2321-8045 Science Park Research Journal Vol-1, Issue-39, 17th April 2014

Original Article

INTRUSION DETECTION SYSTEM
An Approach for Finding Attacks

Ashutosh Kumar and Mayank Kumar Mittra

ABSTRACT

Traditionally firewalls are used to prevent the intruders to make an attack. But they have static configurations that prevent attacks based on source and destination ports and IP addresses. These are not sufficient to provide security from all the attacks. Therefore, we need an IDS system which will identify the all types of attacks and generate an alarm. Proposed IDS is in two phases. In Phase-I, A database is maintained in the server side which contains the authorized IP address of the Local Area Network (LAN).Then a matching between stored and incoming IP will be matched up here. We will find a perfect match,this value depend on the less or higher threshold value. The value will show the infected packets and reported to the admin by an alert message like email. In Phase-II, the proposed concept includes state protocol analysis and packet filtering techniques. At last the proposed IDS can effectively and efficiently detect the attacks that are similar to DOS, U2R, RST and Experimental results are also show that the proposed method can effectively detect the attack that is similar to TCP SYN FLOOD and other attacks.

Keywords:
Local Area Network (LAN) , TCP SYN FLOOD , techniques.

Ashutosh Kumar and Mayank Kumar Mittra

From
B.TECH Scholar, CSE Dept B.TECH Scholar, CSE Dept
IT Bilaspur , CG.

The Article Is Published On April 2014 Issue & Available At www.scienceparks.in

DOI:10.9780/23218045/1202013/49

Introduction

INTRUSION DETECTION SYSTEM (IDS) is used as instrument or safe guard for preventing the network and system from the malicious or abnormal activities like threats, virus, hacker etc.

By the name intrusion detection system we can simply make an idea, where a system will protects the networks .system means a set rules or program which will act as a safety wall between host and internet.

Firewalls are also used as a protector but current firewall cannot defend against every category of intrusion. So here we required some set of specified techniques to avoid all type of intrusions and send an alert message to the user.

What Is An Intrusion?

Act of wrongfully or unauthorized access upon sizing or taking possessions of the property of other.

Or

Simply unwanted access and activities which is not good for system.

There are mainly two types of intrusion:

1. Active
2. Passive

Active attacks or intrusion are those where an attacker can modify and remove the data
Passive intrusion are those where attackers can only reads the systems' files
Intrusion detection system (IDS)
IDS can be classified into two category

1. NETWORK BASED
2. HOST BASED

In network IDS we detect the intrusions generated by the different layers as transport layer, application layer, network layer.

On the other hand in Host based the sensors of the IDS locate inside the particular host to monitor the system level behavior. Here we secure over host system by giving the login option in the system and keep the eye on basic activities.

Proposed intrusion detection system monitors individual systems upon the network. In this case, the sensor of the IDS is located inside of the particular host to monitor system-level behavior. This type of intrusion detection is especially useful for monitoring potentially dangerous user activity within the network. It's clear that there are two types of host-based intrusion detection software:

1.HOST WRAPPERS (or personal firewalls) and
2.AGENT BASED SOFTWARE.

Here describes the host wrappers as tools that can be configured to look at all network packets, connection attempts, or login attempts to the monitored machine. The agent-based software has the same abilities as the host wrappers, but can also detect changes in system files and changes in user privileges. A report by Network Associates makes a good argument for host-based intrusion detection, stating, and any masking techniques such as insertion, padding, fragmentation, or out-of-sequence delivery, which would evade a network-based IDS can be easily caught by a host-based IDS." Additionally, host-based IDSs can be quite effective in switched environments, whereas network-based IDS systems are less effective in that environment. A switch tends to isolate communications on the network, making it difficult for network-based IDS to monitor all traffic. However, if the systems on the switched network have host-based IDSs installed, potential attacks may be thwarted.

IDS (Intrusion Detection System)

An intrusion detection system is a software application or hardware device that monitors a system network and data base and analysis them for intrusion.

Generally we can understand intrusion detection system as a set of program or rule which a machine follow for detection of any harmful object or access over the system or network.

