Real Time Detection Of Network Attacks Using Signature Based Approach

Nikhil S. Mangrulkar

Dept. of Computer Technology Yeshwantrao Chavan College of Engineering Nagpur, India mangrulkar.nikhil@gmail.com

Snehal H. Chaflekar

Department of Information Technology Priyadarshini Bhagwati College of Engineering Nagpur, India snehalchaflekar@gmail.com

Abstract—Network attack detection is an essential technology in business as well as dynamic research area. It is essential for security of the information. Attacks on network can cause legitimate users being strived or denied services. A network attack detection approach is designed to detect attacks on network which follows the signature based methodology for determining attacks. In our proposed approach a log is maintained which displays the list of attacks initiated on the system to administrator for evasive action by generating alerts to control attacks on server.

Keywords- Network attack, Denial of Service, Signature based attack detection

I. INTRODUCTION

In computer networks, an attack is an effort to steal, disable, destroy, alter, or obtain unauthorized access to or to make unauthorized use of an asset. Network attacks can cause network services slow, temporarily unavailable, or down for a long duration of time. Therefore it is essential for users and network administrator to detect these attacks before they cause damage to the system. Achieving real-time under high-speed network intrusion is the challenge for the network intrusion detection technology.

Denial of Service (DoS) attacks has become a major threat to current computer networks. The aim of a denial of service attack is to oppose authorized users access to a particular resource. Known DoS attacks in the Internet generally conquer the target by exhausting its resources that can be anything related to network computing and service performance, such as TCP connection buffers, service/application buffers, link bandwidth, CPU cycles, etc. Individual attackers can also exploit vulnerability in the network, break in the target servers, and then bring down services. DoS attacks can be classified on the basis of the type of resources that is consumed.

A. Resource Flooding:

The attacker consumes victim's resources such as memory, CPU, hard disk to make it unavailable for normal users.

B. Bandwidth Flooding:

The attacker floods the victims' network by unwanted traffic to prevent the normal traffic from reaching the victim network.

II. TYPES OF ATTACK DETECTION SYSTEMS

Generally, the behaviour of an intruder is noticeably different from that of a legitimate user and hence can be detected [2]. Classification of the attack detection systems can be done the basis of their deployment in real-time.

A. Host Based Detection

The host based detection systems detects and examines the internals of a computing system rather than its external interfaces [2]. Such systems might detect internal activity such as which program accesses what resources and attempts illegitimate access. An example is a word processor that suddenly and inexplicably starts modifying the system password.

B. Network Based Detection

A network is connected to the rest of the world through the Internet. The Network based detection system reads all incoming packets or network traffic, trying to find suspicious patterns. For example, if a huge number of TCP connection requests to an extremely large number of different ports are observed within a short time, we could assume that someone is doing a "port scan" at some of the computer(s) in the network [2].

III. SIGNATURE BASED NETWORK ATTACK DETECTION

Just like many variants and forms of internet based threats are around the world, there are many different forms of protections against the threats. Signature based detection is one of the different forms of network attack detection that have been developed in order to keep network protected from attacks.

Signature-based attack detection can be argued to have been overshadowed by more sophisticated methods of attack detection in some environments; it is still a core technique for detecting network attacks and protecting network from attacks.

A. Working of Signature Based Detection

The working of signature-based detection is based on scanning the contents of packets received over the network interface and cross referencing their contents with the "attack signature" belonging to known attacks. If an attack signature is detected, the software acts to protect the system from the possible harm. Suspected packets are typically dropped in order to keep system working and available to legitimate users.

IV. PROPOSED WORK

A host based attack detection mechanism which focuses on detecting network attacks using signature based methodology is proposed in this paper. Proposed approach checks every packet received at the selected network interface for known attack patterns. A packet is classified as attack packet on detecting improper or missing fields of the received packet. This approach is used for detecting TCP attack packets and UDP attack packets. For detecting TCP-SYN flood and UDP flood attack, we have implemented rate limiting mechanism in which if number of packets received from a particular IP crosses the set threshold value within specified time, packets are classified as TCP flood attack packets.



