# Naïve Bayes Anomaly Detection System Design On Openflow Network

Nehemia Edbertus<sup>1</sup>, Samuel Hutagalung<sup>2</sup>, Hargyo Tri Nugroho<sup>3</sup> Multimedia Nusantara University: Departement of Computer Engineering, Tangerang, Indonesia

> Accepted on 11 July 2019 Approved on 20 December 2019

Abstract— One of the generally launched attacks is Distributed Denial of Service that renders its target unable to provide its service. Gaussian Naïve Bayes Classifier is one out of several techniques used in detecting those attacks by classifying network traffic in a window as an attack or a normal traffic based on normal distribution previously calculated from normal and attack traffic datasets. This research focuses on mitigating SYN Flood Type DDoS attacks on OpenFlow Network using Zodiac FX as a switch. The developed system utilizes OpenFlow Protocol to apply flow rule in switch's flow table in order to detect and mitigate SYN Flood attacks in real-time. Applied mitigation procedure is to divert incoming packets into SYN Proxy so that only legitimate TCP packets are able to reach the server. The results show that the system has a bandwidth of up to 60Mbps under normal condition and 5.03Mbps under attack. Maximum malicious packets that could reach server before it is diverted to SYN Proxy is estimated to be 400 packets and not affected by the number of attacks, assuming that the flow rule sent by the controller are enacted immediately.

#### Index Terms— DDoS Mitigation, Naïve Baye, OpenFlow Protocol, SYN Proxy, Zodiac FX

#### I. INTRODUCTION

With the development of services and content available on the internet, network security has become a very important part in it. The advancementin network security is due to increasing number of various crimes in cyberspace. One type of attack that is well known and is still frequently launched is Denial of Service (DoS) which is renders its target unable to run its services [1].

Symantec Corporation in its annual report, 2017 Internet Security Threat Report, published in April 2017 describes a new trend of DDoS attacks that utilize various Internet of Things (IoT) devices that have a low level of security as a tool to launch DDoS attacks. One of the notable incidents was when Mirai (botnet consisting of IoT devices) managed to do DDoS on a DNS company called Dyn, which resulted in obstruction of access to several well-known websites such as Netflix, Twitter and Paypal [2]. Another report on DDoS attack fromKasperskyLab for the fourth quarter of 2017 stated that among all DDoS attack methods, SYN Flood was reported as the most frequently launched attack method with a percentage reaching 55.63% of all existing DDoS attacks as shown in Figure 1 [3].



Figure 1.Distribution of DDoS Attacks by Type in Q4 2017 [3]

Various solutions for detecting DDoS attacks, especially the type of SYN Flood attack have been developed and one of them is "Implementation of Count-Min Sketch on Naïve Bayes Anomaly Detection System". The research compares the performance of an anomaly detection system using a count-min sketch data structure with a data structure linked to the Naïve Bayes Classifier to read patterns of captured network traffic and determine the occurrence of attacks. Another related research is [4] which has successfully implemented Bloom Filter to detect DDoS on OpenFlow networks. In addition, [7] has conducted research on HTTP Flood detection using Naïve Bayes and can detect SYN Flood with 99.8% accuracy. Lastly, [6] utilizeOpenFlow controller's ability to mitigate attacks by diverting and enforcing special actions against the suspected maliciouspackets. By manipulating incoming packets to be sent to its destination and detection system simultaneously, each incoming packet can be analyzed and forwarded concurrently.If analyzed packets found to exceed the calculated threshold, it can be concluded that the flow is an attack. This research proposed to do mitigation based on current network condition so that under normal circumstances, all incoming packets can directly access the server, otherwise it will be filtered before reaching the server.

## ISSN 2355-0082

With those goal in mind, this research is built on OpenFlow protocol which in recent years have been gaining more attention and is predicted to be the future of network technology. While still being under continuous development, this protocol is fully functional. Using this protocol, user can manipulate switches behavior by programming flow tables in various switch that supports this protocol [6] and [7] and consistently produce identical behavior.

In order to detect SYN Flooding, this research used gaussian naïve bayes classifier, a machine learning technique to classify a sets of data based on their feature. Before used to classify, it needs to be trained using existing data belonged to specific classes. While assuming each feature is has no corelation or independent from one another, most cases were violating this assumption, but even with corelation or dependencies between its feature, Harry Zhang proves in his research [4] that naïve bayes could still work optimally. In gaussian naïve bayes, it used normal or gaussian distribution in representing its probabilistic value from each feature for each class. First, estimating normal distribution from training data sets by calculating mean( $\mu$ ) and variance( $\sigma^2$ ) for each feature, then prior probability(p(Cn)) of each classes.

$$p(C_n) = \frac{N_c}{\Sigma(N_c)} \quad (1)$$

$$p(X_i|C) = \frac{1}{\sqrt{2\pi\sigma_c^2}} exp\left(-\frac{(X_i - \mu_C)^2}{2\sigma_c^2}\right) \quad (2)$$

$$p(X|C) = p(X_1|C) * p(X_2|C) * \dots * p(X_n|C) \quad (3)$$

$$P(C_n|X) = \frac{p(X|C_1) * p(C_1)}{p(X|C_1) * p(C_1) + p(X|C_2) * p(C_2) + \dots + p(X|C_n) * p(C_n)} \quad (4)$$