As previously we discuss about intrusion, ids have to perform various method or ways to catch the attack. Basically intrusion detection system have to perform following activity:-

1-monitering the activity of system
2-provides the integrity to system
3-helps admin to setup policies

According to attacks, IDS can be classified into two types:-

Active and passive

In REACTIVE IDS .we also known it as intrusion detection and prevention system IPDS. It is configured automatically to block the suspect attacks without any intervention of operation. An active ids is capable of performing any protective and corrective function on its own.

In PASSIVE IDS, the system is configured to only monitor and analysis the network traffic

andalert operation to potential vulnerabilities and attacks.

Classification of IDS:-

Intrusion can be occurred over the system like PC or laptops or on the network like LAN or WAN which effect the set of systems. We can classify the IDS in to following types:-

1:-host based IDS
2:-network based IDS

1:-Host based IDS:- a piece of software loaded to a system to detection of intrusion .software uses log files or system auditing agent ,which look at communication traffic. The software then checks the integrity of the system files. Agent are installed on publically accessible server such corporate mail server or application server. The agent then report events to the central console that is protected by agent software.

Host based system are used on the end point which helps ids to customized the activities on the system and have an eye on the activities eg. By giving log in id and password etc.

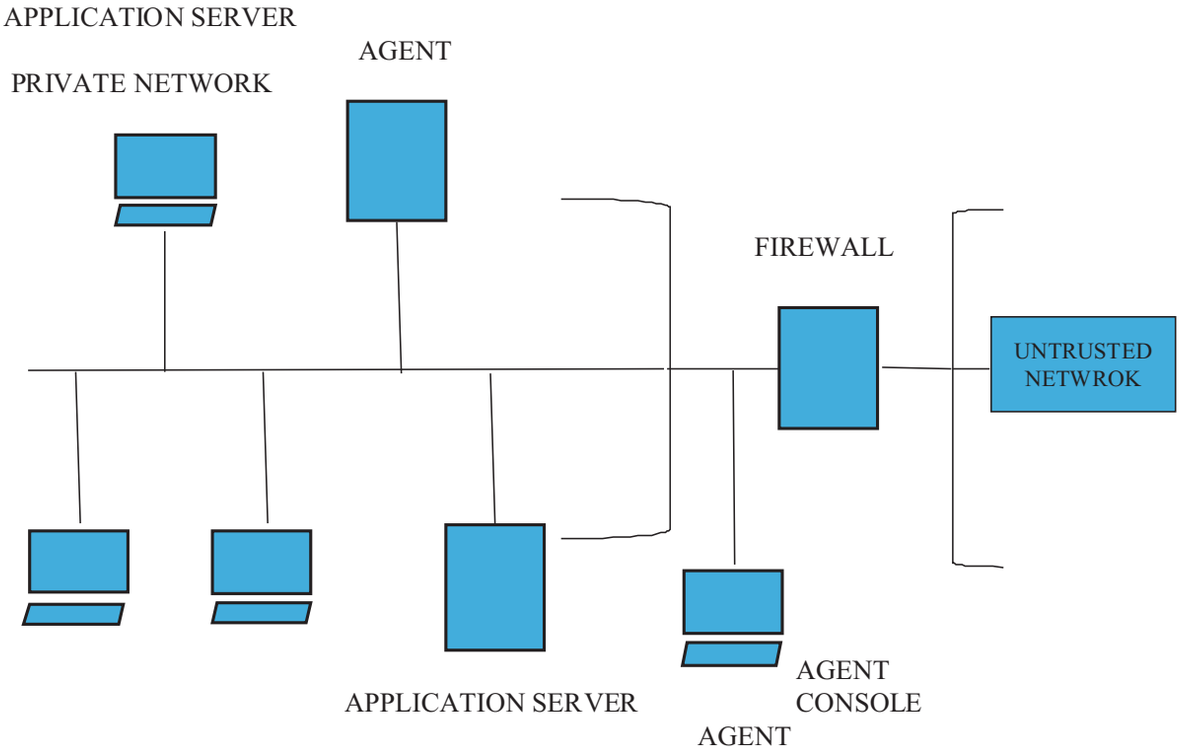


FIG1.HOST BASED INTRUSION DETECTION SYSTEM

2:- Network based IDS

Network based ids monitors the network by capturing the networks packets. They parse the packets analyze them and extract useful information from them.

In network based intrusion we used various devise in network for detecting the intrusion i.e. IDS sensor, IDS collector etc.

