National College of Ireland

Detection and Mitigation of High and Low Rate DDOS Attack on SDN Using Traffic Behaviour and Game Theory

MSc Internship
Cyber Security

Vikas Sharma
Student ID: X18119743

School of Computing
National College of Ireland

Supervisor: Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Vikas Sharma
Student ID:	X18119743
Programme:	MSC Cyber Security **Year:** 2019
Module:	Internship
Supervisor:	Imran Khan
Submission Due Date:	12th August 2019
Project Title:	Detection and Mitigation of High and Low Rate DDOS Attack on SDN Using Traffic Behaviour and Game Theory
Word Count:	5099 **Page Count: 15**

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

Signature: ……

Date: 8th August 2019……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

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

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

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

Detection and Mitigation of High and Low Rate DDOS Attack on SDN Using Traffic Behavior and Game Theory

Vikas Sharma
X18119743

Abstract

A new lightweight system to detect and mitigate low and high rate DDOS attacks on SDN by analysing traffic flow count and game theory model. The model is comprised of two layers, one for detection and layer two performs the mitigation. Detection is carried out by analysing the flow and mitigation is carried by blocking the IP address or forwarding the packets towards the honeypot. The system needs to be implemented at gate way point of software defined network and analyse the traffic before entering the network and mitigate the detected attacks. The system can detect low and high rate DDOS attacks for network and application layer of TCP/IP network topology. The experimental system has been evaluated by setting up virtual machines and results show that system can detect the high rate, low rate DDOS attack from spoofed IP address and can mitigate the attack by blocking the IP or routing the traffic towards the honeypot.

1 Introduction

The world of Internet is growing very rapidly and has become major part of individuals. The modern business highly depends on the availability of internet. With more and more dependency over the Internet, bad actors cause a great threat to modern world by disrupting the availability of internet to users and service providers. Distributed Denial of Service (DDOS) is one of major threat to internet and it is very handy attack for attackers as it is easy to carry out and can harm the target very badly (Hoque, 2015). It is a technique where threat actors send malicious requests to the servers and makes the service unavailable to legitimate users. The study on impact of DDOS attack on e-commerce shows that USD 40,000 per annum is the estimated average loss caused during one DDOS attack (Alamri, 2018). The DDOS attack can be carried out at various layers of the IP/TCP network topology. This attack can also impact badly on software defined networks (SDN). These networks are complex networks and provides more flexibility and control management as compared to traditional networks (H. D. Zubaydi, 2017). Advanced techniques have been introduced and opted by threat actors to perform the DDOS attack which makes it very simple and don't require much of computer skills. These techniques require few clicks to flood the target with malicious requests and make the services unavailable. These techniques also make it very difficult to detect the attack at early stages and mitigate it. Threat actors are using techniques which sends malicious request at very low rate and gradually makes the service unavailable to users. Thus, a new approach is required which can dealt with modern DDOS threats. In this paper, a new approach has been proposed which can detect the high and low rate DDOS attack and can mitigate it by using the game theory. The rest of paper is composed as follow: Section 2 provides the insights of related work by critically analysing the existing approaches, section 3 outlines the research methodology for the research, in section 4, design specifications of system has been discussed, section 5 presents the implementation of system,

evaluation has been carried out in section 6. Section 7 presents the conclusion of research and future work on this research.

2 Related Work

Distributed Denial of service attack is one of the most major threat for online service providers and its users. An attacker makes the service unavailable to users by sending fake networks packets to web server and makes the server busy. The DDOS attack can be carried out on multiple ways and can target different layers of TCP/IP protocol. Christos Douligers et al in (Mitrokotsa) has described the various classifications of DDOS attack. The DDOS attack can be classified as Network Device level, OS level, Application based attacks, Data flooding and attacks based on protocol features (Mitrokotsa).

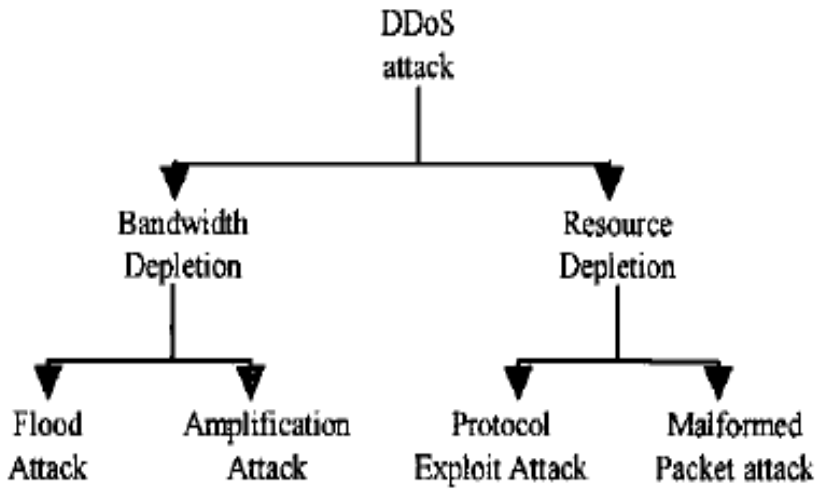

Figure 1 Classification of DDOS (Mitrokotsa)

In (Paxson, 2001), author has eplained various approaches that attackers can opt to perform DDOS attack. Attackers are taking new approaches to perform the attacks to over come the present detection mechanisums. Spoofing of IP address is a type of approach where attackers spoof the IP address with a legal or valid IP address to perform DDOS attack (Bharti Nagpal, 2015). This type of attack is known as reflect attack. The attacker uses the compromised machines to send the request packets with spoofed IP addresses towards the host and make the services unavialable to legitimate users. (Bharti Nagpal, 2015). In addition to spoofed IP address, bad actors are carrying out DDOS attacks with high rate or low rate of traffic flow. Mahadev et al have eplained the threat classifications of DDOS attacks and provides an overview of low rate DDOS attacks (Mahadev, 2016)