Equation (1) represents prior probability of a class based on its training data sets, where C is class and N is number of event for each class. Equation (2) shows probability of a feature(X<sub>i</sub>) for class(C). Equation (3) shows probability of a data(X) for class(C), where based on naïve bayes assumptions of independencies, every feature for class from equation (2) is multiplied. Equation (4) is the final probabilistic value, predicting the percentage of a class(C) for the data(X) where the result from equation (3) is multiplied with its classes prior proability from equation (1) and divided by the sum of every result from equation (3) multiplied with equation (1) for each class. The class probability with highest value is the predicted class for the data.

$$Multiplier = \frac{2}{TimePeriods + 1}$$
(5)

EMA = (CurrentValue - PreviousEMA) \* Multiplier + PreviousEMA (6)

While to produce a false-positive-proofed system, exponential moving average could be used to determine current trends while keeping track of several previous record of current condition, but put extra weigh on current condition as seen in equation (5) and (6).

#### II. RESEARCH METHOD



Figure 2 shows system's block diagram. Incoming packet will be copied and forwarded to anomaly detection system to be analyzed by extracting its features in buffer. Buffered packet features will then sent to naïve bayes classifier to be classified as normal or malicious flow. If the number of malicious flow is greater than normal flow, the buffer would be concluded as an attack attempt and vice versa. This current condition would then further calculated in exponential moving average module so that the final outcome of current condition would have less false positive. This final outcome will determine which rule enacted by the OpenFlow switch.



Figure 3. Packet Flow Under Normal Condition

Figure 3 shows incoming packetswill be forwarded directly to server by OpenFlow Switch and there is no means to communicate with SYN Proxy directly from the switchunder normal condition.



Figure 4. Packet Flow Under Attacked Condition

However, when under attack, a new set of rules will be enforced, preventing all incoming packet from directly communicating with server by diverting those packets to a SYN Proxy server as shown in figure 4. SYN Proxy server would be filtering all incoming packets and forward legitimate request only so that legitimate user can still access the server and the server wouldn't receive devastating number of malicious packets that potentially exhaust its resources and crashes the server, resulting in greater loss.

Main()
set UNDER ATTACK = false
set BUFFER TRESHOLD = 100
set MOVING AVERAGE VALUE = 0
set MOVING AVERAGE TIME PERIOD = 10
set MOVING AVERAGE MULTIPLIER = 2/(MOVING AVERAGE TIME PERIOD+1)
switch.start()
controller.start()
switch.onPacketReceived(incomingPacket)
forwardBasedOnRule(incomingPacket)
procedure forwardBasedOnRule(packet)
if(packet is tcpPacket)
cloneToController(packet)
if (UNDER_ATTACK)
forwardToSYNProxy(packet)
else
forwardToServer(packet)
Figure 5.Handling Incoming Packet Pseudocode

This research utilize OpenFlow Switch capabilities to forward packets based on enforced flow rules. Figure 5 shows how system is initialized and handles incoming packet events on switch. If the packet is a tcp packet, it will be cloned and forwarded to controller while simultaneously forwarded it to its destination based on system UNDER ATTACK state (to server if UNDER\_ATTACK set to false and to SYN proxy if true).

```
procedure BufferTCPPacket(packet)
    set flow (packet.srcIP, packet.destIP, packet.dstPort)
buffer[flow].append(packet.features)
    increment bufferSize
controller.on(packetReceived)
foreach packet receivedBy controller
     BufferTCPPacket (packet)
    if (bufferSize == BUFFER_TRESHOLD)
AnalyzeBufferWindow(buffer)
          reset buffer
               Figure 6. Buffering Packet Pseudocode
```

Figure 6 explains how cloned TCP packets is buffered in controller. Each received packet's feature will be buffered and when buffer size reach predetermined threshold (BUFFER TRESHOLD in Figure 5), buffer will be analyzed and then resetted.

```
procedure AnalyzeBufferWindow(buffer)
    set normalFlow 0
    set anomalyFlow 0
foreach flow in buffer
        set class = GaussianNaiveBayes(flow.features)
if(class == anomaly)
             increment anomalyFlow
        else
             increment normalFlow
    else
    condition = normal
set UNDER_ATTACK = ExponentialMovingAverage(condition)
              Figure 7. Analyze Buffer Pseudocode
```

Figure 7 shows how buffer is analyzed by classifying each flow in buffer using Gaussian Naïve Bayes Classifier. Condition will be set to anomaly if anomalyFlow counts more than normalFlow, and vice versa. System UNDER ATTACK state will be determined by ExponentialMovingAverage calculation based on current condition as shown in figure 8 below.

tion -- anomal \*MOVING\_AVERAGE\_MULTIPLIER + MOVING\_AVERAGE\_VALU

Figure 8 shows how system determined UNDER ATTACK state by calculating current MOVING AVERAGE VALUE using exponential If moving average. current MOVING AVERAGE VALUE is more than 0.5, UNDER ATTACK will be set to true and if less than 0.5to false. Bv setting MOVING AVERAGE TIME PERIOD to 10 event and BUFFER TRESHOLD to 100 packets, maximum number of anomaly packets received by server can hypothetically be calculated as shown in Table 1 below.