Figure 7. Block diagram for attack detection

A. Algorithm

The proposed algorithm can be explained as below: Read packet from selected network interface If(Protocol == "TCP") Check(Source Port, Destination Port, Sequence

cheek(source i on, Destination i on, seque

Number, Header data, Checksum, Flags)

If all fields are valid

Classify as normal packet

else

Classify as TCP attack packet

endif

for each Source IP, Source Port & Destination Port if(Number of packets > TCP Threshold) Classify as TCP flood attack

else

```
Classify as normal traffic
```

endif

else If(Protocol == "UDP")

Check(Source_Port, Destination_Port, Checksum, Packet length)

If all fields are valid

Classify as normal packet

else

Classify as UDP attack packet endif for each Source IP, Source_Port & Destination_Port if(Number of packets > UDP Threshold) Classify as UDP flood attack

else

Classify as normal traffic

endif

endif

endif

B. Classifying TCP Attack Packets

Among all the packets that have been received on the selected network interface, for classifying an incoming TCP packet as an attacking packet various details of every packet has been checked. For TCP attack traffic following fields are checked-

- Sequence number of the packet If the sequence number of incoming packet is blank, it is invalid and packet is classified as attack packet.
- Source or destination Port number If the source or destination port number of incoming packet is invalid (0) then packet is classified as attack packet.
- TCP Header data If there is no data present in TCP header then such packet is classified as attack packet.
- Checksum If the packet is having blank checksum value then it is classified as attacking packet.
- Flags If all the flags of received TCP packet are set to zero then packet is classified as attack packet.

C. Classifying TCP SYN Flood Attack Packets

For classifying incoming packets as SYN Flood packets, rate limiting technique has been used. If number of packets that have being received from a particular IP and Port with its SYN flag set, crosses the threshold value that has been set, then those packets are classified as TCP-SYN flood attacking packets.

D. Classifying UDP Attack Packets

For classifying an incoming UDP packet as an attack packet various details of every packet has been checked. For detecting UDP attack traffic fields that have been checked are-

- Source or destination Port number If the source or destination port number of incoming packet is invalid (0) then packet is classified as attack packet.
- Checksum If the packet is having blank checksum value then it is classified as attacking packet.
- Length If the length of packet field of the received packet is 0 or blank, then it is classified as attack packet.

E. Classifying UDP Flood Attack Packets

For classifying incoming UDP packets as flood attacking packets, rate limiting technique has been used. If number of packets that have being received from a particular IP and Port crosses the threshold value that has been set, then those packets are classified as UDP flood attacking packets.

V. IMPLEMENTATION

For packet capturing and checking various fields of packets detection approach is developed using Microsoft® Visual Studio®.

Figure 2 shows user interface on which details of every packet that has been received on the selected network interface is displayed to the user/administrator. Details include: Source IP and Source port of the packet, Destination IP and Destination port, Type of packet (TCP / UDP), Data, In-time of packet and the time at which that packet was classified as attack packet, Remarks which specifies type of attack that has been classified by the approach. Options to set different threshold values for TCP flood and UDP flood attack is also provided to the administrator.

Figure 3 shows detection of TCP attack on the target system. Here packets those are highlighted using red color, indicates that those packets were classified as attack packets as one of the required field was having missing or improper value.