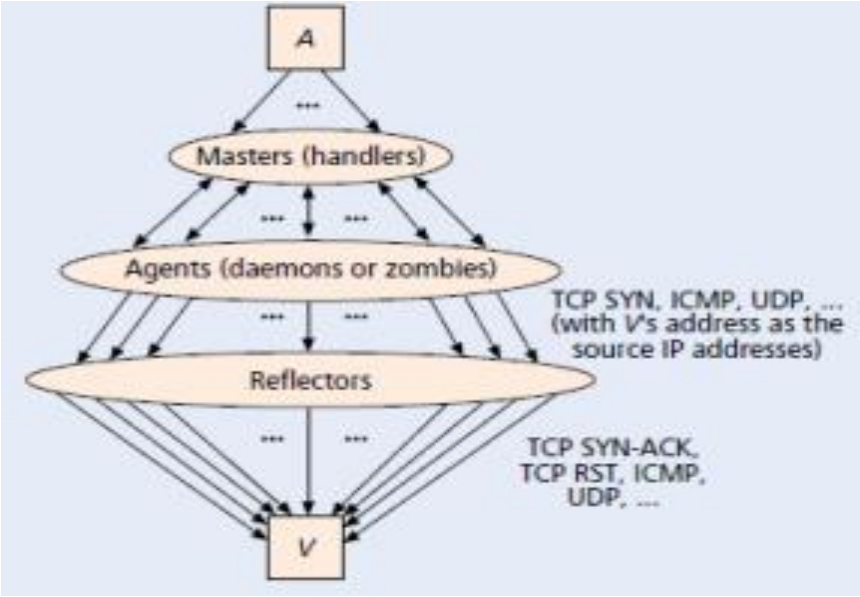

Figure 2 Architecture of Reflected DDOS Attack (Bharti Nagpal, 2015)

The increase in frequency of DDOS attack has resulted in numerous DDOS defence mechanisms (Mohd. Jameel Hashmi, 2019). In (Koay, 2019) Koay has critically examined various mechanisums to encounter DDOS attck and concluded that present mechansiums have their boundaries and can be breached by bad actors. An experiemnt was carried out by researcher Sundar et al to check the protection provided by Windows in windows 2012 server R2 against DDOS attack (Sundar, 2016). The result of experiement shows that the protection provided in server by windows is not able to mitigate the simple SYN type DDOS attack and server got compromised with the traffic flow of less than 3.1 GB (Sundar, 2016). The threat of DDOS atttack is not limited to traditional infrasturture, it is also a great threat for software defined networks (SDN). In (Qiao Yan, 2016) has explained the the impacts on SDNs from the DDOS attack and how it can be carried out in SDN. Researcher Shui Yu et al in (Guo, 2014) has advised various approaches to beat the DDOS attack in SDNs and proposed mitigation technique by using the dynamic resource allocation capability of cloud. The researcher has proposed to use the idle resources of cloud by cloning adequate intrusion preventive systems for the victime machine (Guo, 2014). However, the appraoch can only be used for mitigation of attack. Also it has limitations that there should be adequate idle resources present on cloud infrastructure which can be used for cloning (Guo, 2014) .In (P. Kamboj, 2017), resercher P. Kamboj et al has explained the way attackers takes advantage of open internet architecuture and perform the DDOS attacks to victims machine. Therefore propoer mechanisums in network or machines should be in place to detect the attack at initial stages and mitigate it (P. Kamboj, 2017).

Mrs Ajagekar and et al has compared various present mechanisum and has proposed an approach using Bayes Multinomial classifier method to detect the DDOS attck on layer seven (Jadhav, 2016). The system proposed in (Jadhav, 2016) first captures the network packets and extracts the important information. The extracted information can be used for detection of attack by employing classified. The proposed approach is capable of detecting the attack with less false positive rate, however it lags in detecting the attack in early stages and attack on other network layers. Another approach of detecting the attack based on defined rules has been discussed in (Md.Khamruddin, 2013). The proposed approach is very simple and easy to implement. The proposed mechhanisum detects the attack by monitoring the traffic flow and

mitigates it by balancing the load of victim machine and finally push back the router to upstream. The mechanisum is effective, however, approach requires regular monitoring and cannot detect the attacks carried out using modern techniques (Md.Khamruddin, 2013).

In (Kian Son Hoon, 2018) researcher K.S.Hoon has critically analyized the use of machine learning algorithms to detect and mitigate the DDOS attacks carried out by attackers using modern techniques. The researcher has used data mining tool WEKA and H2O to implement the learning models. (Kian Son Hoon, 2018). The results reflect that Naïve Bayes, Gradient Boosting machine Distributed random forest alogorithms can detect the DDOS attack with very high accuracy. L. Barki et al has performed another research using intrusion detection system with four different machine learning alogoriths: K meathod, Naïve Bayes, K-means and KNN (L. Barki, 2016). The result of the research reflects that machine learning algorith Naïve Bayes is best algorithm for DDOS protecteion. That said, (Kian Son Hoon, 2018) and (L. Barki, 2016) researches showed that machine learning algorithms can be used to detect the modern DDOS attacks in SDNs and Naïve Bayes is best algorithm for the detection of attack.

The machine learning algorithms can be imlemented to detect the attack by analysing the anomly in network traffic (U. Dincalp, 2018). Reseacher U. Dincalp et al advised an approach in which they break the incoming network traffic into datasets and analyze it. The datasets are then saved in the database. The system is capable of deteting the attack, however it is not capable of mitigating the attack by its own. In another approach, T.M.Thang et al has implemented Bloom filter algorith (T. M. Thang, 2018). The system captures the packets and uses the packet identification approach to detect the attack from spoofed IP address. The approch advised in (T. M. Thang, 2018) is capable of detecting SYN flood high rate type of DDOS attack only. In (Zhijun WU, 2011), provides the flow of flood based high rate attack and low rate DDOS attack. The comparision makes it easy to understand on working of low and flood type attack and detection mechanisums that can be implemented (Zhijun WU, 2011).

