP)

Figure 4-47: Page load time when u100 as packets interval in SYN flood attack (After GLBP)
CHAPTER 4: TESTING RESULTS

Figure 4-48: Page load time when u1000 as packets interval in SYN flood attack (After GLBP)

Figure 4-49: Page load time when u10000 as packets interval in SYN flood attack (After GLBP)

Figure 4-50: Page load time when u100000 as packets interval in SYN flood attack (After GLBP)
CHAPTER 4: TESTING RESULTS

Figure 4-51: Graph of page load time with SYN flood packets interval varies (After GLBP)

Generally, the graph above shows the page load time after mitigation of SYN flood attack with varying packets sent interval. The page load time is said to be increasing as the packets sent interval is decreasing same as before mitigation. This is due to the concept that when packets sent interval is shorter, more packets are sent to the victim web server, thus more resource is occupied and barely can serve the next request causing longer page load time.

Figure 4-52: Graph of page load time with SYN flood packets interval varies (Before and After GLBP)
CHAPTER 4: TESTING RESULTS

The graph above combined graphs before and after mitigation of SYN flood attack to have a contrast. It is obvious that even though the packets sent interval become shorter, however, the page load time after mitigation of SYN flood attack with GLBP is relatively uniform and much faster than the page load time before mitigation. It proved that no matter under what packets sent interval, implementing GLBP could mitigate SYN flood attack effectively and allow clients to have smooth web browsing experience without realizing the impact of SYN flood attack.

Next attack is PING flood attack. The figures below are the page load time of corresponding packets interval before mitigation:

Figure 4-53: Page load time when u1 as packets interval in PING flood attack (Before GLBP)

Figure 4-54: Page load time when u10 as packets interval in PING flood attack (Before GLBP)
CHAPTER 4: TESTING RESULTS

Figure 4-55: Page load time when u100 as packets interval in PING flood attack (Before GLBP)

Figure 4-56: Page load time when u1000 as packets interval in PING flood attack (Before GLBP)

Figure 4-57: Page load time when u10000 as packets interval in PING flood attack (Before GLBP)
CHAPTER 4: TESTING RESULTS

Figure 4-58: Page load time when u100000 as packets interval in PING flood attack (Before GLBP)

Figure 4-59: Graph of page load time with PING flood packets interval varies (Before GLBP)

Same concept applied to PING flood attack, when ICMP packets sent interval become shorter, the page load time will increases. From figure above, it is be said that the page load time is generally increasing as the packets interval decreases. Let’s compare the page load time after mitigation of PING flood attack in varying packets interval. Below are the figures that shows the corresponding page load time after mitigation:
CHAPTER 4: TESTING RESULTS

Figure 4-60: Page load time when u1 as packets interval in PING flood attack (After GLBP)

Figure 4-61: Page load time when u10 as packets interval in PING flood attack (After GLBP)

Figure 4-62: Page load time when u100 as packets interval in PING flood attack (After GLBP)
CHAPTER 4: TESTING RESULTS

Figure 4-63: Page load time when u1000 as packets interval in PING flood attack (After GLBP)

Figure 4-64: Page load time when u10000 as packets interval in PING flood attack (After GLBP)

Figure 4-65: Page load time when u100000 as packets interval in PING flood attack (After GLBP)
CHAPTER 4: TESTING RESULTS

The trend line in the graph above clearly indicates that when packets sent interval increases, the page load time become shorter.

Figure 4-66: Graph of page load time with PING flood packets interval varies (After GLBP)

Figure 4-67: Graph of page load time with SYN flood packets interval varies (Before and After GLBP)
Combining both graphs before and after mitigation of PING flood attack with varying packets sent interval further give prominence to the effectiveness of mitigating PING flood attack even though the PING flood is launched with different packets interval. This is due to the light of the fact that, from the graph above, the page load time in different packets interval after mitigation is generally lower than that of before mitigation. This again proved that implementing GLBP can mitigate PING attack even in wide range of packets sent interval.

