***International Journal of Computing Science and Information Technology*, 2013, Vol.*, pp-pp**
ISSN: 2278-9669, April 2018 (http://ijcsit.org)

Network Intrusion Detection System for Denial of Service Attack based on Anomaly Detection

Y.S.Kalai Vani, E.K.Radhika,
Asst. Professor,Dept .of Computer Science, HOD, Dept. of Computer Science,
Sindhi College, Sindhi college
Bangalore-24. Bangalore – 24

Abstract

In a wireless network system the security is a main concern for a user. It is basically suffering from mainly two security attacks i) Virus Attack ii) Intruders. Intruder does not only mean it want to hack the private information over the network, it also includes using a node bandwidth and increasing the Delay of Service for other host over the network. This paper is basically based on such type of attack. This paper reviews the comparison of different Intrusion Detection System. On the behalf of the reviewed work we proposed a new Network Intrusion System that will mainly detects the most prominent attack of Wireless Network i.e. DoS Attack. The proposed system is an intelligent system that will detect the intrusion dynamically on the bases of Anomaly detection System which detects the unusual behaviour.

Keywords: virus attack, intruders,anomaly detection,network intrusion detection system.

1. INTRODUCTION

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized. Although many incidents are malicious in nature, many others are not; for example, a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization.[1]

The system not only detects the intruders by the IP address, it detects the system with its contents also Introduction Denial of Service (Dos) attacks is one of the greatest attacks an intruder can perform. Dos attacks mainly focus on running out the client's resources so that he will not be able to service a request which is coming on from a legal or a legitimate user who is not an intruder. The intruder basically targets the client on his weak or you may say it as an advantage of the internet, the network bandwidth and its connectivity. The intruder or you may say the attacker targets these open points and floods 1000's or millions of packets so that the machine gets either crashed or dies servicing all those request, if the machine chooses to service the packets the machine will waste all the time by just servicing them which may include connection or data request packets and will not be able to service the clients who are genuinely wanting service from the machine. Dos attacks can be branched into categories based on the perspective of attacks being performed. They are Network Level, Application Level, Operating system Level and finally Data Level. We don't go much deep into the level but just provide a brief details about them.In this paper we have performed a DoS attack on a client machine and we have tried to give a layered based approach to prevent the DoS attack. The prevention algorithm basically takes in three layers and the user requesting has to pass all the three layers of protecting so that he can gain access to the request. Following this introduction the paper is sectioned or progressed in this manner.

2. REVIEWED WORK

2.1.1 Network discovery attacks:

Wireless LAN discovery tools such as Net-Stumbles are designed to identify various network characteristics. Although the use of these tools in not characterized as a real attack, it aims at discovering as much useful information about the network as possible. The derived information is used later on, for launching a real attack against the network. This technique is known as War driving.

2.1.2 Eavesdropping or Traffic analysis

Eavesdropping and traffic analysis attacks allow the aggressor to monitor, capture data, and create statistical results from a wireless network. Since, not all IEEE 802.11 packet headers are encrypted and they travel through the network in clear text format, potential eavesdroppers can easily read them.

2.1.3 Masquerading or Impersonation attacks

This category of attacks considers aggressors trying to steal and thereafter imitate the characteristics of a valid user or most importantly those of a legitimate Access Points (AP). The attacker would most likely trigger an eavesdropping or a network discovery attack to intercept the required characteristics from a user or an AP accordingly. Then, he can either change his Media Access Control address to that of the valid user or utilize software tools like the well-known Host AP that will enable him to act as a fully legitimate AP. This type of attack is also known as Rogue AP

2.1.4 Man-in-the-Middle attacks

The most advanced type of attack on a wireless or wired network is the "Man-In-The-Middle" attack. The attacker attempts to insert himself as man in middle, between the user and an access point. The aggressor then proceeds to forward information between the user and access point, during which he collects log on information. As a result, IJCEM International Journal of Computational Engineering the attacker can maliciously intercept, modify, add, or even delete data.