The detection of low rate attack has been advised by H. Hong in (K. Hong, 2018). The advised system is divided into three groups. The approach is that the request packets will be received by the group three rather than by the web server. The attack will be identified by using the timeout mechanisum by the group three. On detection of slow rate attack, the system will send the IP address will be blocked by SDN (K. Hong, 2018).The results of advised approach are great however it can be used for low rate DDOS attack only.

The low and high rate DDOS attack can be detected by using the approach advised by Neha et al in (Tapaswi, 2017). The researchers has advised mechanisum to detect attack by analysing the flow count and traffic behaviour of incoming traffic. The system detects the attack is the flow count of packets is less than or greater than the threshold level. The approach has shown great results in term of detecting low and high rate attack, however cannot detect the attack if the IP address is spoofed by an attacker. Game theory can be used to identify the spoofed IP address (J. MARCOS, 2017). The researcher Marcos et al has used Game Theory in conjunction with signature based detection mechanisums (J. MARCOS, 2017).

2.1 Game Theory

This can be described as a modelling game where each player act as per the strategy and results in best possible rewards (Sankardas Roy, 2010). The applications of game theory were earlier limited to business to make business descions, however its now widley been used in computer science (Wooldridge, 2012). Researcher Xiaolin et al in (Cui Xiaolin, 2008) has defined a risk assessment model for the use of Game Theory in network information security.The model explained by (Cui Xiaolin, 2008) consists of two playes threat agent and vulberability agent. The threat agent sprreads the threats in the network and vulnerablity plays as counter part of first player. The model is capable of detection of network risk conditions and potential threats to the network (Cui Xiaolin, 2008). Reseracher H.S.Bedi et al in (Harkeerat Singh Bedi, 2011) has defined defence mechanisum against DDOS attack on TCP using the game theory. The system analysis the incoming flow and makes the descion using the game theory in GIDA module. The modules will block or restrict the network towards the target based on computational descions (Harkeerat Singh Bedi, 2011).Although the model shows great results, however it was capable of detecting TCP based DDOS attack. H.S.Bedi et al has concluded that game theory and its applications can be widley used in computer security applications and defense mechanism against the threats such as DDOS (Harkeerat Singh Bedi, 2011).

The number of DDOS attacks are increasing day by day and the inbuilt security fetures of present OS are not capable of mitigation of threats like DDOS attack. The use of machine lerning in detection and mitigation of DDOS has shown great outcomes (Kian Son Hoon, 2018) (L. Barki, 2016) (T. M. Thang, 2018). However these algoriths require time for training. Also the supervised learning algorithms shows better results as compared to unsupervised learning methods (Kian Son Hoon, 2018). The machines learning algorithms can only detect either low rate DDOS attack or high rate/flood DDOS attacks (K. Hong, 2018). The use of machine learning algorithms have increased the scope of detection, however these algorithms require traning time before start detecting the threats. Thus a system is required which can detect the DDOS attack of different layers of TCP/IP model and mitigate it at early stages. The game theory can be used to reduce the false positive and to mitigate the attack.

3 Research Methodology

The research has been conducted after critically analysing the research papers from IEEE, ACM and google scholar.

Reseracher Neha et al (Tapaswi, 2017) has advised a system to detect low and high rate DDOS attack by analysing the traffic flow of incoming traffic. The approach can be used along with the game theory to detect DDOS attack of low and high rate for different layers of TCP/IP network model and to mitigate the attack. In (J. MARCOS, 2017) research has proposed system for detection and mitigation using the Holt Winter signuture and game theory. In this research paper a new system has been proposed which can use the leight weight approach of detection of low and high rate DDOS attack from (Tapaswi, 2017) and game theory as per in (J. MARCOS, 2017). The system is a leight weight system and is capable of detection and mitigation of DDOS attack on SDN. The system can be installed at gateway of the SDN, thus the network packets can be analyzed before they enters the network.

In (Tapaswi, 2017), researcher has crtically analzed the frequency of packets from different DDOS attack tools such as HULK and HOIC. The table below shows the rate of packets sent by different attacking tools at different intervals of time.

Attack	Tools	Flow count at different time instant (interval of 15 sec) with single node					Average flow count with different number of nodes on an average of 45 sec				
		15 sec	30 sec	45 sec	60 sec	75 sec	8 Nodes	16 Nodes	32 Nodes	64 Nodes	128 Nodes
High Rate	HOIC	2100	2200	2200	2248	2267	17624	21190	22640	22701	22700
	HULK	2500	2600	2700	2700	2750	21200	22450	23000	23210	23215
	XOIC	2800	2900	3000	3000	3040	23840	24000	25020	25729	25728
Low Rate	Longcat	75	72	73	70	70	438	462	480	489	485
	TorsHammer	70	60	60	64	61	394	415	440	441	440

Figure 3 Flow count of DDOS attack tools

After analysing the values from the above table, we can figure out that the DDOS attack of high rate sends 2100 to 2800 packets in first 15 seconds and after that the count remains almost constant for up to 75 seconds. Similarly, for low rate, packet count per 15 seconds is in between the 70 to 75 and it reduces to 61 to 70 over 75 seconds. Thus, by applying this conditions, we can detetct the low and high rate DDOS attacks at early stages of attack.

Once the attack is detected, we can mitigate it by impying the game theory as described in (J. MARCOS, 2017). The game will be played by two players. The first player will be the attacker and the second player will be the defence system. The game theory will make the desion based on cost and rewards if the IP address should be black listed or packets needs to be routed to honey pot for further manual analysis. The action for attack player will be either attack or no attack. Similarly, the actions for defence player will be to block or direct the traffic from IP address towards the honey pot. The rewards will be higher for defense system if it detects the attack. Similarly, if defense system detects the attack when there is no attack, the rewards for attacker will remain zero, however it will impact the payoff for the defence as it costs the defense system for blocking or sending the packets towrads the honeypot. Similarly, if defence system sends the packets to honeypot, it will be higher cost for defence system and the rewards should be less as compared to blocking the IP address. The attacker will tries to get the extra rewards by making the defence system to send the packets towards the honeypot (Harkeerat Singh Bedi, 2011). The below matrix has been generated for the rewards for each move of the attacker and defence players.