4.5 DISCUSSION FOR SLOWLORIS ATTACK

The mitigation of Slowloris attack is not successful. This is due to the reasons that Slowloris attack takes the server down by opening many connections via sending the partial-completed HTTP GET request header to the server.

```
GET /Index.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500
Accept: */*
```

Figure 4-68: HTTP GET header

From the figure above, the Carriage Return Line Feed (CRLF) is used to indicate new fresh line in the HTTP GET header. At the end of the header, two CRLF are needed to indicate that the HTTP GET header is complete. Slowloris, by manipulating the HTTP GET header – not showing two CRLF at the end, causes the web server to reserve the connections to wait for the complete HTTP GET header.

![Slowloris -GET Diagram](image_url)
CHAPTER 4: TESTING RESULTS

Once the number of connections is defined in the attacking command, the corresponding number GET requests will be sent to the web server. However, the GET headers are all in partial form only.

Figure 4-70: Slowloris – GET

Once the web server receives the partial GET header, it will open TCP connections for each request. The web server reserved the resources for the connections which waiting for the next portion of GET header in order to complete the requests. However, the subsequent portion of GET headers are sent extremely slow, i.e. waiting for long interval to be sent. According to Muscat (2013), timeout for HTTP request is 300s. Thus, it is considered too long for incomplete requests to timeout and release the resource, the semi-completed connections are maintained for long time. Before the timeout, the next potion of GET request will arrive, making the timeout to be reset, but still the request is not complete yet, the web server has to keep the resource for this semi-completed connections again.

Figure 4-71: GLBP failed to mitigate Slowloris attack
Henceforth, even GLBP is implemented to load balance the GET requests portions among the redundant routers, but the resource is not released for the next legitimate HTTP GET request due to the reason that the GET requests portions are sent very slowly to the web server which causes more time is need to complete the GET request and the timeout is too long for an incomplete request to be released. Load balancing the portions of GET requests does not fasten the subsequent GET request portions to arrive at web server.
CHAPTER 5: CONCLUSION

Chapter 5: CONCLUSION

As the technologies advance in this era of modernization, the usage of Internet or network increases tremendously beyond or imagination. Every day there will millions of even billions of transactions, information transmits all over the world. Internet has become part and parcels of human’s life. However, it is unfortunately that there are some people misuse their knowledge about technology and attempt to launch cyber-attack, one of the most popular attack will be DoS attack. Due to the huge amount of software developed, DoS attack could be done easily and more sophisticated. Many researchers are urged to come out solutions to mitigate DoS attack. Nonetheless, as what had been studied, most of the previous proposed solutions are not comprehensive as they lead to network latency and some even derive another type of attack or breach.

Therefore, in this work, a more comprehensive and yet efficient solution is being proposed which is by implementing GLBP. GLBP is an existing protocol which is one of the First Hop Redundancy Protocol. By just utilizing this protocol, without developing a brand-new protocol, it is meaningful to study whether GLBP could mitigate the effect of DoS attack as it does not add extra workload to the networking devices and lead to network latency. Instead, GLBP will load balance the packets among the redundant routers and link congestion.

To determine whether this proposed solution is workable, the entire project will need to have to simulation. The first simulation which will be conducted to demonstrate SYN flood attack can be successfully launched towards web server before implementing GLBP. Then, the second simulation will start to mitigate SYN flood attack by implementing GLBP in group of redundant routers and average page load time will be collected as the result of simulations. It is proved that the average page load time from second simulation is shorter than the average page load time from the first simulation which indicates GLBP does can mitigate SYN flood attack. Furthermore, to test the comprehensiveness of this mitigation solution, PING flood ACK flood and Slowloris attacks are launched. Eventually, it is determined that these attacks are still be able to be mitigated by the proposed solution. For the PING flood attack, the difference between after and before mitigation is a negative value which means that after mitigation, the page load that is shorter than before mitigation. Same to the ACK flood, after mitigation the page load time is shorter before mitigation.
CHAPTER 5: CONCLUSION

Clients could browse the website without knowledge of attack being launched. The load balancing of huge amount of packets sent by the attacker among redundant routers is certified to be able to alleviate the impact of DoS attack which could be link congestion or resource consumption to the targeted victim host. Nonetheless, mitigation of Slowloris attack is proved to be fail. This is due to reason that GLBP is to load balance the packets, but Slowloris is manipulating the HTTP GET requests by splitting them into different portions and sent slowly to the webserver to complete the request, thus the connections remained opened for long time. Load balancing the portions of GET requests does not fasten the subsequent GET request portions to arrive at web server. Furthermore, the GET request timeout is 300s which is too long to release the resource for a connections making mitigation by GLBP is failed.