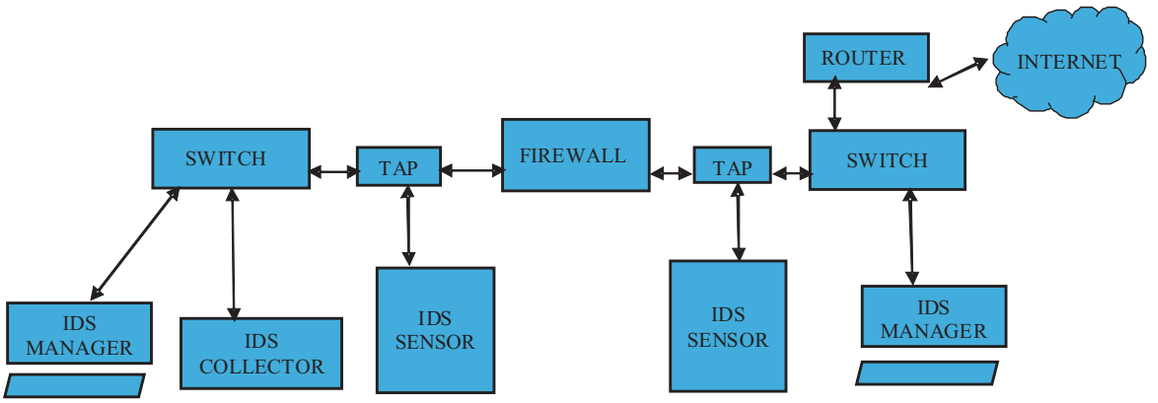


FIG2. NETWORK BASED INTRUSION DETECTION SYSTEM

Signature based intrusion detection technique:

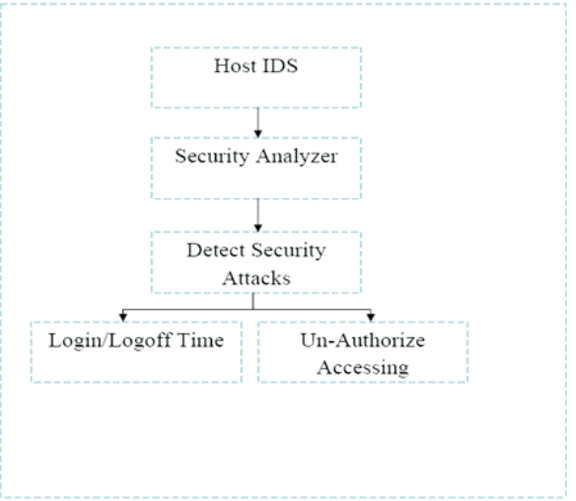
The detection technique uses specifically for known pattern to detect malicious codes. These specified pattern are called signature. Identifying the worm in the network is the example

Of signature base intrusion detection system. In this system we use signature data base for comparing in coming intrusion from the already stored database of various intrusion. For detecting the each and every detection we need to update signature data regularly or say up to dated so that we can find newest type of intrusion.

Anomaly base intrusion detection system:

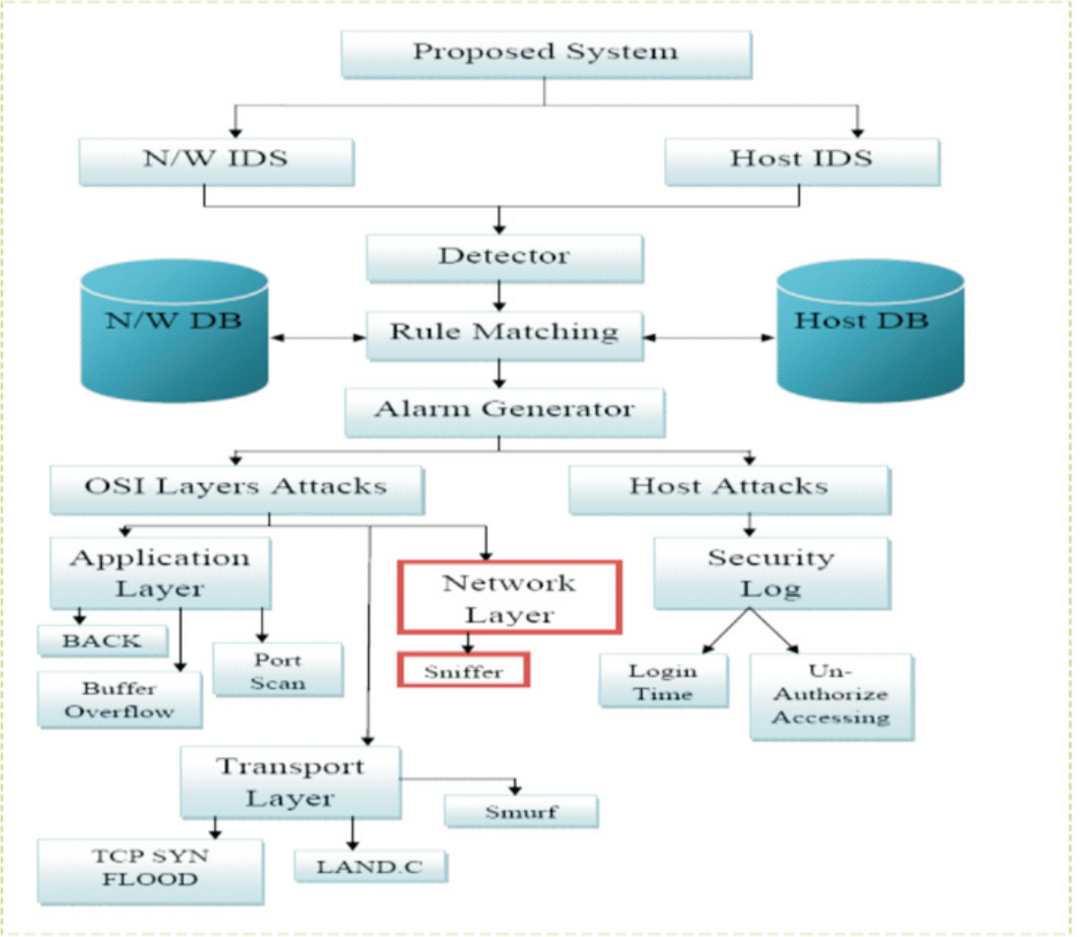
These techniques are design to detect abnormal behavior in the system. The normal uses pattern is the base line and alerts are generates when usage deviate for normal behavior. This system use anomaly database for comparing the coming intrusion. This database is created by inbuilt system by observing the valid users activity over a long time period and if there is any deviation from the normal activity then it generates the alarm. Eg. Up a user logs on and off 20 times in a day while a normal behavior is 1 or 2 time.

“Host Based Intrusion Detections System (HIDS)”. In this system we have concentrating only for security log file where security log analyzer will detect attack which is “Host Based Intrusion Detections System (HIDS)”. In this system we have concentrating only for security log file where security log analyzer will detect attack which is Related with system security. As we know that in this log file there are so many values to analyze security of the system but we have concentrate only two value which is already define above. Proposed HIDS call security analyzer to check or find attack in local host then it will detect security attack in security event log file. After completing this it will produce results. If any illegal activity find in this log file like un-authorize accessing or login failed then it will go to alarm system for information that this system is suffering from attack.



ARCHITECHTURE OF HOST BASED IDS

PROPOSED IDS



ARCHITECHTURE OF PROPOSED INTRUSION DETECTION SYSTEM

Proposed system architecture which is the combination of host based and network based intrusion detection system, and known as “Proposed Intrusion Detection System (PIDS)”.

In above figure particular IDS model capture packets and call to detector agent where detector agent pass capture packets to rule matching process Where rule matching process check attacks criteria from the database, where we have already defend and stored rule to find attack.

After completing this process alarm will activate if any type of attack find in the captured packet otherwise it will be deactivate and this processes will continue till on the proposed system. In network based module we have concentrate on layers wise attack finding mechanism, that mean which layers in the OSI model are producing what type of attack.

All the details of layer attacks are shown in next part. At the time of TCP packets header extracting proposed system checks the arriving IP header. From IP header it selects only TCP protocol. In NIDS we are finding layer attack or abnormality in the captured packets which is follows:

In application layer attack we are finding „Back", "Buffer overflow" and "Port Scan". In Transport layer we are finding "TCP SYN FLOAD Attack" "Land" and "Smurf".