Attack/Defence	Attack	No Attack
Block	1, -1	-2, 0
Honeypot	1, 2	-4, 0

Table 1 Matrix for rewards according to action of players

The payoff for defence and attack can be calculated by using the calculations provided in (J. MARCOS, 2017) (Harkeerat Singh Bedi, 2011).

$$P_{atk} = w_1^{atk} \cdot E - w_2^{atk} \cdot BC - w_3^{atk} \cdot AC$$

$$P_{def} = -w_1^{def} \cdot E + w_2^{def} \cdot BC + w_3^{def} \cdot AC$$

Equation 1

Where Patk is payoff for attack vector and Pdef is payoff for defence. Watk and wdef are weights for attack and defence, BC is bandwith consumed by legitimate users as compared to threat actors and AC is attack cost calculated by considering the number of hosts from attacker as compared to number of hosts from legitimate user.

After calculating the payoff of attack and defence, game theory decides if the attacking IP address needs to be blocked or packet should be sent to honeypot for the analysis. The traffic will be routed towards the honeypot if the detected attack is from spoofed IPs else the module will block the respective IP addresses thus not cosuming the excess of computing power.

The system is installed at gateway point of cloud thus, a cloud network is not required for the evalutaion of the system (J. MARCOS, 2017). The system can be evaluated by setting up a virtual network using virtual box and simulate DDOS attack using the tools slowloris Hping3 and LOIC (Reiher, 2002).The evaluation has be performed on the basis of detection of low and high rate DDOS attack, mitigate rate of system false positive and false negative alarms.

The use case diagram (Figure 4) shows the functionality of the system and the various actors which will be part of the proposed system

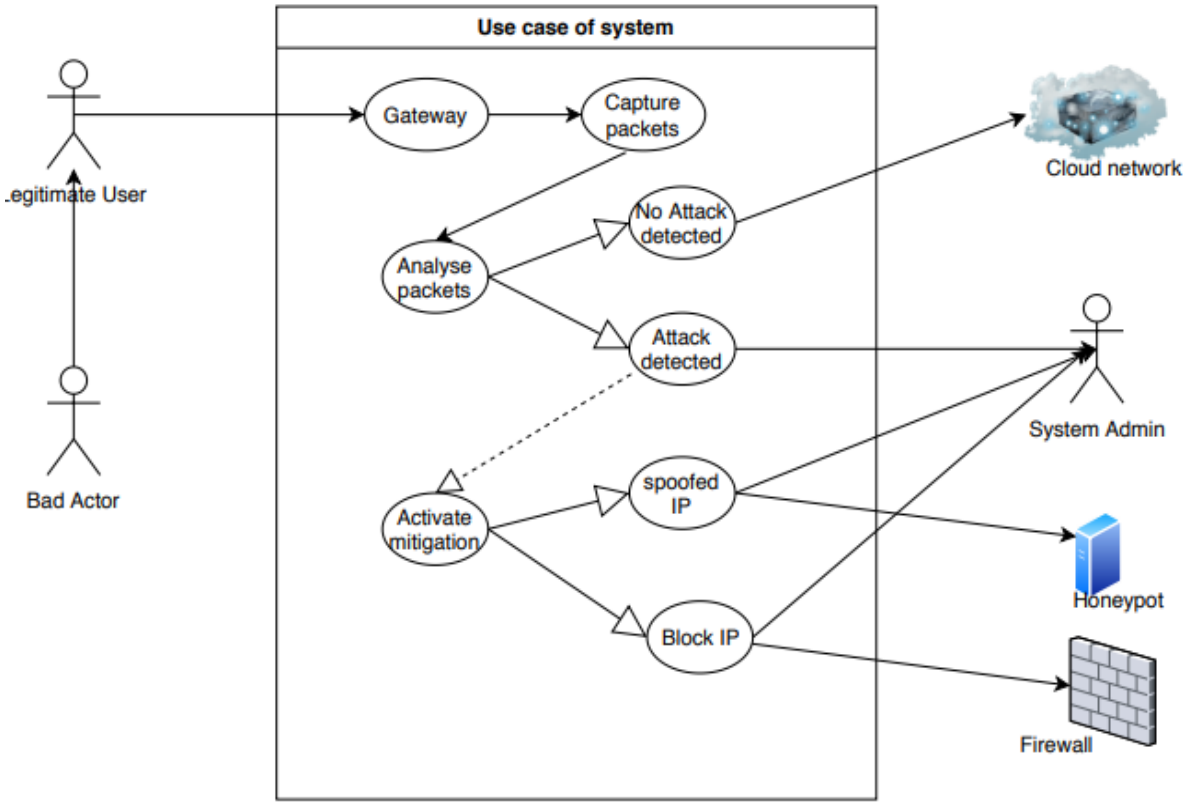

Figure 4 Use case diagram

4 Design Specification

The system is made of two layers: Layer 1 and Layer 2. Layer 1 captures the incoming network flow and analyse the traffic. It detects the low and high rate DDOS attack. Layer 2 gets activated once the layer 1 detects the attack and takes the decision using the game theory. For decision making, it gets the data from layer 1 and either block the IP by adding the IP address of threat actor to firewall blacklist or route the packets towards the honepot.

