A study on Current threats and attacks against Network security and its preventive measures Using Artificial Neural Networks

Ms.S.Vijaya Rani
Assistant Professor,MCA Department
BrindavanCollege, DwarakaNagar
vrani_s@yahoo.co.in

Mr.R.Sekhar
MCA Student, Bharathiyar University
Coimbatore
sekhar_r14@yahoo.co.in

Abstract:

A Network cannot be totally secured by using security aspects such as network sniffing, firewalls, password security, access control,Intrusion detection etc. A secured network must contain all monitoring, early warning devices and intelligent prevention techniques. In this paper new attack against Network security has been studied and given a suggestion to prevent the threats and attacks based on Artificial Neural Networks.

Index Terms – Network Security, Distributed Denial of service, Threat, vulnerability, Intelligent Agent.

Introduction:

In network Security, effective measures should be implemented to avoid attacks. The attacks may be active or passive. The active attacks include alteration of information with an intension to corrupt, destroy or tamper data in a network. The passive attack includes monitoring of information flowing across the network. Securing information is a complex issue depending upon the prediction of the nature of attack.

The common types of network attacks are Eavesdropping, Data modification, Identity spoofing, Password-based attacks, denial of service attacks, man in the middle attacks, compromised key attacks, sniffer attacks, application layer attacks etc.[7] The most challenging attack is the distributed denial of service attack.

The Denial of service attack is an attack methodology by which a person can render a system unusable or significantly slow down the system for legitimate users by overloading the resources and no one can access it. The Dos attacks can be divided in to three classes.[12]

a) **Bandwidth Attacks:-**Bandwidth attacks are used to consume resources, such as network bandwidth or equipment throughput.High data volume attacks can consume all available bandwidth between an ISP and own site. The link fills up, and legitimate traffic slows down. Timeouts may occur, causing retransmission, generating even more traffic.

A basic flood attack might use UDP or ICMP packets to simply consume all available bandwidth. Ie, an attack could consist of TCP or raw IP packets as long as the traffic is routed to own network. Simple bandwidth consumption attack can exploit the throughput limits of servers or network equipment by focusing on high packet rates[11], sending large number of small packets.

b) **Protocol Attacks:-**It uses the expected behavior of protocols such as TCP,UDP and ICMP to the attacker's advantage. Examples are SYN flood attacks in which the attacker floods the victim with TCP SYN packets and the victim allocates resources to accept perceived incoming corrections. Smurf is an asymmetric reflector attack that targets a vulnerable network broadcast address with ICMP ECHO REQUEST packets.

c) **Software vulnerability attacks:-** These are logical attacks which exploit the vulnerabilities in network software, such as a web server or the underlying TCP/IP stack. Some examples are

- Teardrop exploits TCP/IP stacks that do not properly handle overlapping IP fragments.

- Land crafts IP packets with the source address and port set to be the same as the destination address and port.
- Ping of Death sends a single large ICMP ECHO request packet to the target.

DoS attacks may be effective because of a combination of effects. For example, an attack that does not fully consume bandwidth or overload equipment throughput may be effective because it generates enough malformed traffic to crash a particular service, such as a web server or mail server.

DDoS attacks involve breaking into thousands of machines all over the internet.[4] An attacker launches the DDoS attack using several machines. Hence an attacker breaks into several machines to launch an attack against a target or network at the same time. DDoS attack makes it difficult to detect because attacks originate from several IP addresses. Then the attacker installs DDoS software on them, allowing them to control all these infected machines to launch coordinated attacks on victim sites. These attacks typically exhaust bandwidth, router processing capacity or network stack resources, breaking network connectivity to the victim.