Finally network layer attack are future work of this research. The Proposed IDS system is provide additional functionality of"Host Intrusion Detections System (HIDS)"

In this we are finding one type of attack by analysing the security event log file which is stored in local system. From security event log file we have finding two types of attacks which is follows: "Un-authorize accessing" and Login failed".

The proposed NIDS find six different conditions for attacks first it monitor and catch packets which is travelling over public network like internet, after catching packets, TCP header is extracted and analysed its attribute. If RST flag find in its attribute then it will treat as an abnormal packet and will go to the alarm generator tonote that this is infected packets and it should be treat as an attack type.

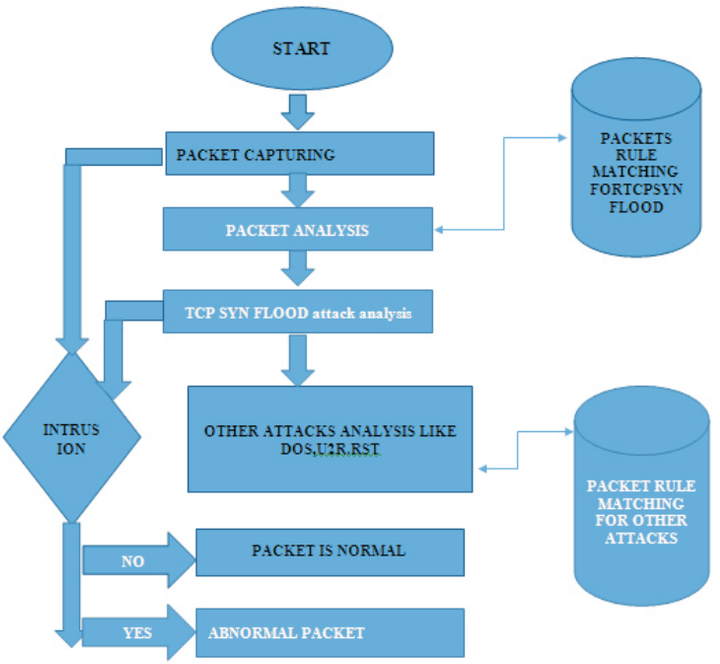
Another condition is for Back/land type attack this type attack is belongs to DOS attack category this will be work on both layer application as well as transport layers also. Basically "Back" attack find on application layers and "Land" attack find on transport layers. The condition for this type of attack is to analyse number of packet which is arriving from same host with in a time. In this we have set time limit to capture such type of packets and the time limit is 3 second time and 15 packets. If the same host are sending 15 or more then 15 packets in 3 second then that host is the intruder which is generating reported fake address then it will also treat as an attack type.

Another condition of application layer attack is the buffer overflow which is belongs to U2R attack is unauthorized access from a remote machine. For this attack we have set window buffer size and check overflow condition if overflow is occurring by the capture packets that mean such type of attack can be activate another definition of this attack capturing packet are lager then the predefined window buffer size then that packet will treat as an attack type.

Another application layer attack is the port scan. A Port Scan is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines Connected to a network run many services that use TCP or UDP ports. A port scan DOS Attack helps the helps the attacker find which ports are available. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed further for weakness.

At transport layer we have check TCPSYNFLOOD attack. In this we check the threshold value of the arriving packets if the threshold value of the arriving packet are less then predefined threshold value then the packet is normal otherwise packet as infected packets and it will treat as an attacks type.