Event#	anomaly_value	EMA	condition	anomaly_packet	anomaly packet received by server	anomaly packet diverted
1	False	0	Normal	0	0	0
2	True	0.181818	Normal	100	100	0
3	True	0.330579	Normal	100	100	0
4	True	0.452292	Normal	100	100	0
5	True	0.551875	Anomaly	100	100	0
6	True	0.633352	Anomaly	100	0	100
7	True	0.700015	Anomaly	100	0	100
8	True	0.754558	Anomaly	100	0	100
9	True	0.799184	Anomaly	100	0	100
10	True	0.835696	Anomaly	100	0	100
11	True	0.865569	Anomaly	100	0	100

Assuming incoming attacks is a bursting 1000 TCP SYN packets with the speed of 10 packets per second and all flow rules sent by controller are enacted immediately, then maximum number of anomaly packets received by server can be estimated to 400 packets or 4 anomaly events before flow rule to divert incoming packets to syn proxy enactedas shown intable 1. Event #2 up to #11 is an attack, on event#5, EMA value pass over 0.5 and acknowledged as an anomaly. This change on condition triggers controller to enact a mitigation rule on OpenFlow switch and from event #6 onward, all packets is diverted to SYN Proxy until EMA value return under 0.5 and triggers controller to revoke mitigation rule on OpenFlow switch.

This research use HPING3 to generate SYN Flood attack to be used in training naïve bayes classifier as anomaly traffic dataset and testing. Testing will be conducted real-time by client accessing a http server under normal condition and under attack by HPING3 SYN Flood condition. System throughput will be tested using iperf on normal and mitigation rule. Testing will be conducted using a laptop with specification Intel core i7 processor, 8GB RAM running Ubuntu Linux VMWare on top Windows10 as OpenFlow controller, 2 PC with specification Intel core i5, 8GB RAM running Windows10 as client and server and another PC with same specification as client/server running Ubuntu Linux VMWare on top of Windows10 as SYN Proxy, and a Zodiac FX as OpenFlow switch.

Figure 8. Exponential Moving Average Pseudocode

#### III. RESULTS AND ANALYSIS

#### A. Mitigation

Using HPING to generate SYN Flood attacks with random source IP designated to the server, the results is shown in figure 9 and 10 below.