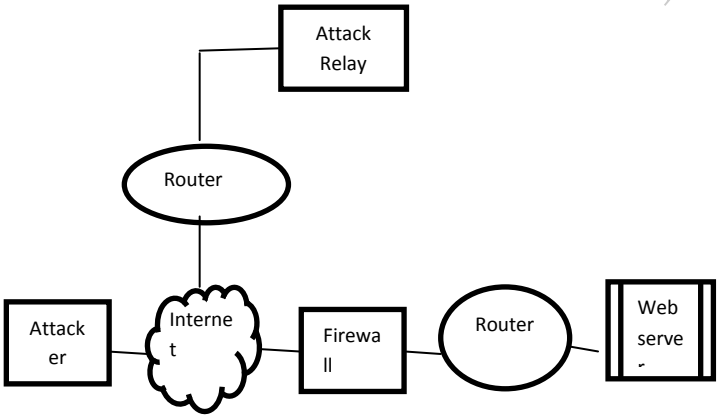

Fig1- Network Diagram –DDos Attack

DDoS is a combination of DoSattacks[8] carried out from various hosts to penalize the target host from further serving its function. The term is used when the source of attack is not coming from a single source, but multiple sources. Such attacks cannot be eliminated with just filtering the source IPs, since it is often launched from multiple points installed with agents. Prominent tools are Mstream, Trinoo, Tribe Flood Network, Stacheldraht, shaft etc.

The main tools for running DoS attacks are,

a) **Ping of Death:-**The attacker send an IP packet larger than the 65,536 bytes allowed by the IP protocol. In this case TCP/IP favors fragmentation. It allows a single IP packet to be broken down into smaller segments. When a large ICMP packet is sent by a hostile machine to a target, the target receives the Ping in fragments and starts reassembling the packet. Due to the size of the packet once it is reassembled, it is too big for the buffer and overflows it. Many OS did not know what to do when they receive such large packet. Ultimately they froze, crash and the system reboots. Ping of death attacks are particularly malicious because the identity of the attacker, who send the large ICMP packets can easily be spoofed, as the attacker just needs an IP address to carry out his attacks.[6]

b) **SYN – Flooder**:-It utilizes a standard technique of flooding the machine with half open connection requests. It is a small utility, which is distributed in Csource, when this utility is used against a Unix Server, it will temporarily stop the server's working.

c) **Land Exploit:-**This is a technique of sending a spoofed packet with the Syn flag which is used in a handshake between a client and a host and set from a host to any port that is open and listening. If the packet is programmed to have the same destination and source IP addresses, where it is sent to a machine, via IP spoofing the transmission can fool the machine into thinking it is sending itself a message, which depending on the OS will crash the machine.

The main hacking tools for DDoS attacks are,

1.Trinoo:-Trinoo is a DDoS attack tool which uses the following TCP ports.

-Attacker to master : 27665/TCP

-Master to Daemon: 27444/UDP

-Daemon to master:31335/UDP

It is on solaris 2.x system compromised by bufferoverrun bug in RPC services: Statd, Cmsd, ttdbserverd. The Trinoo daemon were UDP based, password protected remote command shells running on compromised systems.

2.TFN:- Tribe Flood Network uses a master program to communicate with attack located across multiple networks. TFN launches co-ordinatedDoS attacks that are especially difficult to counter as it can generate multiple types of attacks and it can generate packets with spoofed source IP address. Some of the attacks that can be launched by TFN include UDP Flood, TCP SYN Flood, ICMP eco request flood and ICMP direct broadcast.

3.Stscheldraht v2.666:- It combines the features of TFN and Trinoo but adds encryption between daemons.Stacheldraht uses TCP and ICMP of the following ports.

-Client to Handler: 16660 TCP

-Handler to and from Agents: 65000 ICMP

The DDoS attacks are different from sniffer attacks, which grab logins and passwords that are travelling around on the network.[12]

DoS attacks can be identified by its Ramp-up behavior. It is a change in the traffic volume of the attack as a function of time. In a multisource attack a master typically activates a huge number of Zombies immediately or at some later time. When observed near the victim, the distributed activation of Zombie results in a ramp-up of the attack intensity.

The spectral characteristics of attacks can also be studied for classification of single or multisource attack.