Layer 1:

The layer one captures the incoming traffic and analyse it. The details of packet such as source IP address, destination IP address, source and destination port, protocol type and time it arrived at network. These details will be fed in the database and the flow can be analysized for individual source IP address. The flow of traffic can be calculated by calculating the number of packets received for particular interval of time. If the number of packets received is less than the thresshold value, a pop up will appread on screen with the warning message "Low rate DDOS attack detected for {IP}, GT activated" where IP is the IP address of threat actor. If the number of packets receieved is higher than the threshold value, the system will generate pop up message on the system administrator with warning message High rate DDOS attack detected for {IP}, GT activated"

I. Capture the network traffic and upload the packet details in database
II. Analyse the number of packets received for individual IP address in one second
III. If the number of packets for a IP in given time is less then threshold
    a. Error warning pop up on screen "probeble Low rate DDOS attack detected"
    b. Activate Layer 2
IV. Else If the number of packet received for an IP is higher than the threshold value
    a. Error warning po up message on screen " Probeble High rate DDOS attack detected"
    b. Activate Layer 2

Layer 2:

Once the attack is detected by layer 1, layer two gets activated. It works on game theory approach and takes the descion based on inputs from layer one. In game theory, players takes the statistics approach to makes the decision which results in best rewards. The game can be played between two players in this module. Player one is the attacker and the player two is the defence mechanisum. The reward and cost for each move will be calculated.

I. Calculate payoff for defence and attack using the information provided by layer 1
II. If payoff for defence is higher than the payoff of attack, block the IP address by adding the IP to blacklist IP address
    a. Pop up on screen with message "IP address added to black list database"
III. Else send the packet to honey pot for the analysis
    a. Pop up on screen with message "Packet forwarded to honeypot"

Complete Flow Chart of System:

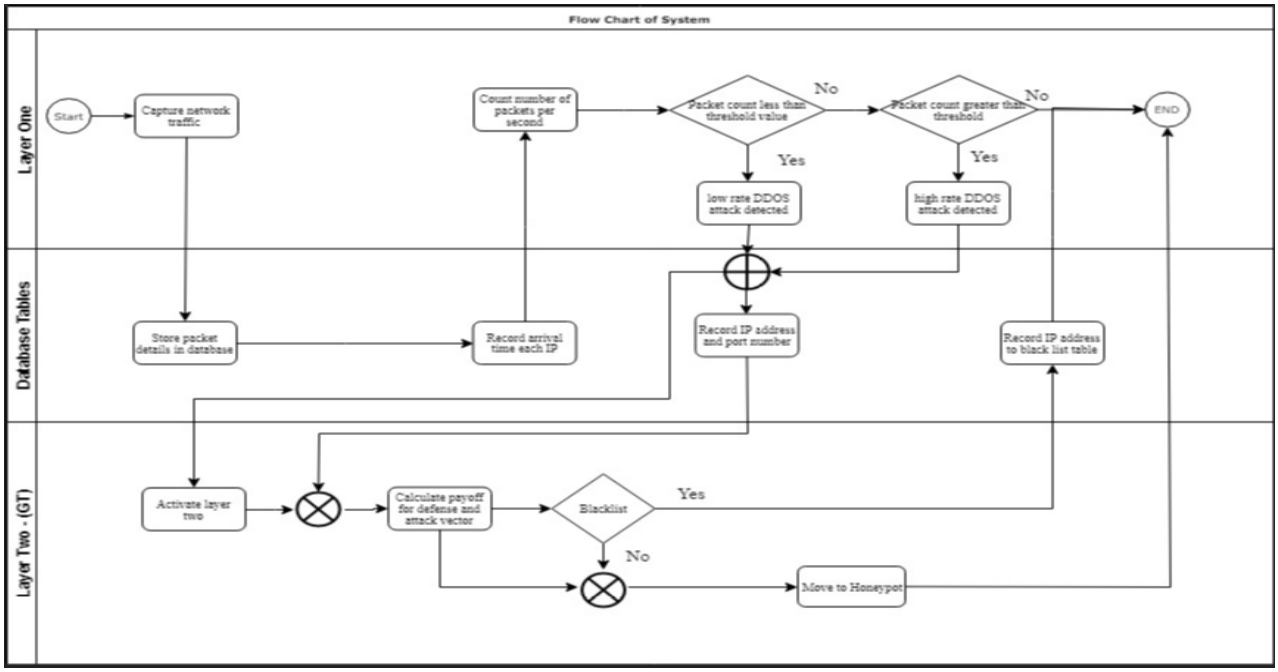

Figure 5 Flow Chart

The design of system has been shown below in figure 6. The gateway gets all the requests from the internet before passing it to the cloud network. The proposed system fetchs the packet details from the gateway point and analyse the packets. The detection carries by layer 1 and activates the layer 2 on detection.

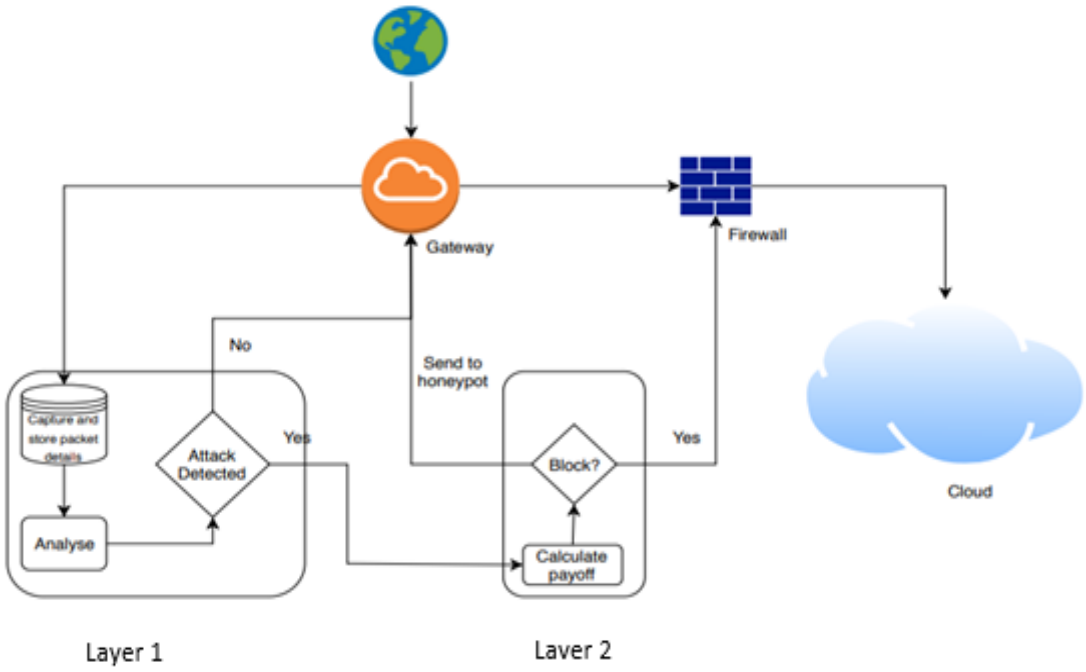

Figure 6 System Design

5 Implementation

The implementation has been carried out by dividing it in two phases. The first phase is for the implementation of layer 1 and 2nd phase is for the implementation of layer two. The final phase is to make both layers working parallelly when attack is detected by layer one.

