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.

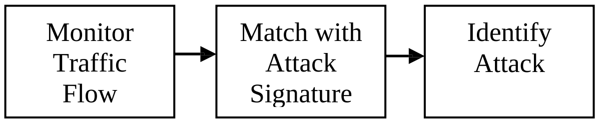

Figure 7. Block diagram for attack detection

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
    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.

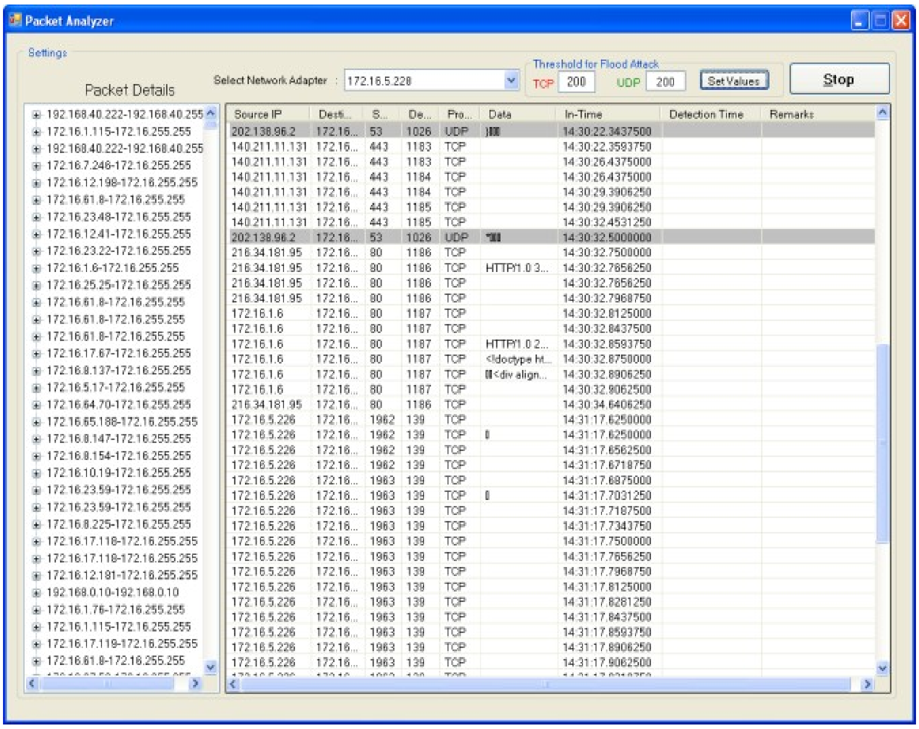

Figure 8. Monitoring network traffic on selected network interface

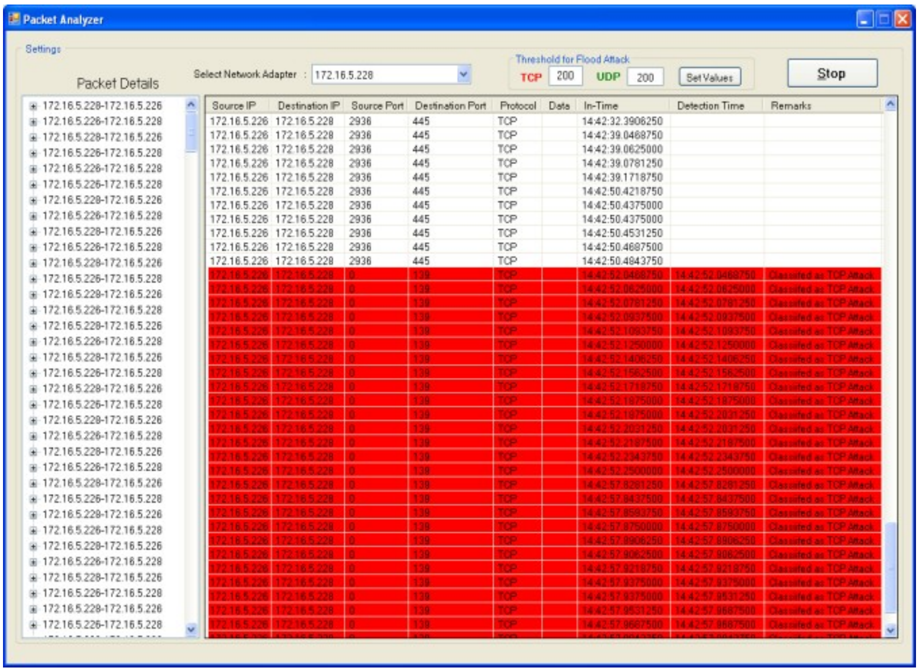

Figure 9. Detection of TCP attack on victim machine

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.