For stationary segments, the spectral density can be find out by performing the discrete-time. Fourier transform on the Auto correlation function of the attack stream.[3] The autocorrelation sequence r(k) at log k,

$$C(k) = 1/N \sum_{t=0}^{N-K} [(x(t) - \bar{x})(x(t+k)-\bar{x})]$$

where $\bar{x}$ is the mean of x(t) and N is the length of the attack stream x(t). The power spectrum s(f) of attack obtained by the discrete time Fourier transform of the auto correlation sequence of length m.

$$s(f)=\sum_{t=0}^{m} r(k)\, e\, N\text{-}k\ 2\pi fk$$

The highest frequency observable by this method is 500 Hz for 1ms time interval and the Fourier transform is symmetric.

IDS based on mode on Deployment:

To detect intrusion, the various approaches are Data mining, Clustering, Naive Bayesian Classifiers, Bayesian Networks, Hidden Markov models, Decision trees,ANN support vector machine etc.[11]

Improved IDS may have the following functional requirements,

-It should continuously monitor and report intrusion.[6]

- It may also be designed to rectify or repair basic intrusion.
- It should find and neutralize coordinated attacks.[5]
- It should bear more traffic loads.[8]
- It should prevent damages to network and its devices.[9]

An ANN agent is aimed to overcome the following limitations,

-Excessive data traffic [10]

- Intruders can perform insertion and evasion attacks. Normally data collection is performed in a host different from the one where analysis is performed.
- It controls analyzes and prevents favourable target to attackers.

The new concept should have the following characteristics

-Intelligence
-Flexibility [9]
-Mobility
-Speedy reaction
-Early warning system
-Updation
-Immunity to attacks.

The new design of IDS should have some special functions such as Event material, filtering

function, Identification function, checking genuineness function with AN Networks of intelligence agents, mobility agents, flexibility agent etc.