tep 8& ip.src! = 172.17.1.201 8& ip.src! = 172.17.1.202 8& ip.src! = 172.17.1.203 8& ip.src! = 172.17.1.101							
. Time	Source	Destination	Protocol	Length Info			
4123 69.217430	209.196.98.172	172.17.1.101	TCP	60 2226 → 80 [SYN] Seq=0 Win=512 Len-			
4125 69.319172	147.211.228.162	172.17.1.101	TCP	60 2227 → 80 [SYN] Seq=0 Win=512 Len-			
4127 69.423541	214.58.136.209	172.17.1.101	TCP	60 2228 → 80 [SYN] Seq=0 Win=512 Len-			
4129 69.526186	98.213.84.1	172.17.1.101	TCP	60 2229 → 80 [SYN] Seq=0 Win=512 Len-			
4131 69.627842	143.53.221.183	172.17.1.101	TCP	60 2230 → 80 [SYN] Seq=0 Win=512 Len-			
4133 69.729510	78.24.25.228	172.17.1.101	TCP	60 2231 → 80 [SYN] Seq=0 Win=512 Len-			
4135 69.830708	54.122.224.23	172.17.1.101	TCP	60 2232 → 80 [SYN] Seq=0 Win=512 Len-			
4137 69.932633	227.87.176.201	172.17.1.101	TCP	60 2233 → 80 [SYN] Seq=0 Win=512 Len=			
4138 70.034102	120.240.71.216	172.17.1.101	TCP	60 2234 → 80 [SYN] Seq=0 Win=512 Len=			
4140 70.135434	199.19.146.227	172.17.1.101	TCP	60 2235 → 80 [SYN] Seq=0 Win=512 Len:			
Frame 4123: 60 bytes	s on wire (480 bits).	60 bytes captured (4	480 bits)				
Ethernet II. Src: Ve	ware 38:6c:aa (00:50	:56:38:6c:aa), Dst: 0	Siga-Byt 99:0	8d:8c (1c:1b:0d:99:0d:8c)			
Internet Protocol Ve	ersion 4. Sec: 209.19	6.98.172. Dst: 172.17	7.1.101	(,			
Transmission Control	Protocol, Src Port:	2226, Dst Port: 80.	Seg: 0, Len:	: <b>0</b>			
100 1c 1b 0d 99 0d 8	c 00 50 56 38 6c aa	08 00 45 00	-P V81E-				
7 test overall server	eth0 new pcap			Packets: 7402 : Displayed: 305 (5 3%)			
	0	4		robest fire bigstycar and other			
Fig	ure 9. Canti	ired SYN Fl	lood Re	eceived by Server			
5	are of oup of						
				1 101			
tcp && ip.src != 172.17.1.20	11 aa/p.src 1= 172.17.1.2020	salpisici = 1/2.1/.1.203 da	p.src (= 1/2.1/.)				
tcp && ip.src != 172.17.1.20 Time	Source	Destination	Protocol	Length Info			
tcp && ip.src != 172.17.1.20 Time 1 0.000000	Source 53.63.94.240	Destination 172.17.1.101	Protocol TCP	Length Info 60 2622 + 80 [SYN] Seq=0 Win=512 Len=			
tep 8& ip.src != 172.17.1.20 Time 1 0.000000 2 0.101250	Source 53.63.94.240 13.93.127.250	Destination 172.17.1.101 172.17.1.101	Protocol TCP TCP	Length Info 60 2622 + 80 [SYN] Seq=0 Win=512 Len 60 2623 + 80 [SYN] Seq=0 Win=512 Len			
tcp 88 ip.src != 172.17.1.20 Time 1 0.000000 2 0.101250 3 0.211691	Source 53.63.94.240 13.93.127.250 116.180.83.100	Destination 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101	Protocol TCP TCP TCP	Lengh Info 60 2622 + 80 [SYN] Seq=0 Win=512 Len- 60 2623 + 80 [SYN] Seq=0 Win=512 Len- 60 2624 + 80 [SYN] Seq=0 Win=512 Len- 60 2624 + 80 [SYN] Seq=0 Win=512 Len-			
tep 8& ip.src != 172.17.1.20 Time 1 0.0000000 2 0.101250 3 0.211691 4 0.304147	Source 53.63.94.240 13.93.127.250 116.180.83.100 230.244.83.200	Destination 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101	Protocol TCP TCP TCP TCP	Length         Info         Comparison           60         2622 → 80         [SYN]         Seq=0         Min=512         Lenn           60         2623 → 80         [SYN]         Seq=0         Min=512         Lenn           60         2624 → 80         [SYN]         Seq=0         Min=512         Lenn           60         2625 → 80         [SYN]         Seq=0         Min=512         Lenn			
tep 8& ip.src != 172.17.1.20 Time 1 0.000000 2 0.101250 3 0.211691 4 0.304147 5 0.405508	Source 53.63.94.240 13.93.127.250 116.180.83.100 230.244.83.200 192.140.192.66	Destination 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101	Protocol TCP TCP TCP TCP TCP TCP	Longht         Info           600         2622 + 80         [SVN]         Seq=0         Min=512         Lenn           60         2622 + 80         [SVN]         Seq=0         Min=512         Lenn           60         2624 + 80         [SVN]         Seq=0         Min=512         Lenn           60         2624 + 80         [SVN]         Seq=0         Min=512         Lenn           60         2626 + 80         [SVN]         Seq=0         Min=512         Lenn           60         2626 + 80         [SVN]         Seq=0         Min=512         Lenn			
tep 8& ip.src   = 172.17.1.20 Time 1 0.0000000 2 0.1012500 3 0.211691 4 0.304147 5 0.495586 6 0.506878 6 0.506878	Source Source 53.63.94.240 13.93.127.250 116.180.83.100 230.244.83.200 192.140.192.66 193.179.73.247	Destnation 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101	Protocol TCP TCP TCP TCP TCP TCP TCP	Longth         Info           60         2622         80         [SWN]         Seq=0         Min=512         Len           60         2622         80         [SWN]         Seq=0         Min=512         Len           60         2624         80         [SWN]         Seq=0         Min=512         Len           60         2625         80         [SWN]         Seq=0         Min=512         Len           60         2627         80         [SWN]         Seq=0         Min=512         Len           60         2627         80         [SWN]         Seq=0         Min=512         Len			
tep 8& ip.sec 1 = 172.17.1.20 Tme 1 0.0000000 2 0.101250 3 0.211691 4 0.304147 5 0.405508 6 0.566878 7 0.608331 - 0.00031	Source 53.63.94.240 13.93.127.250 116.180.83.100 230.244.83.200 192.140.192.66 133.179.73.247 82.178.174.194	Destination 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101	Protocol TCP TCP TCP TCP TCP TCP TCP TCP TCP	Longh         Longh <th< td=""></th<>			
tep 8& p.set (= 172.17.120 Tme 1 0.000000 2 0.101250 3 0.211691 4 0.304147 5 0.405508 6 0.506878 7 0.688331 8 0.709742	Saurce 53,63,94,240 13,93,127,250 116,180,83,100 230,244,83,200 192,140,192,66 193,179,73,247 82,178,174,194 125,203,122,13	Destination 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101	Protocol TCP TCP TCP TCP TCP TCP TCP TCP TCP	Use         Use           (Brgh)         Infg           (Brg)         2622 + 80           (String)         Seq=0           (Brg)         2624 + 80           (String)         Seq=0           (Brg)         2624 + 80           (String)         Seq=0           (Brg)         Seq=0			