ttings						Thre	shold for Flood Attack		- 10
Packet Details	elect Network Ada	pter : 17	2.16.5.2	28		TOP	200 UDP	200 Set Values	<u>S</u> top
192.168.40.222-192.168.40.255	Source IP	Desti	S	De	Pro	Data	In-Time	Detection Time	Remarks
172.16.1.115-172.16.255.255	202.138.96.2	172.16	53	1026	UDP)808	14:30:22.3437500		
192.168.40.222-192.168.40.255	140.211.11.131	172.16	443	1183	TOP		14:30:22.3593750		
172.16.7.246-172.16.255.255	140.211.11.131	172.16	443	1183	TOP		14:30:26.4375000		
172.16.12.198-172.16.255.255	140.211.11.131	172.16	443	1184	TOP		14:30:26.4375000		
172 16 61 8-172 16 255 255	140.211.11.131	172.16	443	1184	TOP		14:30:29.3906250		
172 16 23 48-172 16 255 255	140.211.11.131	172.16	443	1185	TCP		14:30:29.3906250		
172 16 12 41 172 16 265 265	140.211.11.131	172.16	443	1185	TOP		14:30:32.4531250		
172.10.12.41-172.10.205.205	202.138.96.2	172.16	53	1026	UDP	10	14:30:32.5000000		
172.16.23.22-172.16.205.200	216.34.181.95	172.16	80	1186	TOP	100000	14:30:32.7500000		
172.16.1.6-172.16.255.255	216.34.181.95	172.16	80	1186	TOP	HTTP1.03	14:30:32.7656250		
172.16.25.25-172.16.255.255	216.34.181.95	172.16	80	1186	TOP		14:30:32.7656250		
172.16.61.8-172.16.255.255	216.34.181.95	172.10	80	1180	TOP		14:30:32.7968750		
172.16.61.8-172.16.255.255	172.10.1.0	172.10	80	1107	TOP		14:30:32.8125000		
172.16.61.8-172.16.255.255	172.16.1.6	172.10	80	1107	TOP	LITTEM 0.2	14.30.32.8437500		
172.16.17.67-172.16.255.255	172 16 1 6	172.16	80	1187	TOP	Cidortina ht	14:30:32.8750000		
172.16.8.137-172.16.255.255	172 16 1.6	172.16	80	1187	TOP	Il≤div align	14:30:32.8906250		
172.16.5.17-172.16.255.255	172161.6	172.16	80	1187	TOP	es - arr angen	14:30:32 9062500		
172 16 64 70-172 16 255 255	216 34 181 95	172.16	80	1186	TOP		14:30:34.6406250		
172 16 65 188-172 16 255 255	172.16.5.226	172.16	1962	139	TOP		14:31:17.6250000		
172 16 8 147-172 16 255 255	172.16.5.226	172.16	1962	139	TOP	0	14:31:17.6250000		
172 10 0 164 172 10 200 200	172.16.5.226	172.16	1962	139	TOP		14:31:17.6562500		
172.10.0.104-172.10.200.200	172.16.5.226	172.16	1982	139	TOP		14:31:17.6718750		
172-10-10.19-172-10-209-209	172.16.5.226	172.16	1983	139	TOP		14:31:17.6875000		
172.10.23.59-172.10.255.255	172.16.5.226	172.16	1963	139	TOP	0	14:31:17.7031250		
172.16.23.59-172.16.255.255	172.16.5.226	172.16	1963	139	TCP		14:31:17.7187500		
172.16.8.225-172.16.255.255	172.16.5.226	172.16	1963	139	TOP		14:31:17.7343750		
172.16.17.118-172.16.255.255	172.16.5.226	172.16	1963	139	TOP		14:31:17.7500000		
172.16.17.118-172.16.255.255	172.16.5.226	172.16	1963	139	TOP		14:31:17.7656250		
172.16.12.181-172.16.255.255	172.16.5.226	172.16	1963	139	TOP		14:31:17.7968750		
192.168.0.10-192.168.0.10	172.16.5.226	172.16	1963	139	TOP		14:31:17.8125000		
172.16.1.76-172.16.255.255	172.16.5.226	172.16	1963	139	TOP		14:31:17.8281250		
172 16 1 115-172 16 255 255	172.16.5.226	172.16	1963	139	TCP		14:31:17.8437500		
172 16 17 119-172 16 255 255	172.16.5.226	172.16	1963	139	TOP		14:31:17.8593750		
172 16 61 9-172 16 255 255	172.16.5.226	172.16	1963	139	TOP		14:31:17.8906250		
172.10.01.0172.10.200.200	172.10.5.226	172.10	1903	1.59	TOP		14:31:17.9062500		