BLOCK DIAGRAM FOR PROPOSED IDS

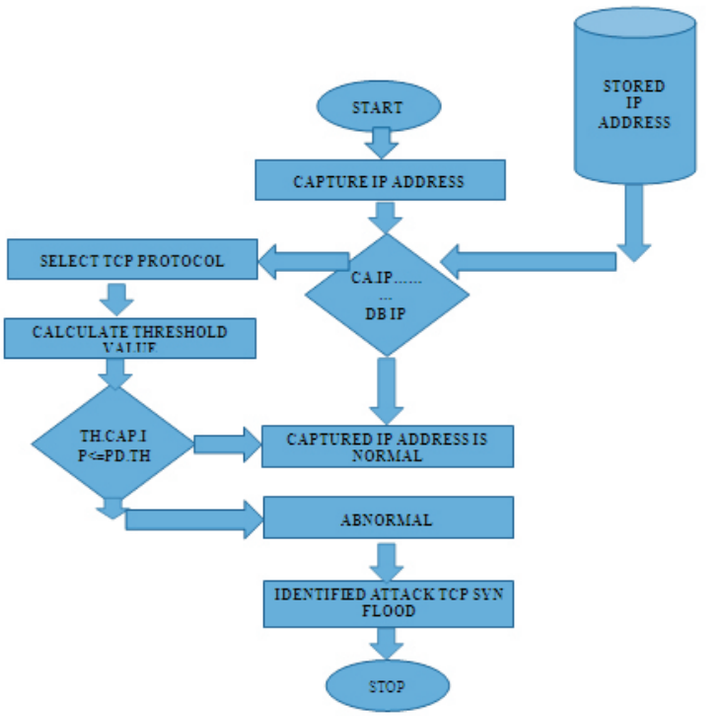


PROPOSED IDS: Proposed ids is in two phase:

1-A database is maintained in the server side which contains the authorized IP address of LAN. If IP address of incoming packet match in stored IP address then proposed concept allow the packet as normal packet, because of predefined IP address,which increases the efficiency of IDS.

If IP address does not match then check the threshold value of incoming Packets, if the value of incoming packets are less than calculated value, then packet Reported as normal packet.

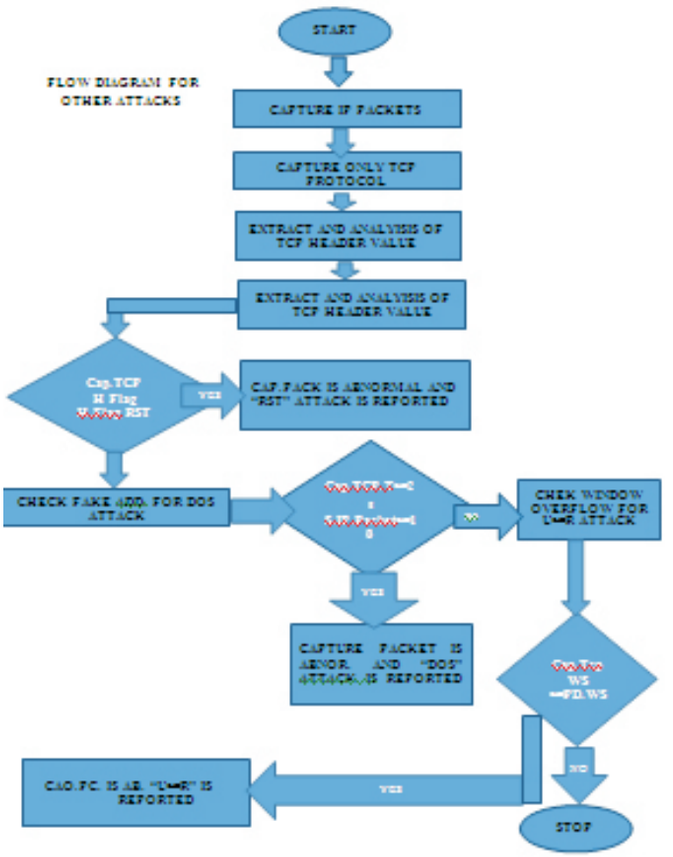
2-IDS includes the state protocol analysis, and packet filtering techniques. At last proposed IDS can effectively and efficiently detect the attacks that is similar to DOS, U2R, and RST.



PARAMETERS USED IN FLOW CHART

Cap.IP – Capture Internet Protocol
DB.IP – Data base Internet Protocol
Th.Cap.IP – Threshold Capture IP
PD.Th – Predefined Threshold

FLOW DIAGRAM FOR TCP SYN FLOOD ATTACK



Proposed Intrusion Detection System Technique

For Capture IP Addrress
Check the IP Header Length
If IP Header Length = 20 then
Choose the protocol = TCP
Check the payload packet

End if

Ifipaddress=db.ipaddress
Then
TCP Packet Normal
goto destination
Else if Check threshold value
If capture packet threshold value<= pre-defined threshold value
Then TCP packet is normal
Else if TCP SYN Flood