tep 8& p.set (= 172.17.120 Time 1 0.000000 2 0.101250 3 0.211691 4 0.304147 5 0.495506 6 0.506878 7 0.608331 8 0.709742 9 0.811091	Sauce Sauce 13. 63.94.240 13. 93.127.250 116.180.83.100 230.244.83.200 192.140.192.66 193.179.73.247 82.178.174.194 125.203.122.13 152.23.36.151	Destination 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101 172.17.1.101	Protocol TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Lingth         Inf         Lingth         Inf           69         2622 + 60         (SNI)         SeqP0         Min-S32         Len           69         2624 + 60         (SNI)         SeqP0         Min-S32         Len           69         2624 + 60         (SNI)         SeqP0         Min-S32         Len           69         2624 + 60         (SNI)         SeqP0         Min-S32         Len           69         2626 + 60         (SNI)         SeqP0         Min-S32         Len           69         2627 + 60         (SNI)         SeqP0         Min-S32         Len           69         2629 + 60         (SNI)         SeqP0         Min-S32         Len           60         2629 + 60         (SNI)         SeqP0         Min-S32         Len           60         2629 + 60         (SNI)         SeqP0         Min-S32         Len			
tep 8& p.src  = 172.17.120 Time 1 0.0000000 2 0.101250 3 0.211691 4 0.304147 5 0.405506 6 0.566678 7 0.608331 8 0.709742 9 0.811091 10 0.912449 10 0.912449	Source 53.63.94.240 13.93.127.250 116.180.83.100 129.140.192.66 193.179.73.447 82.176.174.194 125.263.122.13 129.195.222.201 129.195.222.201	Decination 172, 17, 1, 101 172, 173, 102 173, 174 174, 175 174, 175 175 175, 175 175, 17	Protocol TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Unit         Unit           Gep 1         Info           60         2622 + 80           60         2623 + 80           60         2623 + 80           60         2623 + 80           60         2624 + 80           60         2625 + 80           60         2625 + 80           60         2626 + 80           60         2627 + 80           60         2626 + 80           60         2626 + 80           60         2627 + 80           60         2627 + 80           60         2627 + 80           60         2627 + 80           60         2627 + 80           60         2627 + 80           60         2627 + 80           60         2628 + 80           60         2629 + 80           60         2629 + 80           60         2639 + 80           60         2639 + 80           60         2639 + 80           60         2639 + 80           60         2639 + 80           60         2639 + 80           60         2639 + 80			
Image         1         0.000000           1         0.000000         0.010120           2         0.101250         0.010120           3         0.211691         4         0.304147           5         0.405508         6         6.506578           7         0.608331         8         0.709742           9         0.811091         1         0.912449           11         1.013788	Sarce 53.63.94.240 13.93.127.250 116.180.83.100 230.244.83.200 192.140.192.65 193.179.73.247 62.176.174.194 152.283.6151 239.155.222.201 185.253.143.210	Decination 172, 17, 1, 101 172, 17, 1, 101	Protocol TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Upp         Date         Upp         Upp           69         2622 + 80         [SM]         SeqP0 Min-512 Lenn           69         2623 + 80         [SM]         SeqP0 Min-512 Lenn           69         2623 + 80         [SM]         SeqP0 Min-512 Lenn           69         2625 + 80         [SM]         SeqP0 Min-512 Lenn           69         2625 + 80         [SM]         SeqP0 Min-512 Lenn           69         2626 + 80         [SM]         SeqP0 Min-512 Lenn           69         2628 + 80         [SM]         SeqP0 Min-512 Lenn           69         2628 + 80         [SM]         SeqP0 Min-512 Lenn           69         2629 + 80         [SM]         SeqP0 Min-512 Lenn           69         2531 + 80         [SM]         SeqP0 Min-512 Lenn           69         2531 + 80         [SM]         SeqP0 Min-512 Lenn			
Ips 84 p.src  = 172.171.20           The           1         0.869060           2         0.101250           3         0.211691           4         0.36147           5         0.465508           6         0.566578           7         0.668331           8         0.769742           9         0.811691           10         0.912449           11         1.013788           12         1.115247	Source Source 53.63.94.240 13.93.127.259 116.130.83.190 239.244.83.200 192.140.192.65 193.179.73.247 192.178.174.194 125.203.122.13 129.155.222.201 135.253.143.210 136.191.247.47	Destination 172, 17, 1, 101 172, 17, 1, 101	Protocol TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Bet         Due         Due           60         2623 + 40         (SM)         Seq40         Min-S32         Lens           60         2624 + 40         (SM)         Seq40         Min-S32         Lens           60         2624 + 40         (SM)         Seq40         Min-S32         Lens           60         2625 + 40         (SM)         Seq40         Min-S32         Lens           60         2626 + 40         (SM)         Seq40         Min-S32         Lens           60         2627 + 40         (SM)         Seq40         Min-S32         Lens           60         2626 + 40         (SM)         Seq40         Min-S32         Lens           60         2630 + 40         (SM)         Seq40         Min-S32         Lens           60         2630 + 40         (SM)         Seq40         Min-S32         Lens           60         2631 + 40         (SM)         Seq40         Min-S32         Lens           60         2631 + 40         (SM)         Seq40         Min-S32         Lens           60         2631 + 40         (SM)         Seq40         Min-S32         Lens           60         2632 + 40 <t< td=""></t<>			
tra 84 p.src   = 172.17.120 Ter 1 0.000000 2 0.101250 3 0.211691 4 0.304147 5 0.405508 6 0.506578 7 0.608331 8 0.709742 9 0.811091 10 0.912449 11 1.013788 12 1.11547 13 1.216619	Sarce 5.4 5.4 5.4 5.4 5.4 5.4 5.4 5.4	Certination 172, 17, 1, 161 172, 17, 1, 161	Protocol TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Upp         Upp         Upp           100ph         Indp         100ph         50ph         50p			