Figure 8. Monitoring network traffic on selected network interface

ettings						Threat	hold for	Flood Attack			_	
Packet Details	S	elect Network Ad	apter : 172.16	i.5.228	~	TCP	200	UDP	200	Set Values	L	Stop
172.16.5.228-172.16.5.226	^	Source IP	Destination IP	Source Port	Destination Port	Protocol	Data	In-Time		Detection Time	Bernark	5
172 16 5 226-172 16 5 228		172.16.5.226	172 16 5 228	2936	445	TOP		14-42-32.3	906250			
172 16 5 228-172 16 5 226		172.16.5.226	172.16.5.228	2936	445	TCP		14:42:39.0	468750			
172 16 5 226-172 16 5 228		172.16.5.226	172.16.5.228	2936	445	TCP		14:42:39.0	625000			
172 16 5 228 172 18 5 220		172.16.5.226	172.16.5.228	2936	445	TCP		14:42:39.0	781250			
172.16.5.220-172.16.5.228		172.16.5.226	172.16.5.228	2936	445	TCP		14:42:39.1	718750			
172.10.5.220-172.10.5.220		172.16.5.226	172.16.5.228	2936	445	TCP		14:42:50.4	218750			
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	2936	445	TCP		14:42:50.4	375000			
172.16.5.226-172.16.5.228		172.16.5.226	172.16.5.228	2936	445	TOP		14:42:50.4	375000			
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	2936	445	TOP		14:42:50.4	531250			
172.16.5.228-172.16.5.228		172.16.5.226	172.16.5.228	2936	445	TCP		14:42:50.4	687500			
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	2936	445	TCP		14:42:50.4	843750			
172.16.5.226-172.16.5.228		172.16.5.228	172.16.5.228	0.	139	TCP		14:42:52.0	468750	14.42.52.0468750	Classife	d as TCP Attac
172.16.5.228-172.16.5.226		172.16.5.228	172 16 5 228	0	139	TCP		14.42.52.0		14.42.52.0625000	Gassife	a as TCP Attac
172.16.5.226-172.16.5.228		172.16.5.228	172 16 5 228	0	139	TOP		14/42/52.0		14.42.52.0781250	Classifie	a as TCP Attac
172 16 5 228-172 16 5 226		172185228	172 16 5 228	0	139	TCP TCP		14,42,52,0		14.42.52.0937500	Classifie	ac TCP Allac
172 16 5 228-172 16 5 228		172.16.5.226	172 16 5 228	0	1.38	TOP		14 42 52 1		14 42 52 1083750	Classifie	A as TUP Altac
172 16 5 228 172 16 5 226		172.16.5.226	172165228	0	139	107		14,42,02		14 42 52 1250000	Castone	A so TOP ANAC
172 16 5 220 172 16 5 220		17210.0220	172 16 5 228	0	100	100		14,40,50 4	C60200	14 42 52 1406250	Constanting of the local division of the loc	A set TOP And
172.10.0.220-172.10.0.220		172165226	172 18 5 228	0	100	TOP		14.42.02.1		14 42 52 1002000		A STOP AREA
172.16.5.228-172.16.5.226		172 18 5 228		0	139	TOP		14 42 52 1		14 42 52 1975000	Casarite	A NOTOP ANNO
172.16.5.226-172.16.5.228		172185226		0	134	TOP		14 42 52 1		14 42 52 2021 250		
172.16.5.228-172.18.5.226		172.18.5.226	172165228	0	139	TOP		14 42 52 2	031250	14 42 52 2831 256		d as TOP Allas
172.16.5.226-172.16.5.228		172.16.5.226	172165228	0	139	TOP		14 42 52 2	187500	14 42 52 2187500	Classific	d as TOP Attac
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	0	139	TOP		14 42 52 2	34,3750	14 42 52 2343750	Classoft	as TCP Atlan
172.16.5.226-172.16.5.228		172.16.5.226	172.16.5.228	0	139	TOP		14 42 52 2	500000	14:42:52:2500000	Classife	d as TCP Attac
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	0	139	TOP		14 42 57.8	281250	14-42:57 8281258	Classifie	d as TCP Allas
172.16.5.226-172.16.5.228		172.16.5.226	172.16.5.228	0	139	TOP		14:42:57.8	437500	14.42.57.8437500	Classife	d as TCP Allac
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	0	139	TOP		14 42 57 8	593750	14.42.57.8593750	Classife	d as TCP Attac
172.16.5.226-172.16.5.228		172.16.5.226	172.16.5.228	0	139	TCP		14:42:57.8	750000	14.42.57.8750000	Classife	d as TCP Attac
172 16 5 228-172 16 5 226		172.18.5.228	172.16.5.228	0	139	TOP		14:42:57.8	906250	14.42.57.8906250	Cassile	d as TCP Attac
172 16 5 228-172 16 5 220		172.18.5.226	172185228	8	139	TOP		14:42:57.9	062500	14:42:57 9062500	Classife	d as TCP Attac
170 16 6 000 170 16 6 006		172.16.5.228	172165228	0	139	TOP		14:42:57.9	218750	14.42.57.921 8750	Classife	d as TCP Attac
172.10.0.220-172.10.0.220		172.16.5.226	172165228	0	139	TCP		14.42.57.9	375000	14,42:57 9375000	Classife	d as TCP Attac
1/2.10.5.220-1/2.16.5.228		172.16.5.226	17216.5.228	0.	139	TOP		14.42.57.9	375000	14.42.57.9531250	Classifie	as TCP Attac
172.16.5.228-172.16.5.226		172.16.5.226	172165228	0	139	TOP		14,42.57.9		14,42:57.9687500	Classife	as TCP Attac
172.16.5.226-172.16.5.228	V	172.16.5.226	17216.5.228	0	138	TOP		14/42:57:9	687500	14:42:57.9687500	Classife	d as TCP Altac

Figure 9. Detection of TCP attack on victim machine

Figure 4 shows detection of TCP-SYN flood attack on the target system. Here all the packets after the TCP threshold value failure are highlighted using orange background to indicate that TCP –SYN flood attack was detected.