Technologies Used:

Sr. No	Technology	Version	Purpose
1	Python	3.7	Backend technology for caputring data packets and analysis
2	MySQL	8.0	As database

Table 2 Technologies Used in Project

File Structure:

The project contains three python codes files and database. The file structure is as following:

Caputure.py: Python file to capture the network packets and upload the details in database
Attack.py: Python file to analyse the network packets from database and detect the attack
Gt.py: Python file which calculates the payoff for defnce and attack verctors and makes decisions
Final.py: This file makes call to other two files and run the capture script first and at every two miniutes interval runs the attack.py and gt.py script for detection and mitigation of system
Database Structure: MySQL has been used for database

Table name	Data
Capture	Stores the real time data packets information
Layer_1	Captures the IP address for which layer 1 detects the DDOS attack
Black_IP	Stores the black listed IP address

Table 3 Database Tables

Modules of system: Figure 7 below shows various modules of the system and how these modules are interlinked. The files used by each modules are represented in respective blocks.

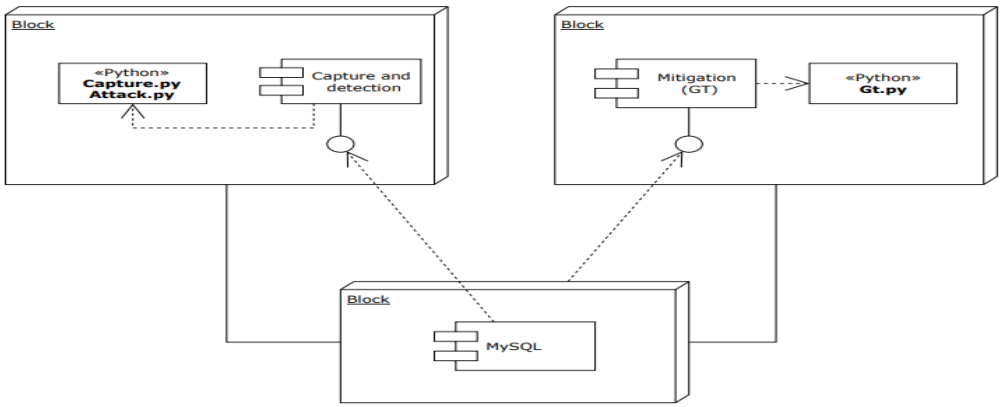

Figure 7 Modules

The final output of system is the warning message on screen of administrator once the attack is detected and followed by the mitigation action. The warning message reflects the type of attack. During the mitigation, the detection continues to run in parallel

6 Evaluation

The evaluation of system has been carried out by performing various tests with different test cases and data. To test the functionality, system has been installed in a virtual machine. Two additional virtual machines are set to simulate DDOS attack. The three virtual machines are running over virtual box installed on Windows 10. The virtual network has been set up between three machines so that these machines can interact with each other without impacting the main production system.For this evaluation, internal network between the virtual machines have been set up.

The DDOS attack can be simulated by using software such as Slowloris, Hping3 and Low Orbit Ion Cannon (LOCI). These three simulation software simulates DDOS attack at different rates. Slowloris can simulate low rate DDOS attack, LOCI can generate high rate DDOS attack and hping3 can simulate DDOS attack from spoofed IP address. Below are the case study to evaluate the functioning of system

6.1 Detection of High rate DDOS attack

High rate DDOS attack has been simulated towards the target virtual machine while the scripts for detection of attack running in target machine. The simulation has been generated by using LOIC. It is an application which can generate send packets with high intensity towards the target IP address or website. It is also capable of sending HTTP, TCP or UDP packets to simulate different types of ddos attack (Mahadev, 2016).

In this test, TCP ddos attack has been generated at port 80 of target using faster rate of sending the packets to target. The system captured the network packets and detected the attack in two minutes from the initial starting of the attack. The GT module of system mitigated the attack by sending the the IP address to firewall to block the traffic coming from the IP address.

The similar simlution has been tested with different options available on LOIC and the output of system remains same i.e. detected the high rate DDOS attack within two minutes from initiation of attack.