Ins S& p.sr. (= 172.17.120)           The           The           0.0809000           2 0.101250           3 0.211691           4 0.304147           5 0.405508           6 0.566578           7 0.668331           8 0.709742           9 0.811091           10 0.512409           11 0.013788           12 1.013788           12 1.013781           13 1.216619           14 1.317796	Source Source 53.63.94.240 13.93.127.259 116.180.83.100 239.244.83.200 192.140.192.66 193.179.73.247 25.178.174.194 125.223.6151 239.195.222.201 185.253.143.210 186.191.247.47 125.47.127.147 193.136.121	Derivative 172, 17, 1, 161 172, 17, 1, 161	Protocol TCP TCP TCP TCP TCP TCP TCP TCP	Bet         Due         Due           60         2623 + 40         (SM)         SeqPE Min-SSL Lens           60         2624 + 40         (SM)         SeqPE Min-SSL Lens           60         2624 + 40         (SM)         SeqPE Min-SSL Lens           60         2624 + 40         (SM)         SeqPE Min-SSL Lens           60         2625 + 40         (SM)         SeqPE Min-SSL Lens           60         2626 + 40         (SM)         SeqPE Min-SSL Lens           60         2626 + 40         (SM)         SeqPE Min-SSL Lens           60         2626 + 40         (SM)         SeqPE Min-SSL Lens           60         2628 + 40         (SM)         SeqPE Min-SSL Lens           60         2638 + 40         (SM)         SeqPE Min-SSL Lens			
Ipp B&B, p.sr. (= 77.17.12)           Ter           Ter           0.808080           2.0.181258           3.0.211691           4.0.384147           5.0.485506           6.0.586576           7.0.686371           8.0.799742           9.0.811991           1.0.13788           1.1.12547	Source 563, 94, 240 1393, 127, 259 116, 180, 83, 100 250, 244, 83, 200 192, 140, 192, 66 193, 129, 73, 247 83, 179, 73, 247 82, 176, 174, 194 152, 263, 122, 13 152, 22, 36, 151 259, 155, 222, 201 195, 255, 143, 210 195, 471, 127, 147 59, 139, 136, 121 211, 201, 25, 152	Cerimation 172, 17, 1, 101 172, 17, 1, 101	Probability           Probability           TCP           TCP <td>Upper         Upper         Upper           100ph         Indp         1</td>	Upper         Upper         Upper           100ph         Indp         1			
Imp S&E part (= 72, 17, 12)           The           1         0.000000           2         0.101250           3         0.211691           4         0.304147           5         0.405500           6         0.506578           7         0.608331           8         0.709742           9         0.811091           10         0.912449           11         1.013788           12         1.11547           13         1.216619           14         1.317796           15         1.419631           14         1.317796	Source 53.63.94.240 13.93.127.250 116.180.83.100 192.140.192.66 193.179.73.247 62.178.174.194 155.263.122.13 152.223.86.151 259.155.222.201 186.151.221.343.210 186.191.247.47 125.47.127.147	Certination 172, 17, 1, 101 172, 17, 1, 101	Protocol           TCP	Both         Date         Date           Corph         Job         Seq.PM (Job Sci.PM (Jo			
ttp:8k3.perc (= 172.17.12)           Tree           1         0.000000           2         0.101250           3         0.211601           4         0.304147           5         0.40550           6         0.50607           7         0.40540           18         0.706742           9         0.81101           19         0.91240           11         1.01276           13         1.25619           14         1.317619           15         1.41832           20         1.61831	Source 53,63,54,240 13,93,127,759 116,180,83,100 192,144,192,66 193,179,73,247 193,179,73,247 193,179,73,247 193,179,73,247 193,179,73,247 193,179,73,247 193,193,194,194 195,253,145,210 195,194,194 195,194,194 195,194,194 195,194,194 195,194,194 195,194,194 195,194,194 195,194,194 195,195,195,195,195,195,195,195,195,195,	Destination 172,17,7,1,101 172,17,7,1,101 172,17,7,1,101 172,17,1,101	Protocol TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Upp         Info         Upp         Upp           60         2622         80         [SYN]         Seq40         Min-312         Len           60         2623         80         [SYN]         Seq40         Min-312         Len           60         2623         80         [SYN]         Seq40         Min-312         Len           60         2624         80         [SYN]         Seq40         Min-321         Len           60         2624         80         [SYN]         Seq40         Min-321         Len           60         2626         60         [SYN]         Seq40         Min-321         Len           60         2626         60         [SYN]         Seq40         Min-321         Len           60         2628         60         [SYN]         Seq40         Min-321         Len           60         2631         60         [SYN]         Seq40         Min-321         Len           60         2634         60         [SYN]         Seq40         Min-321         Len           60         2634         60         [SYN]         Seq40         Min-321         Len           60			
Term         0.000000           2.0.1228         0.001000           2.0.10129         0.01129           3.0.11610         0.00107           4.0.00107         0.00117           5.0.00107         0.00117           6.0.0011         0.00117           7.0.00117         0.00117           9.0.00117         0.00117           10.0.01249         0.011249           11.0.01276         1.01249           12.1.15247         1.115247           13.1.216619         1.115247           15.1.415811         1.115247           15.1.415811         1.115247	Source 53, 63, 54, 240 13, 93, 127, 759 116, 180, 83, 109 129, 140, 192, 66 129, 140, 192, 66 129, 140, 192, 66 129, 140, 192, 66 129, 140, 192, 67 125, 263, 122, 13 155, 263, 124, 127, 147 166, 191, 247, 47 123, 47, 127, 147 123, 421, 125, 129 123, 124, 125, 129 123, 124, 125, 129 124, 125, 129 124, 125, 129 125, 126, 126, 126 125, 126, 126, 126 125, 126, 126, 126 125, 126, 126, 126 125, 126 125, 126, 126 125, 1	Cestrator 172,17,1.101 174,17,101 174,17,17,101 174,17,17,101 174,17,17,101 174,17,17,101 174,17,17,101 174,17,17,101 174,17,17,101 174,17,17,101 174,17,17,101 174,17,17,101 174,17,17,17,17,17,17,17,17,17,17,17,17,17,	Protocol TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Upp         Inf         Upp         Inf           100         100         Sec0 400         Sec0 400         Sec0 400           100         2624 400         Sec0 400         Sec0 400         Sec0 400         Sec0 400           100         2624 400         Sec0			