Then

Report to admin
End if
For Other Attacks
Capture IP Address
Check TCP packet and Extract TCP Header Value
If Header Flag find RST
Then TCP packet is abnormal
Else if capture TCP packets time >= 2 second and number of TCP packet generated from same IP address >=10
Then TCP packets is abnormal
Else if captured TCP packets window Size>= pre-defined window size
Then TCP packet is abnormal
End if
End for

Basically proposed IDS concentrating on TCP SYN Flood is major threat. At this stage Packet are divided into two groups infected and normal. Arrived packet are distinguish for analysis to conform, weather the packet truly comes for the attacker

RESULT ANALIYSIS

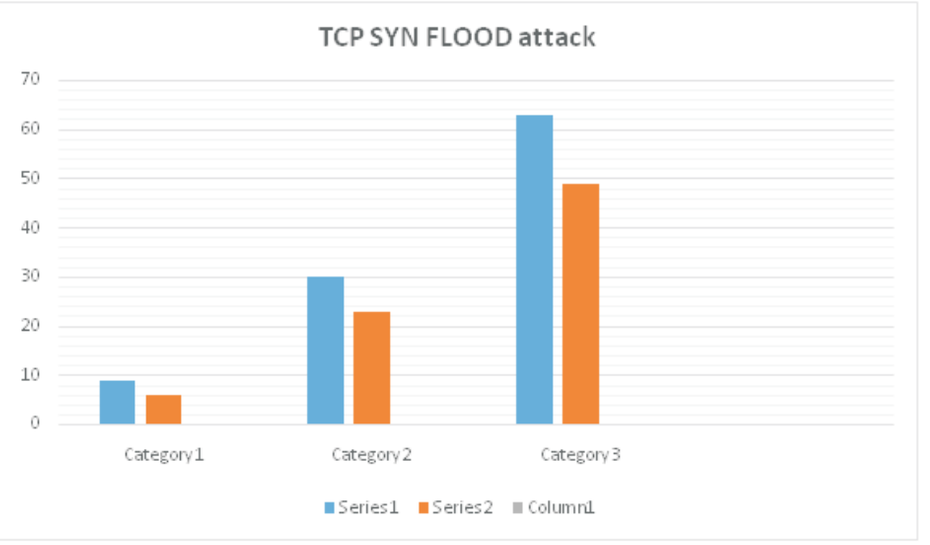
This paper will focus on TCP SYN FLOOD attack and some other attack like DOS, U2R and RST also tested. In order to facilitate observation of the effects of SYN attack detection, existing concept and proposed concept use the time interval value of Δ T that should not be too small and should not be too large So we set Δ T =10 sec, 20 sec and 30 sec and T=500 millisecond by default if we didn't calculate threshold value at run time otherwise run time threshold value will be set in this experiment. The only differences between existing and proposed concept is the maintaining authorized IP address in proposed concept. Table I is showing the comparison between two techniques of the IDS first one is the existing [4] and second one is the proposed detect intrusion detection. Three experiments are conducted in the same environment. Test time (sec) is 10, 20 and 30.

ANALYSIS TABLE OF TCPSYN attack

SERIAL NO	Time Of Capture Of TCP Packets	No Of Finding Attacks In Existing Concept	No Of Finding Attacks In Proposed concept
1	10	9	6
2	20	30	23
3	30	63	49

The test results of table I show that the second method can effectively filter out the packets which are needed to detect. The efficiency of intrusion detection is improved by this method. —TCP SYN FLOOD|| and other attack can be detected by this method. The test results of Table I show that the first method for the detection of SYN attack is higher as compare proposed because proposed concept of IDS has an extra filter which is authorized IP database. So those packets are in database they all are assuming as normal packets where existing concept does not maintaining authorized database concept. As a result, existing concept

expend unnecessary time to read authorized IP address and check threshold value if unfortunately threshold value exceed of authorized IP address then it will reported as abnormal packet which is the cause of poor efficiency and producing large number of attacks. This problem is avoiding by the proposed concept which is clearly seen in the table I. Graph I is representation graphical view of table 1. In this blue line is for existing concept results and red line is for proposed concept results.