Further proving the effectiveness of GLBP in mitigating DoS attack, packets interval is varied from a broad range i.e. 1μs to 100000μs. As from the testing results, it is undeniable that even though the SYN flood and PING flood attacks are launched with different packets interval, the proposed solution still able to mitigate the effect of DoS attack. It is not only can avoid link congestion but also prevent the targeted victim host like web server to be down due to resource overconsumption.

In conclusion, implementing GLBP is robust enough to mitigate different type of DoS attack like SYN flood, PING flood and Slowloris attack. Even if the attacker launches the attack by sending packets in very short interval, the proposed solution is robust and efficient enough to mitigate and alleviate the impact of DoS attack.


APPENDICES

APPENDICES A: Router Configuration with GLBP implemented

Figure below is the configuration in Router 1:

```bash
interface FastEthernet0/0
 ip address 192.168.2.222 255.255.255.0
duplex auto
 speed auto
glbp 10 ip 192.168.2.254
!
interface FastEthernet0/1
 ip address 192.168.1.222 255.255.255.0
duplex auto
 speed auto
glbp 10 ip 192.168.1.254
!
```

Figure below is the configuration in Router 2:

```bash
!
interface FastEthernet0/0
 ip address 192.168.2.233 255.255.255.0
duplex auto
 speed auto
glbp 10 ip 192.168.2.254
!
interface FastEthernet0/1
 ip address 192.168.1.233 255.255.255.0
duplex auto
 speed auto
glbp 10 ip 192.168.1.254
!```
APPENDICES

APPENDICES B : Configuration on PC running Apache Web Server

Install and start Apache web server in PC on Windows10.

Host a webpage in the Apache web server. The webpage is as shown in figure above
Change IP address of the PC running Apache web server to be 192.168.2.1/24 with IP gateway 192.168.2.254
APPENDICES C: Configuration on Attacker’s PC

Change the IP address of attacker’s PC on Kali Linux to be 192.168.1.1/24 with IP gateway 192.168.1.254.
Launch SYN flood using the command as shown in figure above.

Change the packets interval for SYN flood attack.
APPENDICES

Change the packets interval for PING flood attack.

Launching Slowloris attack.
Impact of Slowloris attack.
APPENDICES

APPENDICES D: Final Year Project Biweekly Report

FINAL YEAR PROJECT WEEKLY REPORT
(Project II)

Trimester, Year: 3, 3  |  Study week no.: 7
Student Name & ID: KHONG JOHNSON 140ACB3535
Supervisor: DR. GAN MING LEE
Project Title: UTILIZING FIRST HOP REDUNDANCY PROTOCOL TO MITIGATE THE EFFECT OF DENIAL-OF-SERVICE ATTACK

1. WORK DONE
[Please write the details of the work done in the last fortnight.]

- Setup network topology from figure 1 to figure 2 as shows below:

  ![Network topology](image1.png)

  Figure 1: Network topology for first simulation

  ![Network topology](image2.png)

  Figure 2: Network topology for first simulation in FYP lab.

- Two switches and one Cisco router are requested from the lab instructor. Total of five straight-through Ethernet cables were used to connect the devices with PCs. One of the PC is installed and running Apache web server. Attacker’s PC is running on Kali Linux OS.
- PC with Apache web server was configured to have IP address of 192.168.2.1/24 with IP default gateway of 192.168.2.254.
- Attacker’s PC was configured to have IP address of 192.168.1.1/24 with IP gateway of 192.168.1.254.
- Legitimate user’s PC was configured to have IP address of 192.168.1.2/24 with IP default gateway of 192.168.1.254.
- Router interface Fa0/0 was configured to be 192.168.2.254/24.
- Router interface Fa0/1 was configured to be 192.168.1.254/24.
### APPENDICES

- Launching DoS attack, more specifically SYN flood attack
  
  ```
  hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.2.1
  ```

- Compare page load time is longer than that before SYN flood attack

### 2. WORK TO BE DONE

- Ping all the hosts and devices’ interface successfully.