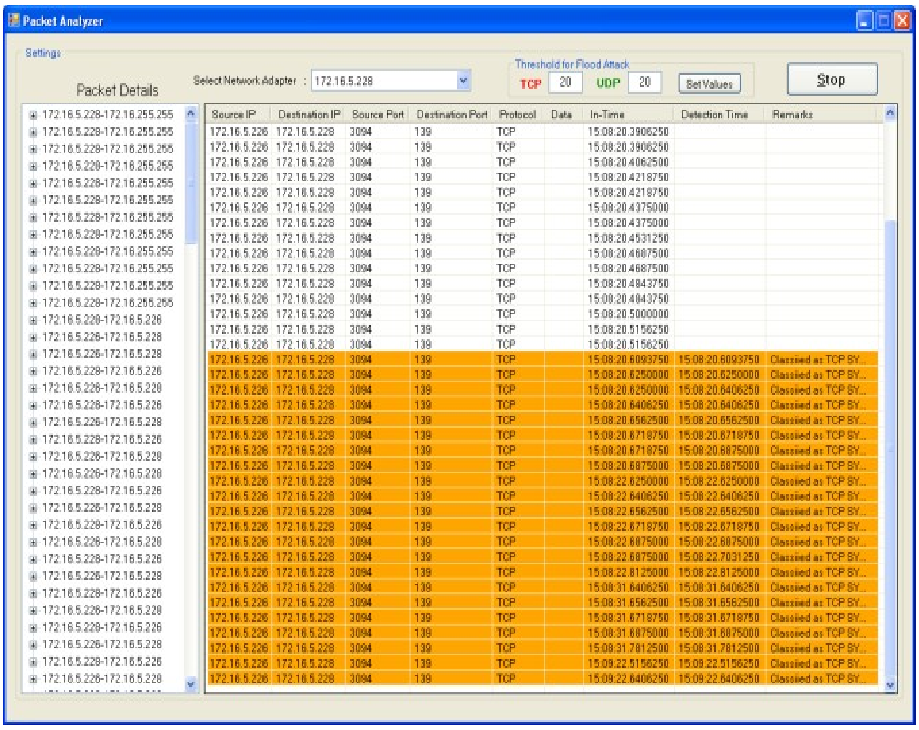

Figure 10. Detection of TCP SYN flood attack on victim machine

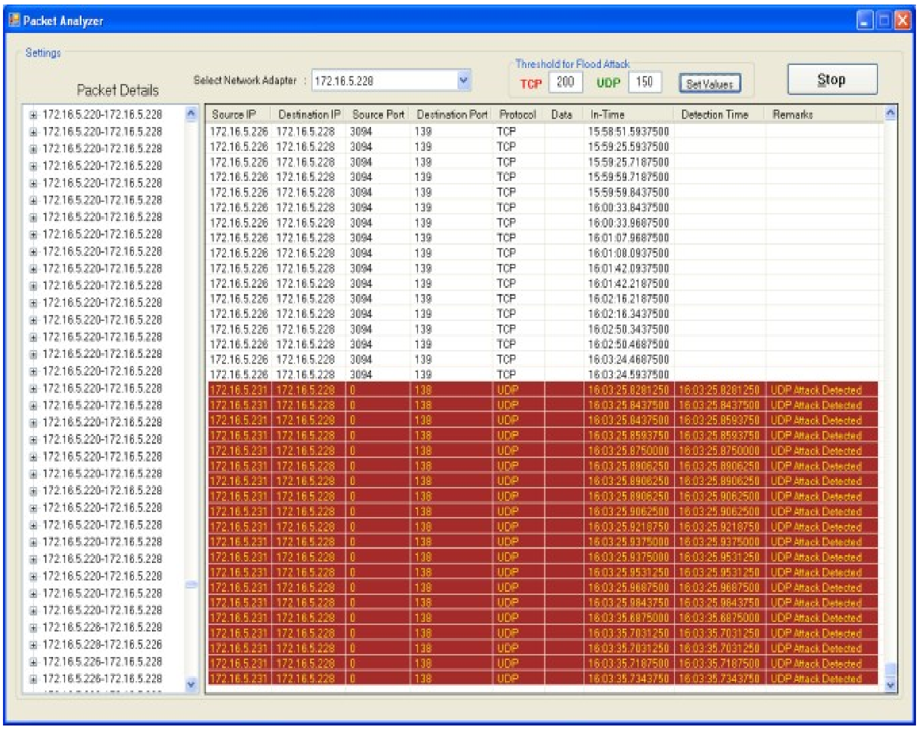

Figure 11. Detection of UDP attack on victim machine

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%.

