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

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. The IDS recognizes any activity in the area of computer and network system that violates security policies. In case of risk exposure from any attack, IDS can submit early alarm. Used to warn device managers to perform subsequent analyses of the effects and reduce the risk of major losses. A PC-implemented intrusion detection system is a method that is used for in-press surveillance of a computer system for real-time access by unauthorized persons or devices. The system detects unauthorized users who are trying to enter a computer system by matching user behavior to a User profile. When a computer user first tries to log on to the computer system and the identity of the user is dynamically updated, the user profiles are created for each computer user. False alarms are minimized by contrasting user behavior to the dynamically configured user profile. The attack attacks on computer systems are now on the rise, together with the advanced penetration methods, with the promotion of internet and local networks [3].**

***Keywords*: IDS systems, abnormal detection system, WSN, cluster head, adhoc networking**

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.

WSN Threats

WSN is now one of the most common technologies. It is recorded in a number of assaults on WSN. Various tests have been suggested to address such assaults. The key category of attacks are described below. The passive assault is limited to traffic listening and study. It is easy to execute this sort of attack and hard to identify. As there is no impact on the data transmitted by the intruder. Through studying routing details and by planning a successful attack, the purpose of the intruder could be a knowledge about sensitive information or the awareness of critical network nodes. During an active assault, the intruder tries to erase or alter communications. During attempting to interrupt a site Denial, he can either insert his own traffic or re-play old messaging. The most common active attacks involve network transmissions. Network service or following:

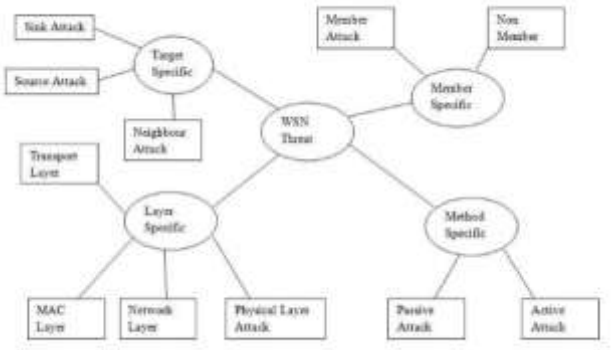


Fig1. Structure of WSN Threats

Need of Security:-
Different types of protection requirements are required to maintain the WSN communication process.
That can be described simply as:-

Fig 2. Basic Need of security

Confidentiality:-
This protection parameter is used to maintain the confidentiality of any details and in a person. It is one of the most important functions of health.

Integrity:-
The transmitted messages that intrude or not steal or alter. CRC is usually used for test failures (Cyclic Redundancy Checksum). At the time of transmission, it is mainly the job of securing the data.

Availability:-
Different kinds of attacks allow attacks that minimize or abrupt the network's efficiency. The access denial is one of the most crippling assaults on the accessible network.

Authentication:
It is the health factor that is most significant. It is used primarily for the private holding of the communication nodes. At the time of transmission, each node present in the network should be checked repeatedly.

Privacy:-
This criteria for encryption is to insure that data enters the correct destination only. By submitting data to the appropriate destination, it protects consumer and sender privacy.

Survivability:-
This is one of the essential protection criteria in the face of attacks in the event that a device capacity is timely to accomplish its task.

Time Synchronization:-
Time synchronization is an essential, highly sensitive aspect of sensor network protection. When there is a period difference, it is exceedingly complicated and imprecise to classify the target by the sensor.

Fig 3. Security requirements in WSN

Restriction in WSN:
A WSN comprises of extension nodes of sensors that are resource-limited machines. When transmitting data, capacity is that by the nodes, less data transmission volume and restricted communication bandwidth. Due to the available resources and the tiny size of the sensor nodes, it is challenging to enforce the protection function in WSN.

Memory Restrictions:-
Less memory use as available capacity is utilized. Likewise, sensors are also sponsored. Likewise, sensors go with them, too. The sensor provides less data storage space so that less memory is used. Basically, the sensor node is a flash and RAM memory. The application data has been placed in flash memory, and RAM is contained in the framework software. This is very difficult to perform complicated algorithms due to reduced space following installation of the program code and the OS.

Energy Restrictions:-
WSN's biggest weakness is electricity. While transmission takes place in WSN, it is examined that WSN consumes the same strength as 800 to 1000 orders. The utilization of electricity is classified into three segments :-(a) transmitting electricity; (b) microprocessor processing energy. c.) power used by the sensor transducer.