The test results of four different experiemnts are shown in Figure 8

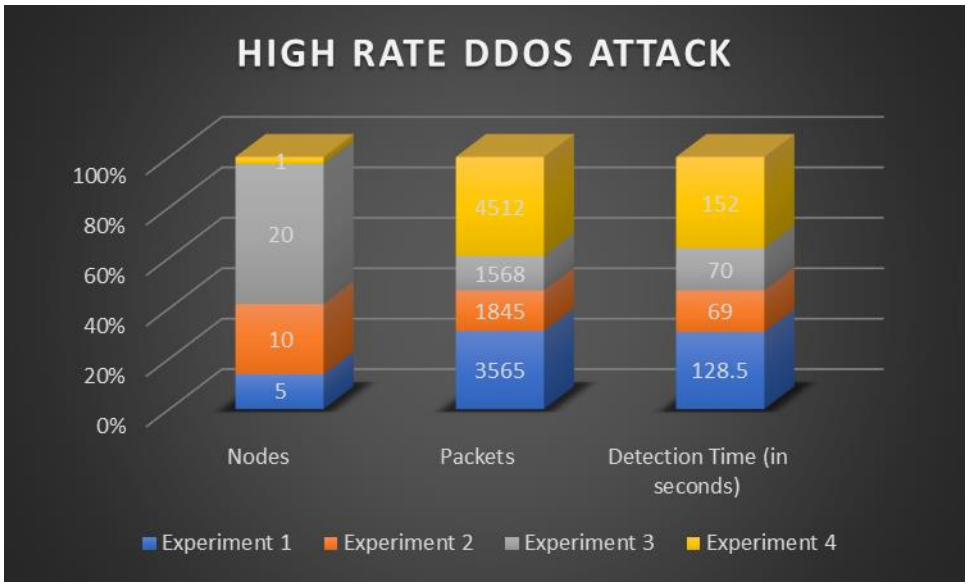

Figure 8 Test results for High Rate DDOS attack

6.2 Detection of Low rate DDOS attack

Low rate DDOS attack has been simulated using Slowloris software. It can send the TCP packets at very low rate and keep the connection alive for longer time (Tapaswi, 2017). The attack was directed to target machine. The system detected the attack in four minutes from initiation of attack. The GT module mitigated the attack by sending the IP address to firewall to block the IP address.

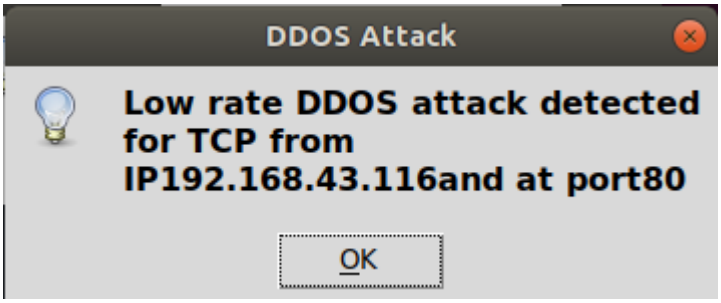

Figure 9 Warning message for Low rate DDOS attack

The results from four different experiment are analyzed and have been curved in below figure 10. The graph shows the number of packets captured during the simulation for individual experiment and time taken by system for detection and mitigation of attack.

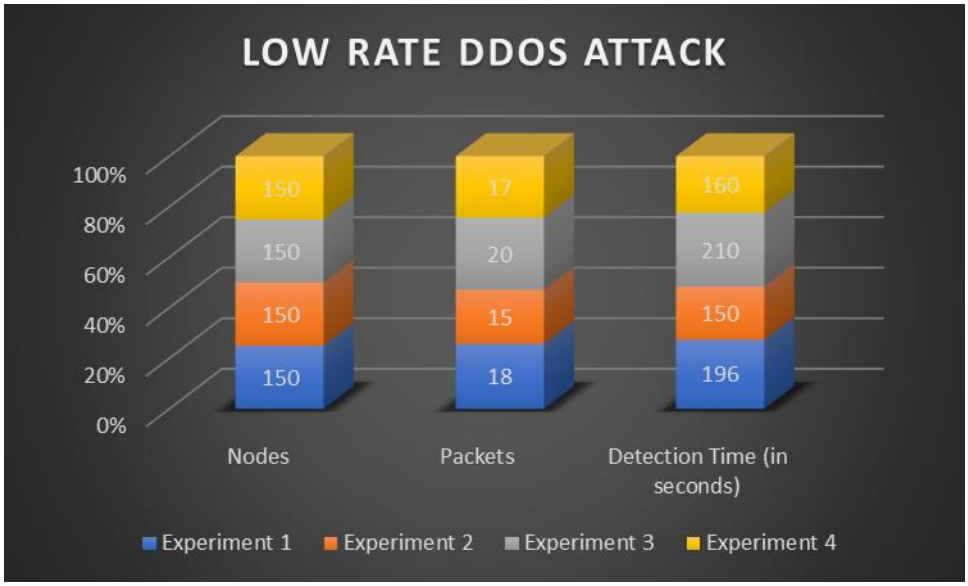

Figure 10 Test results for Low Rate DDOS attack

6.3 Detection of DDOS attack from spoofed IP address

The high rate attack from spoofed IP address has been generated by using Hping3 (Bhatnagar, Som, & Khatri, 2019). The system successfully detects the attack and GT module routed the traffic towards the honeypot. The system was able to detect the attack in first two attempts; however, it was not able to detect if it was spoofed as it sends the IP address to block list. However, subsequent attempts were successful. This is because system can detect the spoofed address based on historic traffic from the spoofed IP address.

Figure 11 Warning message from Layer 2

The results of five experiments have been shown in table 4 below. During the first experiment, system blocked the IP address as there was no historical data present for the spoofed IP address. During the subsequent tests, the historical data was feed into system by generating normal traffic towards the target system and later simulate the DDOS attack towards the target machine.

Attack/Detection	Attack Detection	Spoofed Detection
Experiment 1	Yes	No
Experiment 2	Yes	Yes
Experiment 3	Yes	Yes

Experiment 4	Yes	Yes
Experiment 5	Yes	Yes

Table 4 Test results of DDOS attack spoofed IP address

6.4 Discussion

The behaviour of low and high rate DDOS attack is very different. Multiple experiments using proposed system reflects that low and high rate DDOS attack can be detected using this approach. Also, attack using spoofed IP address can be detected. The use of Game Theory is possible for the mitigation. Different tools have been used to evaluate the functionality and capabilities of the proposed system. LOIC has been used to test the detection capabilities of high rate DDOS attack, similarly, low rate DDOS attack has been simulated by using the Slowloris and Hping3 has been used to test the detection and mitigation capability for attack from spoofed IP addresses.

Based on the various experiments, the average of true positive rate and true negative rates have been calculated as 98.98% and 99.05 % respectively. Throughout the experiments, there was one case where the system blocked the IP address instead of forwarding the network packets to honeypot as the attack was simulated from spoofed IP address. The failure of system is because of design, the system calculates the payoff by comparing the number and rate of packets received from the same IP address in past. As this was first experiment and there were no previous tracks for the IP address, thus system updates the firewall blacklist database to block the IP address. Therefore, Game theory can be effectively used for the mitigation of DDOS attack.

