Detection of Malicious Activities within the Network Nodes in MANET using IDS Approach: A Review

Arti[1], Rekha[2]

[1]M. Tech. Scholar, [2]Assistant Professor
CBS Group of Institutions, Jhajjar, Haryana
Maharishi Dayanand University, Rohtak.

Abstract: **Many IDS systems use one of two detection methods, the misused detection or the detection of irregularities, each with their own restricted use in the current scenario. Technology has developed technologies which is known as Hybrid intrusion detection. The objective is to increase the detection rate and reduce the false positive rate by using abuse detection and irregular detection, which incorporates the abuse detection system with the abnormal detection system (ADS) and the host intruder intrusion detection system. There is a study of the prototype IDS. It discusses many main aspects of hybrid recognition and has also discussed some of the major research in hybrid IDS. This model shows a comparative study of the performance criteria in various studies. We effectively use Snort to detect malicious attacks for NIDS and Kfsensor for HIDS. Then we use Snort to fix threat issues in network-based and host-based IDS in hybrid. Cybercrime has also grown with the rapid growth in network technology. The intruders are currently concerned about a variety of risks and threats to vulnerable, defenseless infrastructure such as databases, web servers and whole networks. Using the Intrusion Detection System you will detect unauthorized access to files, networks and any serious security danger.**

Keywords: **IDS systems, abnormal detection system, WSN**

Introduction

WSN is basically a sensor service. Growing sensor network consists of various segments: antenna, battery, microcontroller, analog circuit and sensor device. The whole network was operating concurrently by the implementation of various sensor measurements and the multi-routing technique, also known as wireless adhoc networking, function. It is being used in broad and rough environments in WSN's strongest benefit. We don't have any cable interference and versatility. This maintains a small energy base. There are several WSN programs used to check, evaluate and search. The configuration of the routing protocol is the principal limitation in WSN and the finite capacity of the sensor nodes used for the energy output of the contact protocol. The routing is focused on the cluster-oriented routing method that matches the prominent usage of static and mobile WSN systems. Sensors are grouped into different clusters where each cluster contains the cluster head (CH), which allows to gather information in the form of clusters at all nodes.

Review of literature

Every day, the users are treated by the advanced users of a computer network who increase the influence of the social web on the users and at the same time the growth is created. And how the material was communicated and interpreted by the network is the basis of the modern corporate practice that reflects and fuses personal and company interactions. Their primary purpose is to secure the network against intrusions, which may disrupt the data to the different systems, steal passwords, or exploit the network... The intrusion detection system in the field of protection, considerations such as honesty, secrecy and network connectivity are primarily three separate principles. Accordingly, secrecy ensures the security of the details. Ignorance of intelligence theft and authorization for illegal access to or malicious activity gained without deception. Yet quality indicates the operating performance and the potential for regeneration in severe circumstances. During the 0s and 1s, multimedia material was introduced that can be taken out via the network's illicit connectivity. The missing details generated by the malicious intent discovered internally or externally are rather real danger to the knowledge assets. And anyone who is legitimate users carrying out the illegal activity, or actions resulting in an illegal information leak, can lose control of the computing assets, this is a malicious node.

In the first days, it was used to network mostly conventional approaches, such as encryption, firewalls, the virtual private network, etc. Static protection strategies are hard to be fully reliant on. This raises the need for complex infrastructure, the surveillance network and the detection of illegal activities. In order to improve the dynamic approach to network security, the so called Intrusion Detection System is introduced. Intrusion detection system gathers online network knowledge after it tracks, analyzes and partitions this information in normal & harmful operations.

Many artificial intelligence methods in the area of information technology have been established to the efforts of humans. Therefore, due to the attacks contained in this program, the framework for intrusion detection is divided into several kinds. The intrusion detection system thus serves mainly to warn the authority holder of the assaults.