Upp MA.purc (= 172.17.2)           Tree           1         0.000000           2         0.101250           3         0.211601           4         0.304147           5         0.43550           6         0.50417           9         0.211071           9         0.211071           10         0.20250           11         1.013768           12         1.115247           13         1.226619           14         1.137768           15         1.43881           16         1.45881           Frame 1:         16 Uptornet TL, Serci W	Barger 10, 27, 17, 20 53, 63, 54, 240 13, 33, 127, 759 116, 180, 83, 100 130, 244, 33, 200 130, 140, 312, 60 130, 140, 312, 60 151, 223, 140, 312, 61 155, 223, 140, 310, 310 155, 233, 140, 310, 310 155, 233, 140, 310 155, 255, 256, 310 155, 255, 310 155, 255, 310 155, 255, 310 155, 31	Cestration 172,17,1,101	Protocol TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Lingth         Info         Lingth         Info           60         2622         80         [SYN]         Seq0         Min-512         Len           60         2623         80         [SYN]         Seq0         Min-512         Len           60         2623         80         [SYN]         Seq0         Min-512         Len           60         2624         80         [SYN]         Seq0         Min-512         Len           60         2623         80         [SYN]         Seq0         Min-52         Len           60         2627         60         [SYN]         Seq0         Min-52         Len           60         2628         60         [SYN]         Seq0         Min-52         Len           60         2628         60         [SYN]         Seq0         Min-52         Len           60         2634         60         [SYN]         Seq0         Min-52         Len           60         2634         60         [SYN]         Seq0         Min-52         Len           60         2634         60         [SYN]         Seq0         Min-52         Len           60         2635			
Imp B&parce (= 172.17.2)           The           0.000000           2.0.101250           3.0.101250           3.0.101260           3.0.101260           3.0.101260           3.0.101260           3.0.101270           3.0.101210           3.0.10110           3.0.10110           3.0.10110           3.0.10110           3.0.10110           3.0.10110           3.0.10110           3.0.10110           3.1.10110	Barrer 51, 36, 344, 246 33, 36, 344, 246 13, 33, 127, 256 131, 134, 33, 136 132, 134, 33, 136 133, 134, 33, 136 133, 134, 33, 136 133, 134, 34, 134 135, 236, 345, 135 135, 233, 345, 234 135, 233, 345, 234 135, 233, 345, 234 135, 234, 245, 245, 234, 245, 245, 245, 245, 245, 245, 245, 24	Destruction 172, 177, 1.191 172, 177, 174 172, 177, 174 174, 175 174, 175 175 175 175 175 175 175 175 175 175	pot         Protocol           TCP         TCP           TCP </td <td>Up         Def         Def           100</td>	Up         Def         Def           100			
Upp MA.porc (= 172.17.2)           Tree           1         0.000000           2         0.101250           3         0.211601           4         0.304147           5         0.40550           6         0.50617           9         0.211071           10         0.20200           9         0.211071           10         0.212601           11         1.31768           12         1.132247           13         1.226619           14         1.317768           15         1.43881           16         1.458921           17         1.512669           16         1.458931           17         1.3126619           16         1.458931           17         1.458931           10         1.458931           10         1.458931           10         1.45931           11         1.45931           11         1.45931           11         1.45931           11         1.45931           11         1.45931           12         1.45041	Source 15.3.63.94.240 13.3.93.127.559 11.6.180.83.100 13.92.127.559 11.6.180.83.100 13.92.144.33.200 13.92.144.34.200 13.94.24.24.2	Centration 172,17,1,181 172,17,181 172,17,181 172,17,182 172,17,182 172,17,182 172,17,182 172,17,182 172,17,182 172,17,182 172,17,182 172,17,182 172,17,182 172,17,182 172,17,182 172,17,182 172,17,182 172,17,182 172,17,182 172,17,182 172,17,17,182 172,17,17,182 172,17,17,182 172,17,182 172,17,182 172,17,17,182 172,17,17,182 172,17,17,182 172,17,182 172,17,17,182 172,17,17,182 172,17,17,182 172,17,17,182 172,17,17,182 172,17,17,182 172,17,17,182 172,17,17,182 172,17,17,17,17,172,172,172,172 172,172,172,172,172,172,172,172,172,172,	Part - 172 - 7 Protocol TCP TCP TCP TCP TCP TCP TCP TCP	Beth         Detect         Detect           (8)         2623 + 80         [SN]         SeqP Min-S21         Lens           (8)         2625 + 80         [SN]         SeqP Min-S21         Lens           (9)         2626 + 80         [SN]         SeqP Min-S21         Lens           (9)         2627 + 80         [SN]         SeqP Min-S21         Lens           (9)         2628 + 80         [SN]         SeqP Min-S21         Lens           (9)         2631 + 80         [SN]         SeqP Min-S21         Lens           (9)         2631 + 80         [SN]         SeqP Min-S21         Lens           (9)         2631 + 80         [SN]         SeqP Min-S21         Lens           (9)         2634 + 80         [SN]         SeqP Min-S21         Lens           (9)         2634 + 80         [SN]         SeqP Min-S21         Lens           (9)         2634 + 80         [SN]         SeqP Min-S21         L			
Trans         1         0.00000           1         0.000000         0.011250           2         0.010120         0.010120           3         0.11010         0.00000           4         0.00000         0.00000           5         0.00000         0.00000           6         0.00000         0.00000           10         0.011000         0.00000           11         0.011000         0.00000           12         0.011000         0.00000           14         0.011000         0.00000           15         1.40000         1.115200           15         1.40000         1.115200           15         1.40000         1.115200           15         1.40000         1.115200           16         0.012000         0.010000           16         0.010000         1.010000           16         0.000000         1.0100000	Barrer 57, 16, 26, 12, 26, 13, 33, 127, 2500 13, 33, 127, 2500 13, 33, 127, 2500 13, 13, 34, 127, 2500 13, 13, 144, 137, 260 139, 139, 139, 139, 146, 139, 146, 147, 147, 147, 147, 147, 147, 147, 147	Destruction 172,177,1.101 172,177,1.012 172,177,1.013 172,177,172,172	part         Protocol           Protocol         Protocol           TCP         TCP           Seg(a)         A, Lens           Litel         P V81E	Up         Up <thup< th="">         Up         Up         Up<!--</td--></thup<>			