A comparison of proposed system with previously proposed systems has been showed in table 5 below. From the experiments, the system has shown capabilities of detecting different type of attack and can mitigate it successfully. However further testing on SDN network and simulated attack from different DDOS tools is required to test the capabilities of system.

Sr. No	Present mechanisms	Low Rate	High Rate	Mitigation	Spoofed IP address
1	Resource allocation (Guo, 2014)	N/A	N/A	Yes	N/A
2	Multinomial Classifier (Jadhav, 2016)	N/A	Yes	No	N/A
3	Bloom filter (T. M. Thang, 2018)	No	Yes	No	Yes
4	Slow DDOS (K. Hong, 2018)	Yes	No	No	N/A
5	High/Low rate (Tapaswi, 2017)	Yes	Yes	No	No
6	GT-HWDS (J. MARCOS, 2017)	N/A	Yes	Yes	N/A
7	Proposed Solution	Yes	Yes	Yes	Yes

Table 5 Comparison of proposed approach with existing approaches

7 Conclusion and Future Work

In this paper, an approach to detect low and high rate DDOS attack on SDN has been proposed. The system detects the attack by analysing the incoming traffic and mitigates by using the game theory approach. The proposed system has been evaluated by performing various tests and can detect the attack in early stages i.e. 50 – 60 seconds on average. By comparing the results with existing approaches, it has been observed that proposed approach is more dynamic in nature of detection and mitigation. The mitigation process either block the IP address or route the packets towards the honeypot based on decision made by game theory model. The results of experiments show that the applications of game theory can be implemented to mitigate the DDOS attack on SDNs. As a future work, using the game theory for detection of attack as well as mitigation.

References

Alamri, N. I. (2018). *The Impact of DDoS on E-commerce.* Riyadh: IEEE.

Bharti Nagpal, P. S. (2015). *DDoS Tools: Classification, Analysis and Comparison .* Delhi: IEEE.

Bhatnagar, D., Som, S., & Khatri, S. K. (2019). *Advance Persistant Threat and Cyber Spying - The Big Picture, Its Tools, Attack Vectors and Countermeasures.* Dubai: IEEE.

Cui Xiaolin, T. X. (2008). *A Markov Game Theory-based Risk Assessment Model for Network Information System.* China: IEEE.

Guo, S. Y. (2014). *Can We Beat DDoS Attacks in Clouds?* IEEE.

H. D. Zubaydi, M. A. (2017). *Review on Detection Techniques against DDoS Attacks on a Software-Defined Networking Controller.* Palestinian: IEEE.

Harkeerat Singh Bedi, S. R. (2011). *Game Theory-based Defense Mechanisms against DDoS Attacks on TCP/TCP-friendly Flows .* TN: IEEE.

Hoque, D. K. (2015). *Botnet in DDoS Attacks: Trends and Challenges.* Tezpur: IEEE.

J. MARCOS, V. O. (2017). *A Game Theoretical Based System Using Holt-Winters and Genetic Algorithm With Fuzzy Logic for DoS/DDoS Mitigation on SDN Networks.* Brazil: IEEE.

Jadhav, M. S. (2016). *Study on Web DDOS Attacks Detection Using Multinomial Classifier.* Mumbai: IEEE.

K. Hong, Y. K. (2018). *SDN-Assisted Slow HTTP DDoS Attack Defense Method.* Korea: IEEE.

Kian Son Hoon, K. C. (2018). *Critical review of machine learning approaches to apply big data analytics in DDoS forensics .* Australia: IEEE.

Koay, A. M. (2019). *Detecting High and Low Intensity Distributed Denialof Service (DDoS) Attacks.* Wellington: IEEE.

L. Barki, A. S. (2016). *Detection of distributed denial of service attacks in software defined networks.* Jaipur: IEEE.

Mahadev, V. K. (2016). *Classification of DDoS Attack Tools and Its Handling Techniques and Strategy at Application.* Haridwar: IEEE .

Md.Khamruddin, D. C. (2013). *A Rule Based DDoS Detection and Mitigation Technique.* IEEE.

Mitrokotsa, C. D. (n.d.). *DDOS ATTACKS AND DEFENSE MECHANISMS: A CLASSIFICATION.* Greece: IEEE.

Mohd. Jameel Hashmi, M. S. (2019). *Classification of DDoS Attacks and their Defense Techniques using Intrusion Prevention Systems.* Rajasthan: International Journal of Computer Science & Communication Network.

P. Kamboj, M. C. (2017). *Detection techniques of DDoS attacks: A survey.* Mathura: IEEE.

Paxson, V. (2001). *An analysis of using reflectors for distributed denial-of-service attacks.* New York: ACM.

Qiao Yan, F. R. (2016). *Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges.* IEEE.

Reiher, J. M. (2002). Los Angles: IEEE.

Sankardas Roy, C. E. (2010). *A Survey of Game Theory as Applied to Network Security.* Memphis: IEEE.

Sundar, S. K. (2016). *Blue Screen of Death Observed for Microsoft Windows Server 2012 R2 under DDoS Security Attack.* Texas: Journal of Information Security.

T. M. Thang, C. Q. (2018). *Synflood Spoofed Source DDoS Attack Defense Based on Packet ID Anomaly Detection with Bloom Filter.* Hanoi: IEEE.

Tapaswi, N. A. (2017). *A Lightweight Approach to Detect the Low/High Rate IP Spoofed Cloud DDoS Attacks.* Gawalior: IEEE.

U. Dincalp, M. S. (2018). *Anomaly Based Distributed Denial of Service Attack Detection and Prevention with Machine Learning.* Ankara: IEEE.

Wooldridge, M. (2012). *Does Game Theory Work?* IEEE.

Zhijun WU, C. W. (2011). *Research on the Comparison of Flood DDoS and Low-rate DDoS .* Tianjin: IEEE.