- Legitimate user can access the webpage before DoS attack launched

### 3. PROBLEMS ENCOUNTERED

- Attacker’s PC and legitimate user’s PC cannot ping the PC running Apache web server.
- Suspect that it is the problem of Windows Firewall or the proxy that hinder the connectivity check
- With no choice, I have to use two switches as FYP lab does not provide cross-over cable.

### 4. SELF EVALUATION OF THE PROGRESS

- Familiarized with how to connect the hosts and devices to form a network topology
- SYN flood attack is launched successfully

_________________________  ____________________
Supervisor’s signature     Student’s signature
1. WORK DONE
[Please write the details of the work done in the last fortnight.]

- Setup network topology as shows below:

  ![Network Diagram]

  - Implement GLBP in two redundant routers.
  - Launched SYN flood attack
    
    ```
    hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.2.1
    ```
  - Record average page load time and compare that of before mitigation of SYN flood attack

2. WORK TO BE DONE
- Launch PING flood attack to get average page load time before and after mitigation

3. PROBLEMS ENCOUNTERED
4. SELF EVALUATION OF THE PROGRESS

- Setup network topology became faster as I had familiarized with that.
- Every interface in the network can be ping successfully.
- Able to get the expected result which the average page load time after mitigation is shorter than that of before mitigation.
- It could be said that 50% of works had been done in this week.

<table>
<thead>
<tr>
<th>Supervisor’s signature</th>
<th>Student’s signature</th>
</tr>
</thead>
</table>
FINAL YEAR PROJECT WEEKLY REPORT
(Project II)

Trimester, Year: 3, 3  Study week no.: 9
Student Name & ID: KHONG JOHNSON 140ACB3535
Supervisor: DR. GAN MING LEE
Project Title: UTILIZING FIRST HOP REDUNDANCY PROTOCOL TO MITIGATE THE EFFECT OF DENIAL-OF-SERVICE ATTACK

1. WORK DONE
[Please write the details of the work done in the last fortnight.]

- Launched PING flood attack
  `hping3 --icmp --flood gateway_IP_Address`
- Record and compare average page load time before and after mitigation of PING flood
- Launched Slowloris attack
- Compared the impact of before and after mitigation of Slowloris attack

2. WORK TO BE DONE

- Change the packets interval in SYN flood attack and PING flood to test its comprehensiveness.

3. PROBLEMS ENCOUNTERED
N/A

4. SELF EVALUATION OF THE PROGRESS

- 80% of project had been done.
- Mitigation of SYN flood attack, PING flood attack and Slowloris attack are having positive results like I expected.

_________________________  _____________________
Supervisor’s signature    Student’s signature
FINAL YEAR PROJECT WEEKLY REPORT
(Project II)

Trimester, Year: 3, 3 | Study week no.: 10
Student Name & ID: KHONG JOHNSON 140ACB3535
Supervisor: DR. GAN MING LEE
Project Title: UTILIZING FIRST HOP REDUNDANCY PROTOCOL TO MITIGATE THE EFFECT OF DENIAL-OF-SERVICE ATTACK

1. WORK DONE
[Please write the details of the work done in the last fortnight.]

- Launched SYN flood attack with varying packets interval (1µs, 10µs, 100µs, 1000µs, 10000µs and 100000µs)
  
  hping3 -d 120 -S -w 64 -p 80 -i u10000 --rand-source 192.168.2.1

- Launched PING flood attack with varying packets interval (1µs, 10µs, 100µs, 1000µs, 10000µs and 100000µs)
  
  hping3 --icmp -i u10000 192.168.2.1

- Record and compare the results before and after mitigation for both attack with varying packets interval

2. WORK TO BE DONE

- Start to prepare report
- Insert all the screenshots
- Plot graphs

3. PROBLEMS ENCOUNTERED

(N/A)

4. SELF EVALUATION OF THE PROGRESS

- As what expected, the page load time increases when the packets interval decreases.
- After implementing GLBP, even the packets interval changes, still it able to mitigate SYN and PING flood attacks
- FYP report left 20%