Figure 10. Captured SYN Flood Diverted to SYN Proxy

Out of 1000 SYN flood packets sent, 394 packets received by server and the other 604 packets was successfully diverted to SYN Proxy. This results may vary depending on initial configuration on BUFFER\_TRESHOLD and MOVING\_AVERAGE\_TIME\_PERIOD as calculation in table 1 will change accordingly.

#### B. Equations

Using iperf, system's throughput is estimated under normal rule and mitigation rule as shown on table 2 below.

Table 2. System Th	roughput Test Result
Condition	Speed (Mbps)
Normal	60
Under Attack	5.03

This results shows the system have a throughput of 60Mbps on normal condition and the results mainly caused by Zodiac FX specification which has a 10/100Mbps ethernet port. Another factor that affects this result is the complexity of the flow tables at the time as more complex rules enacted, the slower transfer rate on OpenFlow switches gets. When mitigating attacks, the system has a throughput of 5.03Mbps. This gap between normal and under attack system performance is affected by Network Address Translation applied by SYN proxy to connect client and server when under attack. This results may vary when using SYN proxy, controller or OpenFlow switches with different specifications.

### IV. CONCLUSION

From this research developed system can detect and mitigate SYN Flood attacks on OpenFlow networks in real-time. The developed system has a throughput of 60Mbps under normal conditions and 5.03 Mbps when under attack. This speed can vary by using switches or controllers with different specifications. And maximum number of SYN Flood packets that can reach the server is estimated to be 400 packets without being affected by the number of attack packets sent with the condition that all flow rules sent by the controller are immediately applied and the rest will be transferred to SYN Proxy. This number can be tweaked to accommodate user preferences by changing buffer size treshold and moving average time period. Further development can be carried out to detect and mitigate other attacks on OpenFlow networks and use other classification method.

## References

- C. Patrikakis, M. Masikos and O. Zouraraki, "Distributed Denial of Service Attacks," The Internet Protocol Journal, vol. 7, no. 4, pp. 13-35, 2004.
- [2] Symantec Corporation, "Internet Security Threat Report 2017," p. 66, April 2017.
- [3] A. Khalimonenko, O. Kupreev and K. Ilganaev, "DDoS attacks in Q4 2017 - Securelist," 6 February 2018. [Online]. Available: https://securelist.com/ddos-attacks-in-q4-2017/83729/. [Accessed 10 March 2018].
- [4] P. Xiao, Z. Li, H. Qi, W. Qu and H. Yu, "An Efficient DDoS Detection with Bloom Filter in SDN," in IEEE TrustCom/BigDataSE/ISPA, Tianjin, 2016.
- [5] V. Katkar, A. Zinjade, S. Dalvi, T. Bafna and R. Mahajan, "Detection of DoS/DDoS attack against HTTP," in International Conference on Computing Communication Control and Automation, Pune, 2015.
- [6] Y.-K. Lai, C.-C. Lee, B.-H. Huang, T. Wellem, N.-C. Wang, T.-Y. Chou and H. T. Nugroho, "Real-time detection of changes in network with OpenFlow based on NetFPGA implementation," Microprocessors and Microsystems, vol. 38, no. 5, pp. 431-442, 2014.
- [7] Samuel, S., & Samudera, C, "Rancang Bangun Mekanisme Load Sharing Pada Link Aggregation Menggunakan Software Defined Networking," Ultima Computing : Jurnal Sistem Komputer, 9(1), 41-47, 2017.