Figure 5 shows detection of UDP attack on the target system. Here packets those are highlighted using brown color, indicates that those packets were classified as attack packets as one of the required field was having missing or improper value.

ttings						Thresh	old for F	Rood Attack			
Packet Details	Se	ect Network Ad	apter : 172.16	5.228	*	TCP	20	UDP 20	Set Values	Stop	1
172.16.5.228-172.16.255.255	٨	Source IP	Destination IP	Source Port	Destination Port	Protocol	Data	In-Time	Detection Time	Remark:	
172.16.5.228-172.16.255.255		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:20.390625	0		
172.16.5.228-172.16.255.255		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:20.390625	0		
172.16.5.228-172.16.255.255		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:20.40625	0		
172.16.5.228-172.16.255.255		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:20.421875	0		
172 16 5 228-172 16 255 255		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:20.421875	0		
172 16 5 228-172 16 255 255		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:20.43750	0		
133 10 5 330 173 10 365 365		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:20.43750	0		
172.10.0.220-172.10.200.200		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:20.453125	0		
172.16.5.228-172.18.255.255		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:20.46875	0		
172.16.5.228-172.16.255.255		172.16.5.226	172.16.5.228	3094	139	TOP		15:08:20.46875	0		
172.16.5.228-172.16.255.255		172.16.5.226	172.16.5.228	3094	139	TOP		15:08:20.484375	0		
172.16.5.228-172.16.255.255		172.10.0.220	172.10.0.228	3094	139	TOP		15:08:20.484371	0		
172.16.5.228-172.16.5.226		172.16.5.220	172.10.3.220	3034	138	TOP		15:00:20.500001	0		
172.16.5.226-172.16.5.228		172 18 5 228	172.16.5.228	3094	139	TCP		15:08:20.515625	0		
172.16.5.226-172.16.5.228		172 16 5 226	172 16 5 228	3094	130	TCP		15-08-20 80937	0 15:08:20 8093750	Classified as TCP SY	
172.16.5.228-172.16.5.226		172.16.5.226	172 16 5 228	3094	139	TCP		15:08:20.62500	0 15:08:20.6250000	Classied as TCP SY.	
172.16.5.226-172.16.5.228		172.18.5.226	172.16.5.228	3094	139	TCP		15:08:20.625000	0 15:08:20.6406250	Classied as TCP SY.	
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:20.640625	0 15:08:20.6406250	Classied as TCP SY.	
172 16 5 225-172 16 5 228		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:20.656250	0 15:08:20.6562500	Classied as TCP SY	
172 16 5 228-172 16 5 226		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:20.671975	0 15:08:20.6718750	Classied as TCP SY	
170 16 5 208 170 18 5 200		172.16.5.228	172.16.5.228	3094	139	TCP		15:08:20.671875	0 15:08:20.6875000	Classied as TCP SY	
172.10.0.220-172.10.0.220		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:20.68750	0 15:08:20.6875000	Classied as TCP SY	
1/2.16.5.226-1/2.16.5.228		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:22.62500	0 15:08:22.8250000	Classied as TCP SY	
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:22.840625	0 15:08:22.8406250	Classied as TCP SY	
172.16.5.226-172.16.5.228		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:22.65625	0 15:08:22.6562500	Classied as TCP SY	
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:22.671875	0 15:08:22.6718750	Classied as TCP SY	
172.16.5.226-172.16.5.228		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:22.68750	0 15:08:22.6875000	Classied as TCP SY	
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:22.68750	0 15:08:22.7031250	Classied as TCP SY	
172.16.5.226-172.16.5.228		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:22.81250	0 15:08:22.8125000	Classied as TCP SY	
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:31.64062	0 15:08:31.6406250	Classied as TCP SY	
172 16 5 228-172 16 5 228		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:31.65625	0 15:08:31.6562500	Classied as TCP SY	
172 16 5 228-172 16 5 226		172.16.5.226	172.16.5.228	3094	139	TCP		15:08:31.671875	0 15:08:31.6718750	Classied as TCP SY	
172 16 5 226 172 16 5 228		172.16.5.226	172.16.5.228	3094	139	TOP		15:08:31.88750	0 15:08:31.8875000	Classied as TCP SY	
173 16 8 330.173 16 8 336		172.16.5.228	172.18.5.228	3054	139	TOP		15:08:31.78125	0 15:08:31.781.2500	Classied as TCP SY	
130 10 5 220 172 10 5 220		172.16.5.226	172.18.5.228	3034	139	TOP		15.09.22.51562	0 15:09:22:5156250	Classied as TCP SY	