The IDS definition specifics are now listed below:

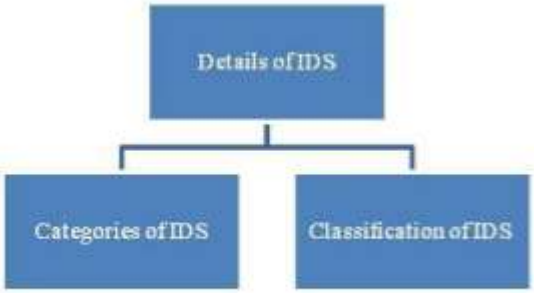


Fig.5 Details of IDS

Categories of IDS

IDS listed in two groups, according to the strategies for intrusion detection dependent on information or uncertain patterns:

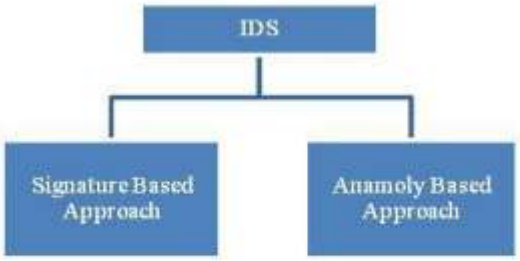


Fig.6 Categories of IDS

Signature Based Approach:

That is the way that threats that are affected by the device are detected. It tracks the network activities and the pre-defined signatures within this system. Here, by monitoring the actual traffic, the IDS can attempt to detect suspicious activities to detect the type of attacks. The Signature-based method of detection is often referred to as the warning generation depending on a particular signature.

Anomaly Based Approach:

This type of approach is designed to expose patterns that do not match regular behavior and are also regarded as an attack. Two types of detectors, including the static sensor and the dynamic sensors, exist within this method. The suspicious behavior within the network has been checked in this process. No prior knowledge of the patterns of attacks is required, even the latest intrusions can be identified.

Passive system vs. Reactive system:

With the passive IDS, all security breaches are identified and all suspicious operations are evaluated, a log file produced and the safety officer notified. The reactive framework creates a log file that records the user's actions and also reports the user off the network.

The biggest challenge is to distinguish between normal and abnormal activity in computer networks. The great challenge here is to combine both types of data. A false alarm is often produced when attempting to detect a malfunction of a device based upon the anomaly intrusion detection. How will this question be resolved.

Classification of IDS

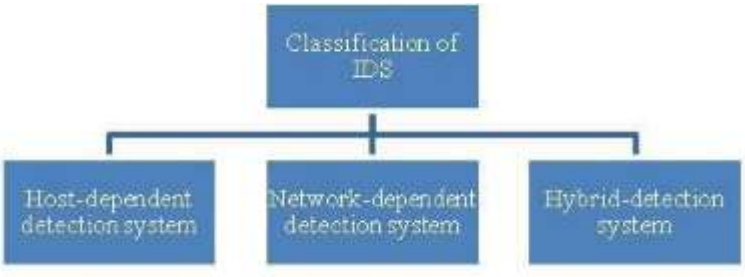


Fig.7 Classification of IDS

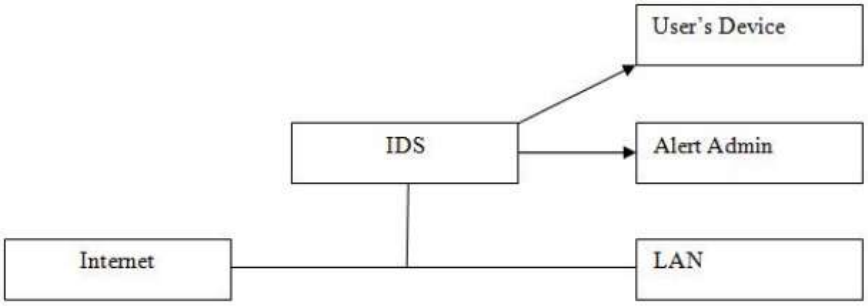
Host-dependent detection system

The detection is done on one host machine in this sort of intrusion detection method. The validity of the data obtained by the host system is tested in order to assess some form of device change or alteration. The use of hacking software, device logs and even the search of system calls for the discovery of interferences makes this possible.

Network-dependent detection system
This type of intrusion detection program is directed at the host network rather than the computer network. This program detects attacks by capturing network packets and then tracking them. Here, NIDS will listen to network traffic or switch traffic and track it that affects specific hosts connected to the network, and thus protect host systems as well.

Hybrid-detection system
In order to create the hybrid intrusion detection system, this method is the combined combination of the cluster-based approach and the regulatory approaches. This method uses all approaches to the advantages. Using this combination, it can provide a fast, easy detection and a low energy usage with a high safety rate. It allows for the higher identification rate and the lower false-positive rate.