2.1.5 Denial-of-Service attacks

The main goal of Denial-of-Service (DoS) attacks is to inhibit or even worse prevent legitimate users from accessing network resources, services, and information. More specifically, this sort of attack targets the availability of the network i.e. by blocking network access, causing excessive delays, consuming valuable network resources, etc. A denial of service occurs when an attacker has engaged most of the resources a host or network has available, rendering it unavailable to legitimate users. More specifically, this sort of attack targets the availability of the network i.e. by blocking network access, causing excessive delays, consuming valuable network resources, etc. [3], [4]

2.2 Intrusion Detection Method

Intrusion detection (ID) is the art of detecting inappropriate, incorrect, or anomalous activity. It also evaluates suspicious activity that occurs in corporate network. Intrusion detection system (IDS) is the process of detecting and identifying unauthorized or unusual activity on the system.

Table1: Difference between Firewall and Intrusion detection system.

Firewall	Intrusion Detection System Intrusion
It is the first defending line, which can prevent network efficiently. It has a deadly defect it only can prevent the intrusion from extranet	IDS is a process of identifying and responding to intrusion activities. It has ability of detecting illegal intrusion and attacks.

2.3 Classification of Intrusion Detection System

IDS can be categorized according to intruder type, detection behavior, and detection techniques.

2.3.
tern

The
they

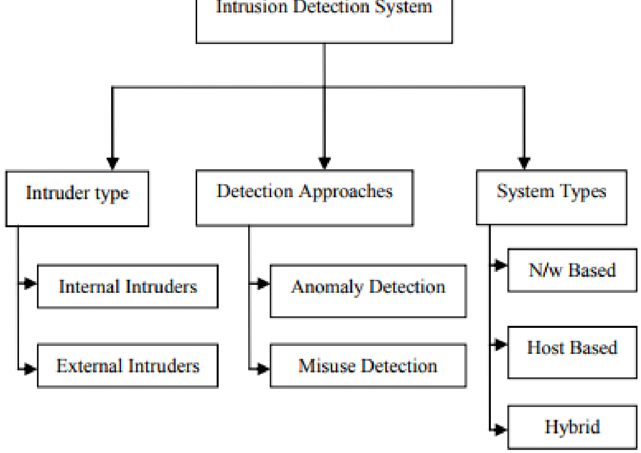


Figure 1: Classification of Intrusion Detection System [5]

Internal intruders have permission to access the system, but not some portions of it. Furthermore internal intruders divide into intruders who masquerade as another user, those with legitimate access to sensitive data and the most dangerous type, the clandestine intruders who have the power to turn off audit control for themselves.[4]

2.3.2 Detection Approaches IDS that monitor computer systems and networks, analyze them for signs of security policy violation, and respond accordingly, is based on one of these approaches:

- Anomaly detection systems
- Misuse detection systems.

These two approaches are used to detect the intrusions in the network and gives the alarm for the network and it is usually used to represent the workload of the network.

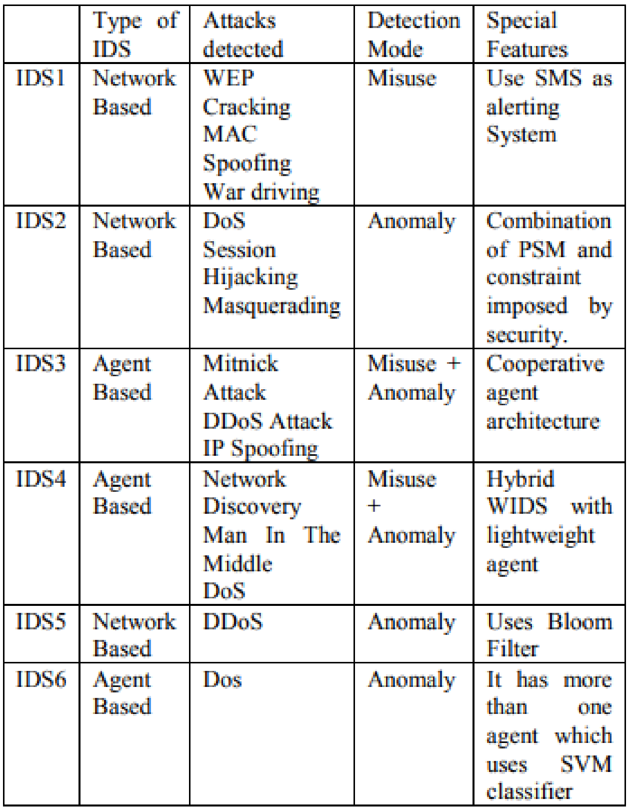
Table 2: Comparison between Anomaly Detection System and Misuse Detection System