_________________________  _________________
Supervisor’s signature  Student’s signature
APPENDICES

FINAL YEAR PROJECT WEEKLY REPORT
(Project I)

<table>
<thead>
<tr>
<th>Trimester, Year: 1, 3</th>
<th>Study week no.: 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Name &amp; ID: KHONG JOHNSON 140ACB3535</td>
<td></td>
</tr>
<tr>
<td>Supervisor: DR. GAN MING LEE</td>
<td></td>
</tr>
<tr>
<td>Project Title: UTILIZING FIRST HOP REDUNDANCY PROTOCOL TO MITIGATE THE EFFECT OF DENIAL-OF-SERVICE ATTACK</td>
<td></td>
</tr>
</tbody>
</table>

1. WORK DONE
[Please write the details of the work done in the last fortnight.]
- Finalize the report
- Add appendices
- Run Turnitin similarity check
- Create a poster

2. WORK TO BE DONE
- Print out the report and poster
- Burn the softcopy of report into CD
- Prepare Presentation slides

3. PROBLEMS ENCOUNTERED
(N/A)

4. SELF EVALUATION OF THE PROGRESS
- Report had been completed

_________________________ _______________________
Supervisor’s signature Student’s signature
APPENDICES

APPENDICES E : POSTER

UNIVERSITY TUNKU ABDUL RAHMAN

KHONG JOHNSON
Supervisor: Dr. Gan Ming Lee

UTILIZING FIRST HOP REDUNDANCY PROTOCOL TO MITIGATE THE EFFECT OF DENIAL-OF-SERVICE ATTACK

INTRODUCTION:
- Denial of service (DoS) - cyber-attack - prevent legitimate users from accessing information or services by intentionally excessive using of the resources
- Threat to network reliability
- Causes tremendous negative effects across many fields
- Gateway Load Balancing Protocol (GLBP) — first hop redundancy protocol that protects data traffic from a failed router, while allowing packet load balancing between a group of redundant routers.
- Load balancing among a group of redundant routers — prevent single point of failure

OBJECTIVES:
1) To study whether DoS attack could be alleviated by implementing GLBP in redundant routers.
2) To prove that GLBP would be an alternative to mitigate various type of DoS attack at the same time with lesser network latency as compared with others proposed solutions
3) To show that GLBP is a more comprehensive and yet effective ways to mitigate DoS attack without leading to any side-effects. Each of the objective is explained further below

Methodology:
- FYP2 - Launch SYN flood, PING flood, and ACK flood attacks (before and after implementing GLBP)
- Output measure: Page Load Time (before and after DoS attack)
- Manipulate the rate of packets sent interval
- FYP3 — Record average page load time before and after launching SYN flood attack to determine that DoS attack will have impact in retrieving the webpages.

Result:
- GLBP is provided to be able to mitigate SYN, PING and ACK flood attack.
- FYP 1 — Average page load time after SYN flood attack is 16742 3s slower.
- FYP 2 — Average page load time after mitigation of SYN flood is 2.34% faster than before mitigation.
- Average page load time after mitigation of PING flood is 11.68% faster than before mitigation.
- Average page load time after mitigation of ACK flood is 7.21% faster than before mitigation.
- As the packets sent interval is shorter, the impact of DoS attack is severer.

Conclusion:
- DoS attack is getting easier to be launched with technologies nowadays.
- Cause huge amount of loss
- Previous proposed solutions causes network latency and might derive another type of attack.
- GLBP – existing protocol, no adding extra workload to routers, do not lead to another attack.
- GLBP even provide redundant routers and paths.
APPENDICES

APPENDICES F : Example of plagiarism check summary
## Utilizing First Hop Redundancy Protocol to Mitigate the Effect of Denial-Of-Service Attack

### Originality Report

<table>
<thead>
<tr>
<th>Similarity Index</th>
<th>Internet Sources</th>
<th>Publications</th>
<th>Student Papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>18%</td>