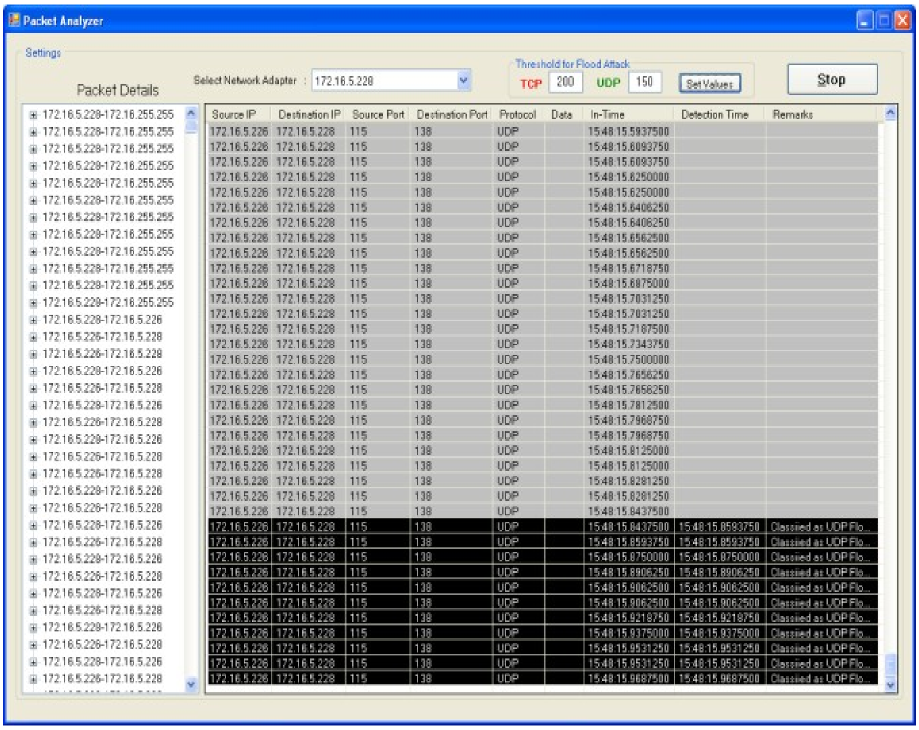

Figure 12. Detection of UDP flood attack on victim machine

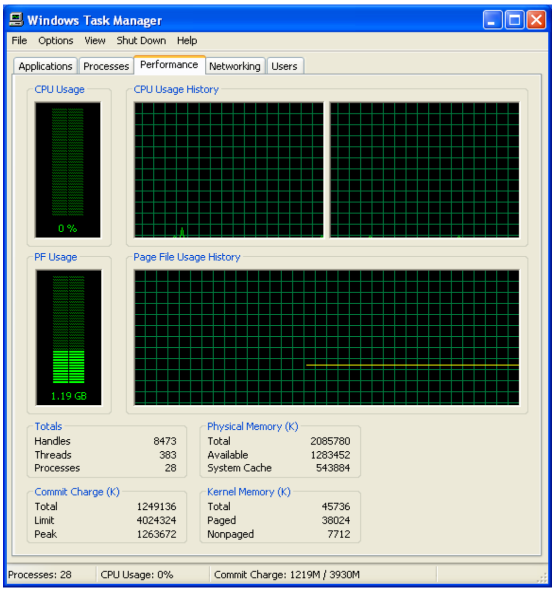

Figure 8. CPU utilization by system before UDP flood attack on victim machine

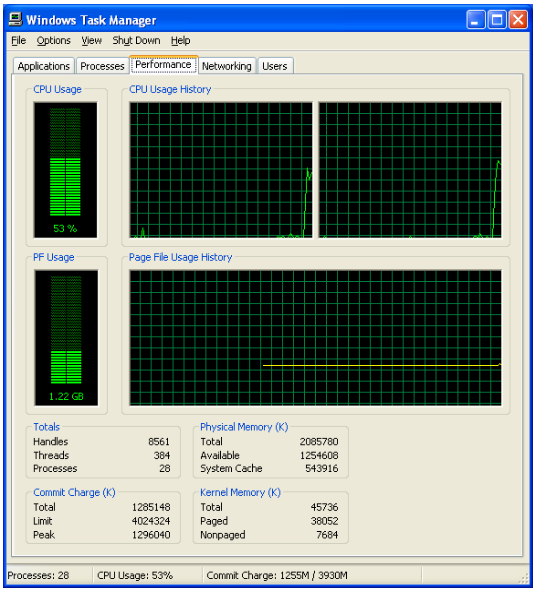

Figure 7. CPU utilization by system during UDP flood attack on victim machine

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.

TABLE I. AVERAGE TIME TAKEN FOR CLASSIFICATION OF ATTACKING TRAFFIC

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 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

[1] 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.