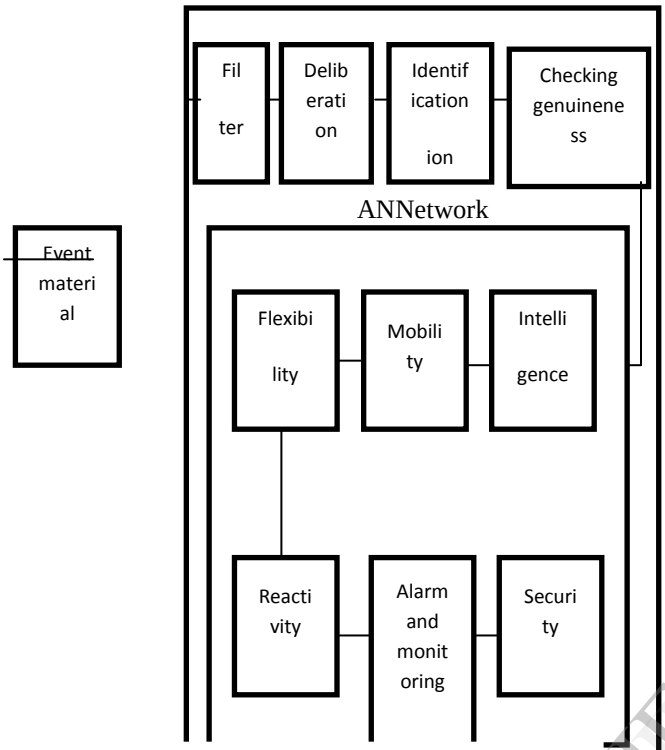

Fig2. The new design of IDS

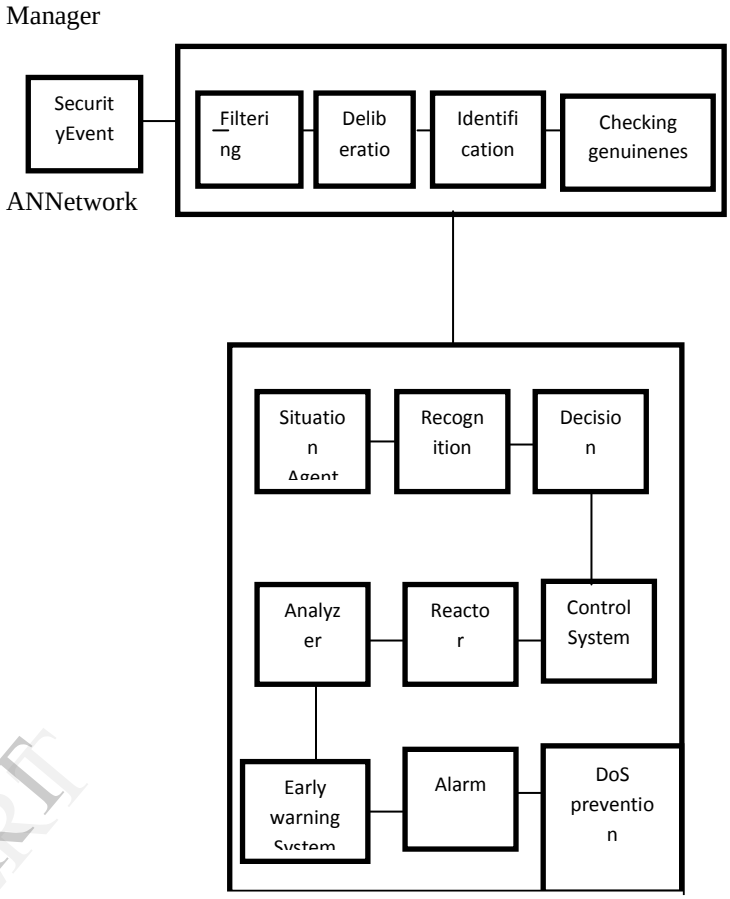

Fig3. Network security using ANN

The filtering events can be stored in deliberation function. It interacts with identification agent where it checks the filtered event with security policies, permissions, denials etc. The genuineness will be checked after identification. Further using ANNetwork system, intelligent agent will further identify and clarify the event with the help of mobility, flexibility functions. Finally the security agent may be in a position to secure any kind of threats.

The proposed Intelligent ANN IDS:

By ANN the IDS may be designed to take a decision at appropriate time to avoid mistakes and thereby effective detection and prevention of target system. The proposed block diagram is as under:

The incoming events arefiltered and passed to the ANN to take decision according to present scenario. The ANN may use knowledge, Recognition, Situation and finally take a decision to mitigate any DoS attacks.

Conclusion:- In this paper, I mentioned some common DoS attacks with an emphasis on recent research work on the subject topic. The proposed security management architecture based on the concept of Intelligent agent in junction with ANN take a decision on the security aspect of DoS attacks. The security dimensions on the proposed network diagram are access control, authentication, non repudiation, data confidentiality, communication security, data integrity, availability and privacy.

References

1.P.Ramasubramanian and A.Kannan, "Intelligent Multi Agent Based Multivariate Statistical Framework for Database intrusion prevention system". School of Computer Science and Engineering, Anna University, India.

2.PrashantDewan, ParthsDasgopts, Vijay Karamcheti,"Defending Against Denial of Service Attacks using Secure Name Resolution".

3."An Analysis of current computer network attack procedures, their Mitigation measures and the development of an improved Denial of Service attack Model", IhekWeabaOgechi, Inyiama H.C, IhekWeabaChukwugoziem.

4."Mitigation of Denial of Service attack", Payal Jain, Juhi Jain, Zatin Gupta.

5."Using Artificial Intelligence in Intrusion Detection Systems", MattiManninen

6."Artificial Intelligence Techniques Applied to Intrusion Detection", BharanidharanShunmugam.

7."Study and performance evaluation on recent DDoS trends of Attack and Defense", Muhammad Aamir, Muhammad Arif

8."Adaption of the neural network-based IDS to new attacks detection", PrzemyslawKukielka, ZbigniewKotulski

9.Data Security based on neural networks-Khaled M G Noaman and Hamid Abdullah Jalab.

10.Detecting and preventing attacks using network intrusion detection systems- Meera Gandhi and S K Srivatsa

11.Network and computer security tutorial version 0.4.0

12.Cisco certified network professional guide.