Figure 10. Detection of TCP SYN flood attack on victim machine

ettings						Threak	old for F	lood áttack				
Packet Details	S	elect Network Ada	pter : 172.16	.5.228	~	TCP	200	UDP	150	SetValues	Stop	
172.16.5.220-172.16.5.228	~	Source IP	Destination IP	Source Port	Destination Port	Protocol	Data	In-Time		Detection Time	Remarks	
172.16.5.220-172.16.5.228		172.16.5.226	172.16.5.228	3094	139	TCP		15:58:51	5937500			
172.16.5.220-172.16.5.228		172.16.5.226 1	172.16.5.228	3094	139	TCP		15:59:25	5937500			
172.16.5.220-172.16.5.228		172.16.5.226	172.16.5.228	3094	139	TCP		15:59:25	7187500			
172 16 5 220-172 16 5 228		172.16.5.226	172.16.5.228	3094	139	TCP		15:59:59	7187500			
172 16 5 220-172 16 5 228		172.16.5.226	172.16.5.228	3094	139	TCP		15:59:59	8437500			
170 16 6 200 170 16 6 200		172.16.5.226	172.16.5.228	3094	139	TCP		16:00:33	8437500			
172.10.5.220-172.10.5.220		172.16.5.226	172.16.5.228	3094	139	TCP		16:00:33	9687500			
172.10.0.220-172.10.0.220		172.16.5.226	172.16.5.228	3094	139	TCP		16:01:07	9687500			
172.10.5.220-172.10.5.220		1/2.16.5.226	172.16.5.228	3094	139	TOP		16:01:08	0937500			
172.16.5.220-172.16.5.228		172.16.5.226	1/2.16.5.228	3094	139	TOP		16:01:42	0937500			
172.16.5.220-172.16.5.228		172.16.5.226	172.16.0.228	3094	139	TOP		16:01:42	2187500			
172.16.5.220-172.18.5.228		172.10.5.220	172.10.3.220	3094	139	TOP		16:02:16	2107500			
172.16.5.220-172.16.5.228		172 16 5 226	172 16 5 228	3094	139	TCP		16:02:50	3437500			
172.16.5.220-172.16.5.228		172.16.5.226	172.16.5.228	3094	139	TCP		16:02:50	4687500			
172.16.5.220-172.16.5.228		172.16.5.226	172.16.5.228	3094	139	TCP		16:03:24	4687500			
172.16.5.220-172.16.5.228		172.16.5.226	172.16.5.228	3094	139	TCP		16:03:24	5937500			
172.16.5.220-172.16.5.228		172.16.5.231 1	172.16.5.228	0	138	UDP		16:03:25	8281250	16:03:25.8281250	UDP Attack Detected	
172.16.5.220-172.16.5.228		172.16.5.231	172.16.5.228	0	138	UDP		16:03:25	8437500	16:03:25.8437500	UDP Attack Detected	
172.16.5.220-172.16.5.228		172.16.5.231 1	172.16.5.228	0	138	UDP		16:03:25	8437500	16:03:25.8593750	UDP Attack Detected	
172.16.5.220-172.16.5.228		172.16.5.231	172.16.5.228	0	138	UDP		16:03:25	8593750	16.03:25.8593750	UDP Attack Detected	
172 16 5 220-172 16 5 228		172.16.5.231 1	172.16.5.228	0	138	UDP		16:03:25	8750000	16:03:25.8750000	UDP Attack Detected	
172 16 5 220-172 16 5 228		172 16 5 231	172.16.5.228	0	138	UDP		16:03:25	8906250	16:03:25.8906250	UDP Attack Detected	
172 18 5 220-172 18 5 228		172.16.5.231 1	172.16.5.228	0	138	UDP		16:03:25	8906250	16:03:25.8906250	UDP Attack Detected	
170 16 5 200 170 16 5 200		172.16.5.231	172.16.5.228	0	138	UDP		16:03:25	8906250	16:03:25.9062500	UDP Attack Detected	
17216 5 220 172 16 5 220		172.16.5.231	172.16.5.228	0	138	UDP		16:03:25	9062500	16:03:25.9062500	UDP Attack Detected	
172.10.5.220-172.10.5.220		172.16.5.231	172.16.5.228	0	138	UDP		16:03:25	9218750	16:03:25.9218750	UDP Attack Detected	
172.10.5.220-172.10.5.220		172.16.5.231	172.10.3.220	0	130	000		10:03:25	0275000	16/03/25/93/2000	UDP Attack Detected	
172.16.5.220+172.16.5.228		172.16.5.231	172.10.0.220	0	130	line		16:03:25	9370000	16.02/26.0521250	LIDP Attack Detected	
172.16.5.220-172.16.5.228	-	172 18 5 231	172 16 5 228	0	138	UDP		16/03/25	9687500	16/03/25 9697500	LIDP Attack Detected	
172.16.5.220-172.16.5.228		172 16 5 231	172 16 5 228	0	138	UDP		16:03:25	9843750	16:03:25:9843750	UDP Attack Detected	
172.16.5.220-172.16.5.228		172.16.5.231	172.16.5.228	0	138	UDP		16:03:35	6875000	16:03:35.6875000	UDP Attack Detected	
172.16.5.228-172.16.5.228		172.16.5.231	172.16.5.228	0	138	UDP		16:03:35	7031250	16:03:35.7031250	UDP Attack Detected	
172.16.5.228-172.16.5.226		172.16.5.231	172.16.5.228	0	138	UDP		16:03:35	7031250	16:03:35.7031250	UDP Attack Detected	
172.16.5.226-172.16.5.228		172.16.5.231 1	172.16.5.228	0	138	UDP		16:03:35	7187500	16:03:35.7187500	UDP Attack Detected	
172.16.5.226-172.16.5.228	100	172.16.5.231	172.16.5.228	0	138	UDP		16:03:35	7343750	16:03:35.7343750	UDP Attack Detected	