Anomaly Detection System	Misuse Detection system
When the events of interest to an IDS define the undesirable behavior, or intrusions the system is said to be a misuse-based IDS. It uses Signature for attack detection. It has a low false positive rate. It cannot able to detect novel attacks or attacks for which no signature is available	When the event of interest to an IDS are expected or normal behaviors of monitored system, with intrusions defined as deviation of monitored behavior from this baseline, the system is said to be an anomaly-based IDS. It relies on identifying attack by detecting deviations from learned normal behavior. It has large number of false positive rate.

2.3.3 Types of Intrusion Detection System There are three main different types of IDS.

- Network-based IDS
- Host-based IDS
- Hybrid IDS.

This classification also depends on their Data Gathering Components (sensors), which they use to collect data to detect possible attacks against system.



	Type of IDS	Attacks detected	Detection Mode	Special Features
IDS1	Network Based	WEP Cracking MAC Spoofing War driving	Misuse	Use SMS as alerting System
IDS2	Network Based	DoS Session Hijacking Masquerading	Anomaly	Combination of PSM and constraint imposed by security.
IDS3	Agent Based	Mitnick Attack DDoS Attack IP Spoofing	Misuse + Anomaly	Cooperative agent architecture
IDS4	Agent Based	Network Discovery Man In The Middle DoS	Misuse + Anomaly	Hybrid WIDS with lightweight agent
IDS5	Network Based	DDoS	Anomaly	Uses Bloom Filter
IDS6	Agent Based	Dos	Anomaly	It has more than one agent which uses SVM classifier

wn ork c.). a ion to lly vel, ted The ore net- ack res ers sed to ific

Table 4: Difference between different IDS

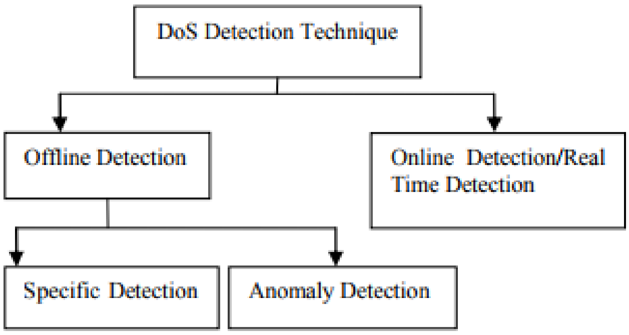


Figure 2: Classification of DoS Attack Detection Techniques

3.1.1.Offline Detection:

Offline detection mechanisms are classified into two groups:

- Specific detection
- Anomaly based detection.

Specific detection uses rule-match methods to justify whether monitored traffic have special attack features. The rule-match approaches maintaining per flow state and matching packets to a pre-defined set of rules has shown a certain good capability. However, rule-match approaches unlikely detect unknown DDoS attacks. Anomaly-based detection models the behavior of normal traffic and then reports any anomalies. PCA, entropy and subspace methods have demonstrated accuracy and efficiency in detecting network-wide traffic behavior anomalies. However, most of these network-wide anomaly detection and machine-learning approaches are performed offline. Thus, it is difficult for them to take timely preventive measures for DDoS attacks.

3.1.2 Online Detection

Real-timely detect and defense DDoS attacks, on-line detection techniques are now paid wide attention. Generally, on-line detection techniques are statistical approaches regarding traffic feature and behaviors. Consequently, computation, memory consumption and detection time are key concerns about on-line detection.