<td>14%</td>
<td>6%</td>
<td>14%</td>
</tr>
</tbody>
</table>

### Primary Sources

1. **Submitted to Universiti Tunku Abdul Rahman**
   - Student Paper
   - 10%

2. **fes.utar.edu.my**
   - Internet Source
   - 1%

3. **www.utar.edu.my**
   - Internet Source
   - 1%

4. **eprints.utar.edu.my**
   - Internet Source
   - 1%

5. **Submitted to Napier University**
   - Student Paper
   - <1%

6. **www.youtube.com**
   - Internet Source
   - <1%

7. **www.studyblue.com**
   - Internet Source
   - <1%

8. **www.coursehero.com**
   - Internet Source
   - <1%

9. **Submitted to University of Teesside**
APPENDICES

Form Number: FM-IAD-005 | Rev No.: 0 | Effective Date: 01/10/2013 | Page No.: 1 of 1

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

<table>
<thead>
<tr>
<th>Full Name(s) of Candidate(s)</th>
<th>KHONG JOHNSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID Number(s)</td>
<td>14ACB03535</td>
</tr>
<tr>
<td>Programme / Course</td>
<td>BACHELOR OF INFORMATION TECHNOLOGY (HONS) COMMUNICATIONS AND NETWORKING</td>
</tr>
<tr>
<td>Title of Final Year Project</td>
<td>UTILIZING FIRST HOP REDUNDANCY PROTOCOL TO MITIGATE THE EFFECT OF DENIAL-OF-SERVICE ATTACK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Similarity</th>
<th>Supervisor’s Comments (Compulsory if parameters of originality exceeds the limits approved by UTAR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall similarity index: <em><strong>18</strong></em>_ %</td>
<td></td>
</tr>
<tr>
<td>Similarity by source</td>
<td></td>
</tr>
<tr>
<td>Internet Sources: <em><strong>14</strong></em>_ %</td>
<td></td>
</tr>
<tr>
<td>Publications: <em><strong>6</strong></em>_ %</td>
<td></td>
</tr>
<tr>
<td>Student Papers: <em><strong>14</strong></em>_ %</td>
<td></td>
</tr>
</tbody>
</table>

| Number of individual sources listed of more than 3% similarity: ___1____ |

Parameters of originality required and limits approved by UTAR are as follows:
(i) Overall similarity index is 20% and below, and
(ii) Matching of individual sources listed must be less than 3% each, and
(iii) Matching texts in continuous block must not exceed 8 words

Note: Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.

__________________________________________  __________________________________________
Signature of Supervisor                      Signature of Co-Supervisor

Name: Dr. GAN MING LEE                      Name: Dr. ROBITHOH ANNUR

Date: 6 March 2018                            Date: 6 March 2018

BCN (Hons) Communication and Networking
Faculty of Information and Communication Technology (Perak Campus), UTAR
# Checklist for FYP2 Thesis Submission

<table>
<thead>
<tr>
<th>TICK (√)</th>
<th>DOCUMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Front Cover</td>
</tr>
<tr>
<td></td>
<td>Signed Report Status Declaration Form</td>
</tr>
<tr>
<td></td>
<td>Title Page</td>
</tr>
<tr>
<td></td>
<td>Signed form of the Declaration of Originality</td>
</tr>
<tr>
<td></td>
<td>Acknowledgement</td>
</tr>
<tr>
<td></td>
<td>Abstract</td>
</tr>
<tr>
<td></td>
<td>Table of Contents</td>
</tr>
<tr>
<td></td>
<td>List of Figures (if applicable)</td>
</tr>
<tr>
<td></td>
<td>List of Tables (if applicable)</td>
</tr>
<tr>
<td></td>
<td>List of Symbols (if applicable)</td>
</tr>
<tr>
<td></td>
<td>List of Abbreviations (if applicable)</td>
</tr>
<tr>
<td></td>
<td>Chapters / Content</td>
</tr>
<tr>
<td></td>
<td>Bibliography (or References)</td>
</tr>
<tr>
<td></td>
<td>All references in bibliography are cited in the thesis, especially in the chapter of literature review</td>
</tr>
<tr>
<td></td>
<td>Appendices (if applicable)</td>
</tr>
<tr>
<td></td>
<td>Poster</td>
</tr>
<tr>
<td></td>
<td>Signed Turnitin Report (Plagiarism Check Result - Form Number: FM-IAD-005)</td>
</tr>
</tbody>
</table>

*Include this form (checklist) in the thesis (Bind together as page 2)