Figure 11. Detection of UDP attack on victim machine

Figure 6 shows detection of UDP flood attack on the target system. Here all the packets after the UDP threshold value failure are highlighted using black background to indicate that UDP flood attack was detected.

Figure 7 shows CPU utilization by the system when there was no attack initiated on the system. During this period the CPU utilization by the system was only 0%.

ettings						Threak	old for F	land Attack		
Packet Details	84	elect Network Ad	apter : 172.16	.5.228	~	TCP	200	UDP 150	SetValues	Stop
172.16.5.228-172.16.255.255	^	Source IP	Destination IP	Source Port	Destination Port	Protocol	Data	In-Time	Detection Time	Remarks
172.16.5.228-172.16.255.255		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.5937500		
172.16.5.228-172.16.255.255		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.6093750		
172 16 5 228-172 16 255 255		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.6093750		
172 16 5 228-172 16 255 255		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.6250000		
172 16 5 228 172 16 255 265		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.6250000		
17210.0.0.00017218.200		172.16.5.228	172.16.5.228	115	138	UDP		15:48:15.6406250		
172.10.5.228-172.10.255.255		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.6406250		
1172.16.0.228-172.16.200.200		172.16.5.228	172.16.5.228	115	138	UDP		15:48:15.6562500		
172.16.5.228-172.16.255.255		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.8562500		
172.16.5.228-172.16.255.255		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.6718750		
172.16.5.228-172.16.255.255		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.6875000		
172.16.5.228-172.18.255.255		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15:7031250		
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	115	138	UDP		15/48:15.7031250		
172.16.5.226-172.16.5.228		172.10.5.220	172.16.5.228	115	130	UDP		15/40/15 2242260		
172.16.5.226-172.16.5.228		172.16.5.220	172.10.0.228	115	130	UDP		15.49.15.7343750		
172.16.5.228-172.16.5.226		172.16.6.226	172.16.5.220	115	130	UDP		15:40:15 7656250		
172 16 5 226-172 16 5 228		172 18 5 228	172 16 5 228	115	138	UDP		15:48:15 7858250		
172 16 5 228-172 16 5 226		172.16.5.226	172 16 5 228	115	138	UDP		15 48 15 781 2500		
172 16 5 228-172 16 5 228		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.7968750		
172 16 5 230 172 16 5 236		172.16.5.226	172.16.5.228	115	138	UDP		15.48:15.7968750		
172165220-172165220		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.8125000		
- 1/2.10.5.220-1/2.10.5.220		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.8125000		
172.16.5.220-172.16.5.228		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.8281250		
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.8281250		
172.16.5.226-172.16.5.228		172.16.5.226	172.16.5.228	115	138	UDP	~ ~	15:48:15.8437500	f	
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.8437500	15:48:15.8593750	Classied as UDP Flo.
172.16.5.226-172.16.5.228		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.8593750	15:48:15.8593750	Classied as UDP Flo.
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	115	138	UDP.		15:48:15.8750000	15:48:15.8750000	Classied as UDP Flo.
172.16.5.226-172.16.5.228		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.8906250	15:48:15.8906250	Classied as UDP Flo.
172.16.5.228-172.16.5.226		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.9062500	15:48:15.9062500	Classied as UDP Flo.
172.16.5.226-172.16.5.228		172,16.5.226	172.16.5.228	115	138	UDP		1548159062500	1548:15.9062500	Classied as UDP Flo.
172 16 5 228-172 16 5 226		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.9218750	15.48:15.9218750	Classied as UDP Flo.
172 16 5 228-172 16 5 228		172.16.5.226	172.16.5.228	115	138	UDP		15:48:15.9375000	15:48:15.9375000	Classied as UDP Flo.
172 16 5 228 172 16 5 226		172.16.5.226	172.16.5.228	115	138	UDP		10:48:10.9531250	15:48:15.9531250	Classied as UDP Flo.
13310 8 330 173 10 8 330		172.10.5.226	17210.0.228	110	150	00/		1040109001250	1040104031250	Classied as COP FIG.