4.PROPOSED WORK

The proposed system is a Network Intrusion Detection System that is an enhancement of the existing system. It is a system level program that works as the lower layer of the firewall. The system not only detects the intruders by the IP address, it detects the system with its contents also. The system checks the database for the already registered intruders. If found intruding, they are forwarded to the firewall for blocking. The firewall is responsible for the blocking of the packets.

The proposed system can be used to attain infor- ie in- , the ed in a that l into esses ound posed rvice rized eting uters may

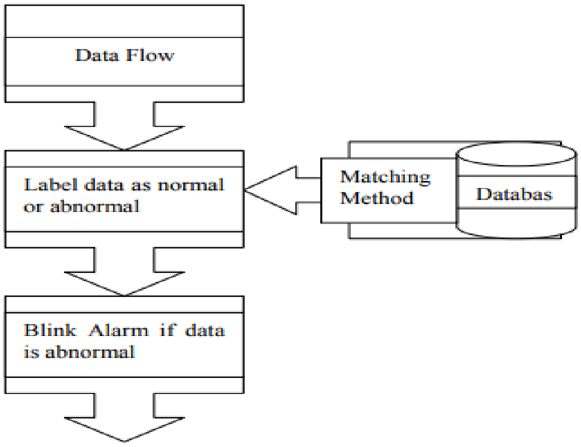

Data Flow
Label data as normal or abnormal
Matching Method
Databas
Blink Alarm if data is abnormal

Figure 3: NIDS Architecture

Figure 1 gives the overview of proposed system that will capture the packets coming from network. Then compare it with the stored information if the capture data is match with stored information of intrusion, the intruder is detected and alarm blinks otherwise normal flow of data take place.

Benefit of Proposed Work

1. User friendly
2. Ease of access
3. Fast retrievals
4. Single point system administration and maintenance
5. Added security to system
6. Can be implemented in any network
7. Easy to mention an IP address

5. CONCLUSION

The proposed system will provide a secure and authenticated system to transfer data over the network. The proposed system will be defined for both the wireless or wired network. This system will provide the safer transmission in Denial of Service (DoS) Attack and ManIn-The-Middle (MITM) Attack which are mostly founds in networks. Beside this it will have single point system administration and maintenance which makes it user friendly. It will also add security to a system as well as networks. Through this proposed system it is easy to mention an IP address.

6. FUTURE WORK

The purposed system can be used for the commercial proposed and it can implement as part of firewall system to combine the working of prevention and the detection system. The enhancement can be made to check the same approach for different other attacks over the network. The future work can be content oriented.

.References

[1] Karen Scarfone Peter Mell "Guide to Intrusion Detection and Prevention Systems (IDPS)", NIST, 2007.

[2] Jaydip Sen "An Agent-Based Intrusion Detection System for Local Area Networks." in International Journal of Communication Networks and Information Security (IJCNIS) Vol. 2, 2010.

[3] F Haddadi, M .A. Sarram, "Wireless Intrusion Detection System Using a Lightweight Agent" IEEE Second International Conference on Computer and Network Technology, pp.84-88, IEEE, 2010.

[4] A.T., G. Kambourakis, S. Gritzalis "Towards effective Wireless Intrusion Detection in IEEE 802.11i", IEEE Third International Workshop on Security, IEEE, 2007.

[5] T. S. Sobh "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art", Computer Standards & Interfaces 28, pp. 670-694, Science Direct, 2006.

[6] Y i Zhang, Qiang Liu, Guofeng Zhao "A RealTime DDoS Attack Detection and Prevention System Based on per-IP Traffic Behavioral Analysis." pp.163-167, IEEE, 2010.

[7]. Scott Fowler, Sherali Zeadally "Defending against Distributed Denial of ervice (DDoS) Attacks with Queue Traffic Differentiation over Micro-MPLSbased Wireless Networks.", IEEE, 2006