Intrusion Detection System
The complex elements of the network security domain are intrusion-detection mechanisms. Attempts to breach the security of information have increased day by day with techniques to test the more vulnerability found both for free and commercial purposes publicly through the Internet. Intrusions occur when the attackers attempt to gain access to the information system and interrupt the network, and the action of the attackers is intended to harm the network. The intrusion detection and prevention mechanisms are effective in preparing the information network for attacks. It is often carried out by gathering and tracking and evaluating information from various systems for the most important safety problems. Nonetheless, a sound or visual warning may be created by the intrusion detection system, even when a violation is detected, or it may be kept quiet, such as an email or a pager alert message.



Intrusions in the network's security setting are currently becoming the biggest issue. And in order to avoid this problem, and method called an intrusion detection system has been implemented in various network domains. Intrusion detection is one of the different ways in which several device and network events may be analyzed to identify reasons for the expected incidents that that breach security policies already established for the system, e.g. unauthorized access to networks, malware and the misconduct of the user. Intrusion-detection system is the application that is able to avoid attacks on the network.
Two specific methods can be used in the field of intrusion detection: abuse detection and detection of anomalies. The key concept behind detection of misuse is to depict attacks in a way that makes it possible to detect even variants of the attacks. This method detects attacks by a broad set of rules defining any known attack on the basis of these signatures.
The key drawback is the difficulty of detecting unknown attacks from the signature-based approach. The primary aim of the anomaly detection procedure is to construct a regular traffic statistical model.

Intrusion Prevention System
Prevention of intrusion is an extension to the intrusion detection technique. The technique of intrusion prevention is used to avoid the intrusion impacting the device, which can be detected by an intrusion detection technique by blocking intrusion activities. The following are some of the common principles for this technique:
Alert: Several warnings are created in form of emails, audible signals and page updates, etc., when device users are alerted of the intrusion.
False negative: this IDPS often fails to detect and avoid attacks.
False-assault stimulus: There might be certain stimuli even though no real attack happens.
False positive: Also no true attack has been created in these warnings, so that extensive users are not responsible for assaults or intrusion.
The main goal of the IDPS is to protect the program from irregular actions triggered by misused information or the detection of security-induced attacks. It includes a specification for the security controller for the device monitoring. For the correct operation of the intrusion IDPs, sufficient information is required in order to take the appropriate recovery step by stopping or blocking the intrusion and closing the connection of the network or of the device accessibility. Based on this information.
.
Research Process
In Figure 6, the analysis method is seen in the flow map. We will analyze how the entire work is carried out utilizing this flowchart.

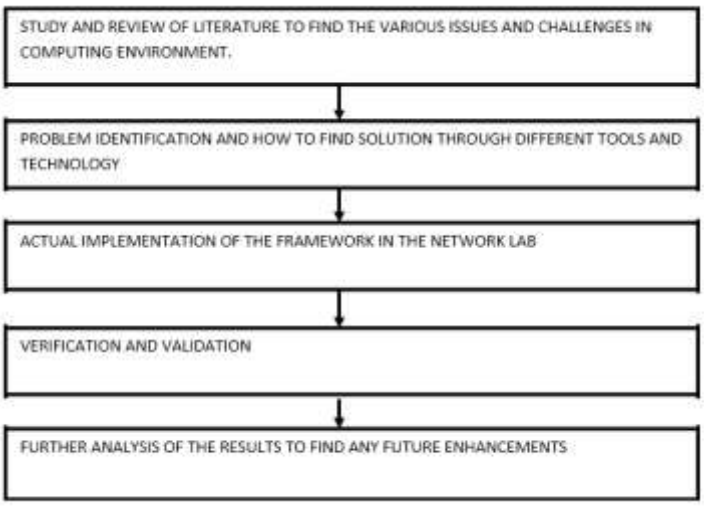


Figure Research Process

The method starts with the literature review in order to find specific study holes. They come up with question detection as soon as the literature review is through. We use numerous methods to conduct simulation for the recognition of the problems. We apply the application function in real time after the simulation and document the testing and validation details. Finally, we should review the findings for more changes.