Figure 8. CPU utilization by system before UDP flood attack on victim machine



Figure 7. CPU utilization by system during UDP flood attack on victim machine

Figure 8 shows CPU utilization by the system when attack was initiated on the system. During this period the CPU utilization of the system increased from 0% during no attack on the system to 53%.

VI. PERFORMANCE EVALUATION

Performance of proposed approach is done on basis of false positive & false negative ratio. From the results based on experimentation performed, there was no false positive or false negative classification of packets.

Table 1 shows average time that was required for classifying the packets as attacking under different network traffic conditions for the four considered attack types; TCP attack, TCP flood attack, UDP attack and UDP flood attack.

Sr. No	Type of Attack	Average Time taken for classification (in Seconds)
1	TCP Attack	0.0018001
2	TCP Flood	0.0010001
3	UDP Attack	0.0017120
4	UDP Flood	0.0010001

TABLE I. AVERAGE TIME TAKEN FOR CLASSIFICATION OF ATTACKING TRAFFIC

TABLE II. CPU UTILIZATION DURING AND BEFORE/AFTER DIFFERENT ATTACK

Sr. No	Type of Attack	CPU Utilization	CPU Utilization During Attack
1	TCP Attack	0 % (Before attack)	50 %
2	TCP Flood	1 % (Before attack)	53 %
3	UDP Attack	0 % (After attack)	53 %
4	UDP Flood	0 % (After attack)	52 %

VII. FUTURE WORK

Future scope includes extending the proposed method to support detection of more types of attacks based on their signatures such as port scan and also for detecting Distributed DoS attacks.

VIII. CONCLUSION

Attack detection approach for the four attacks namely, TCP attack, TCP SYN flood attack, UDP attack and UDP flood attack has been proposed. The approach can effectively differentiate between a normal traffic and attack traffic. The advantage of our approach is that it can identify all occurrences of simultaneous attacks on the system. The approach is based on prior knowledge about attack characteristics in order to detect them. The proposed experiment is a step toward observing the nature, characteristics, behavior of the attacks and accordingly designing the detection methodologies.

REFERENCES

- N. Wattanapongsakorn, S. Srakaew, E. Wonghirunsombat, C. Sribavonmongkol, T. Junhom, P. Jongsubsook, C. Charnsripinyo, "A Practical Network-based Intrusion Detection and Prevention System", 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2012.
- [2] Monowar H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools", IEEE Communications Surveys & Tutorials, 2013.
- [3] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda and Ren Ping Liu, "Triangle-Area-Based Multivariate Correlation Analysis for Effective Denial-of-Service Attack Detection", 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2012.
- [4] A. Kumaravel, M. Niraisha, "Multi-Classification Approach for Detecting Network Attacks", IEEE Conference on Information and Communication Technologies, 2013.
- [5] Risto Vaarandi, "Detecting Anomalous Network Traffic in Organizational Private Networks", IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, San Diego, 2013.
- [6] Shin-Ying Huang, Yen-Nun Huang, "Network traffic anomaly detection based on growing hierarchical SOM", 43rd IEEE/IFIP Annual International Conference on Dependable Systems and Networks, 2013
- [7] B.S. Kiruthika Devi, G. Preetha, S. Mercy Shalinie, "DDoS Detection using Host-Network based Metrics and Mitigation in Experimental Testbed", International Conference Recent Trends In Information Technology, 2012.
- [8] Y. Xie, S. Tang, X. Huang, C. Tang, X. Liu, "Detecting latent attack behavior from aggregated Web traffic", International Journal on Computer Communications, Vol 36, Pg. 895–907, 2013.
- [9] P. Jongsuebsuk, N. Wattanapongsakorn, C. Charnsripinyo, "Network Intrusion Detection with Fuzzy Genetic Algorithm for Unknown Attacks", IEEE International Conference on Information Networking, 2013.
- [10] Ahmad Sanmorino, Setiadi Yazid, "DDoS Attack Detection Method and Mitigation Using Pattern of the Flow", IEEE International Conference of Information and Communication Technology, 2013.
- [11] Sumaiya Thaseen, Ch. Aswani Kumar, "An Analysis of Supervised Tree Based Classifiers for Intrusion Detection System", IEEE International Conference on Pattern Recognition, Informatics and Mobile Engineering, 2013.
- [12] Kapil Wankhade, Sadia Patka, Ravinrda Thool, "An Overview of Intrusion Detection Based on Data Mining Techniques", IEEE International Conference on Communication Systems and Network Technologies, 2013.