X axis – No of attacks Y axis- Time interval of capturing packets

No of attacks finding by existing system

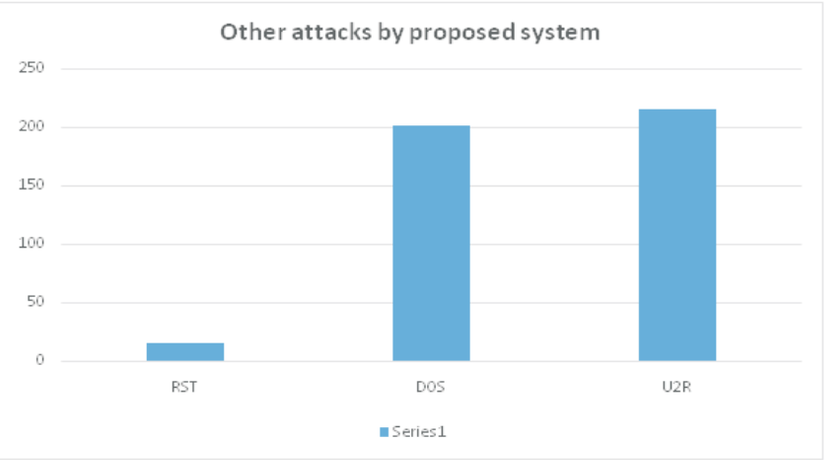
No of attacks finding by proposed system

ANALYSIS TABLE OF OTHER TYPE OF attacks

No Of Abnormal Packets	RST	DOS	U2R
430	16	202	216

RESULT

DOS Attacks packets are 202. U2R Attacks are 216. And RST attacks 16. Graph II is representation graphical view of table II. In this red line is for proposed concept results. In this total number of abnormal packets is 430 in which various attacks is showing.



Conclusion

In this paper, we proposed a new approach for intrusion detection system to detect attacks which is combination of time threshold value and authorized IP database approach and detecting the TCP SYN Flood, DOS, U2R and RST Attack. In this scheme instead of storing the all necessary information only the partial information is stored. At the meantime, the data packet filtering technology is added into the system to improve the efficiency of intrusion detection and the security of the system itself.

REFERENCES

1-Asmaa Shaker Ashoor and Prof.Sharad Gore ΔImportance of Intrusion Detection System (IDS)‖ International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011 ISSN 2229-5518

2-Kiran dhangarArif khan - Intrusion Detection System (A Layered Based Approach for Finding Attacks)International Journal of Advanced Research in Computer Science and Software EngineeringVolume 3, Issue 5, May 2013 ISSN: 2277 128X

3-Kiran dhangarArif khan – A proposed intrusion detection systemInternational Journal of Computer Applications (0975 – 8887) Volume 65– No.23, March 2013

4-Sudha singaraju and Parsikalpana - A Precise Survey on Intrusion Detection Systems International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 9, September 2012 ISSN: 2277 128X

5- D. E. Denning, "An intrusion-detection model." IEEE Transactions on Software Engineering, Vol. SE-13(No. 2):222-232, Feb. 1987.

6- Anderson, James P., ΔComputer Security Threat Monitoring and Surveillance‖,Fort Washington, Pa., 1980.

7- http://www.whitehelm.com/intru-det.html

8-http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf

9- Douglas J. Brown, Bill Suckow, and Tianqiu Wang ΔA Survey of Intrusion Detection Systems‖ 2004

10-Anuradha and Anita Singhrova A Host Based Intrusion Detection System for DDoS Attack in WLAN IEEE International Conference on Computer & Communication Technology (ICCCT)-2011 [10] Chundong Wang,

11-Quancai Deng, Qing Chang,Hua Zhang and Huaibin Wang " A New Intrusion Detection System Based on Protocol Acknowledgement" IEEE 2010

12- D. E. Denning, "An intrusion-detection model." IEEE Transactions on Software Engineering, Vol. SE-13(No. 2):222-232, Feb. 1987. [29] Anderson, James P., "Computer Security Threat Monitoring and 13-Surveillance", Fort Washington, Pa., 1980.

13- http://www.whitehelm.com/intru-det.html

14-http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf

15-Lee, W. and Stolfo, S. J., "A Framework for Constructing Features and Models for Intrusion Detection Systems," ACM Transactions on Information and System Security, vol. 3, November,