Conclusion and Future Work

The honeypot technology framework and the exception-based IDS use two technologies. We also used KF Sensor for honey pot technologies and Snort for network based IDS. We have an algorithm, which is why we have designed and implemented architecture in real time. The cumulative log will enable the network manager take the remedial steps. The research can be expanded further by establishing a system for anomaly-based assaults.

Using this model we will recognize all forms of intruders in the network who are targeted as well as a host mechanism who supports IT organizations to meet with the protection criteria. This innovative model would definitely play a crucial role to maintain data secure, data confidentiality and data transparency respectively. Within a few years, more businesses will be adopting this innovative hybrid IDS paradigm and would thus save their computational climate. This would also play a significant part in the market not just for windows, but also for other operating systems.

References

[1] Cloud Security Alliance: Top Threats to Cloud Computing V1.0. Available: http://www.cloudsecurityalliance.org/topthreats, 2010.
[2] Dimitrios Zissis, Dimitrios Lekkas: Addressing Cloud Computing Security Issues, Future Generation Computer Systems Dec 2010, pp 583-592.
[3] Meiko Jensen et. al. : On Technical Security Issues in Cloud Computing, IEEE International conference on Cloud Computing, 2009.
[4] Jinzhu Kong et. at. : Protecting the Confidentiality of V.M Against Un-trusted Host, International Symposium on Intelligence Information Processing And Trusted Computing, IEEE, 2010, pp. 364-368.
[5] Steve Zdancewic et. al. : Untrusted Hosts and Confidentiality Secure Program Partitioning, Proceeding of the 18th ACM Symposium on Operating System Principles, Oct 2009.
[6] Lucian Popa, Minlan Yu et. al. : Cloud Police: Access Control out of the Network, Hotnets, Monterey, CA, USA, Oct 2010.
[7] Seongwook Jin et. at. : Architectural Support for Secure Virtualization under a Vulnerable Hypervisor, Appears in the 44th Annual IEEE/ACM International Symposium on Microarchitecture, Porto Alegre, Brazil, Dec 2011.
[8] Diego Perez-Botero et. at. : Characterizing Hypervisor Vulnerabilities in Clouding Computing Servers, Cloud Computing, Hangzhou, China, May 2013.
[9] Kai Hwang et. at. : Defending Distributed Systems Against Malicious Intrusions and Network Anomalies, Parallel and Distributed Processing Symposium, Proceedings. 19th IEEE International, 2005.
[10] Zhi-Hong Tian et. at. : An architecture for intrusion detection using honeypot, International Conference on Machine Learning and Cybernetics, IEEE, Nov 2003, pp. 2096-2100.
[11] Li Yun-jie and Guan Xin: An new Intrusion Prevention Attack System Model based on Immune Principle, 2nd International Conference on e-Business and Information SystemSecurity, IEEE, May 2010, pp 1-4.
[12] F5 Synthesis: Cloud Computing Network Solutions, Available: http://www.f5.com/solutions/2014.
[13] Craig Baldinng:. Itg2008 World Cloud Computing Summit, Available: Http://Cloudsecurity.Org, 2008.
[14] Ronald L. Krutz, and Russell Dean Vines: Network Security: A Comprehensive Guide to Secure Network Computing, e-book published by Wiley Publishing, Inc., 2010, pp. 61-169.

[15] Deris Stiawan et. at. : The Trends of Intrusion Prevention System Network, International Conference on Education Technology And Computer, Proceedings IEEE, 2010, pp. 217-221.
[16] Moses Garubas et. at. : Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems, International Conference on Information Technology: New Generations, Proceedings IEEE,2008, pp. 592-598.
[17] J. Gomez et. at. : Design of a Snort based Hybrid Intrusion Detection System, International Work-Conference on Artificial Neural Networks, Part- II, 2009. pp 515-522.
[18] M. Ali Ayadin et. at. : A Hybid Intrusion Detection System Design for Computer Network Security, Computers and Electrical Engineering, Vol. 35, Elsevier, Feb 2009, pp 517-526.
[19] Spyros Antonatos et. at. : Generating Realistic Workloads for Network Intrusion Detection Systems, ACM, Redwood City, CA, Jan 2004.
[20] Emmanuel Hooper, An Intelligent Intrusion Detection and Response System Using Hybrid Ward Hierarchical Clustering Analysis, International Conference on Multimedia and Ubiquitous Engineering, IEEE, 2007, pp 1187-1192.