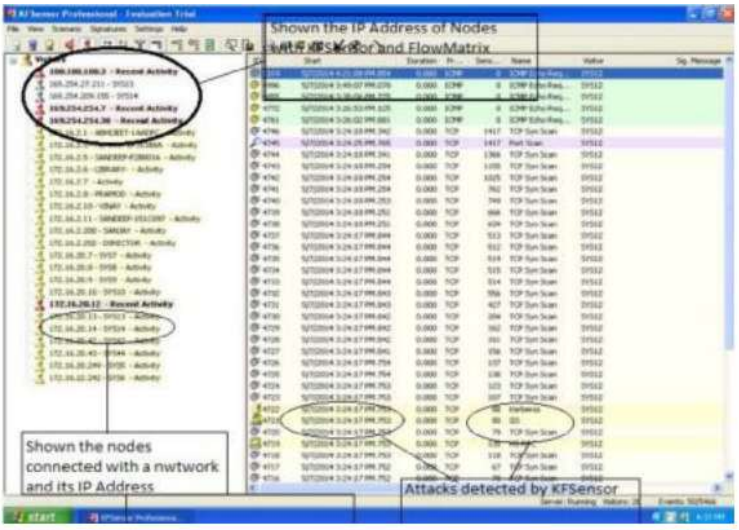
Higher Latency
Synchronization is very challenging to accomplish, and the key factor is for packet delivery, including multi-hop forwarding, network congestion and intermediate node management in WSN. When mentioned above, synchronization is difficult to accomplish but synchronization is important, since other systems rely on the key distribution of encryption and recording crucial events.

Unreliable Communication:-
This is one of the main challenges to sensor stability. The packet-based routing of the network sensor is used on such a wired computer. It is a connection-free protocol. Since packets destroyed by channel errors. When the connection is secure, the contact is not required in certain circumstances. This condition happens as the packets retransmit each other.

The neglecting action of networks:-
In certain approaches, nodes in distant areas which are ignored by WSN are currently placed. This is one of the explanations why the sensor is experiencing a strong body assault.

Challenges in WSN:-
Resource controls are used, for example, to allow the efficient usage of services. Routing mindful of electricity etc.
To reduce the crash in fault tolerance to sudden node failures. A reliability analysis and its process for non-authentic wireless communication was carried out. The data-centered model for non-global sensor recognition is used to concentrate the data produced by the sensor community. For efficient network service, complex conditions and supreme environments are included. Fusion of data and hierarchical sorting techniques are essential for the elimination of database redundancies.

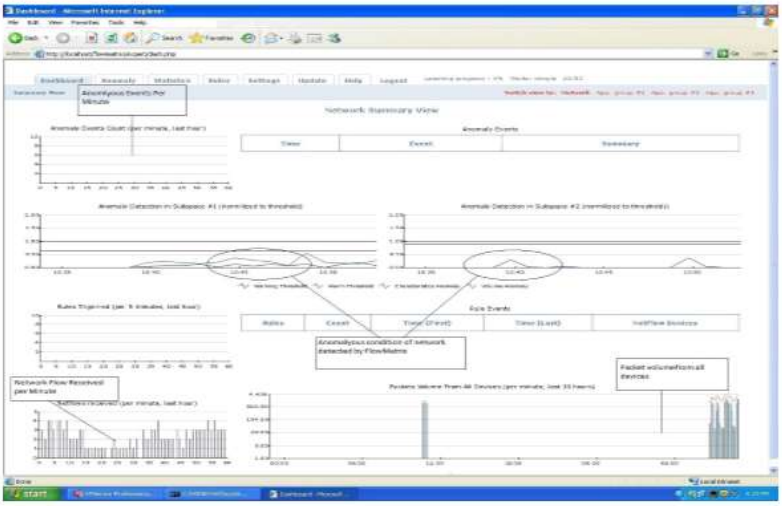
Analysis of Phase
The attack or the creation of network traffic has three nodes (computers). The domain with Flow Matrix and application IP address 172.16.20.13 have an Network address as 172.16.20.10, 172.16.20.11 and 172.16.20.12, and the IP address node as 172.16.20.13 is the domain with KF sensor. Here, we used several more attackers to target various network devices such as router, switches, servers and others. Network traffic is generated through various tools, such as target Ping, free port scanners and free SNMP. These devices will create multiple logs during the attack. The log shows that the KF sensor only explicitly connects to the server, and only tracks certain nodes that ignore other nodes. These three nodes 172.16.20.10, 172.12.10.1, 172.16.2012 and the attack all show the network activity.



GUI of KF Sensor

we can see the operation of the network through nodes and attacks as the circle indicates. Using the KF sensor, you can see that the honeypot is attracting the batter. Then, the honeypot cannot only detect attacks that already exist in the database, but also detect new attacks through honeypot technology, and render and upload the signatures of these attacks. In the database: KF sensor and

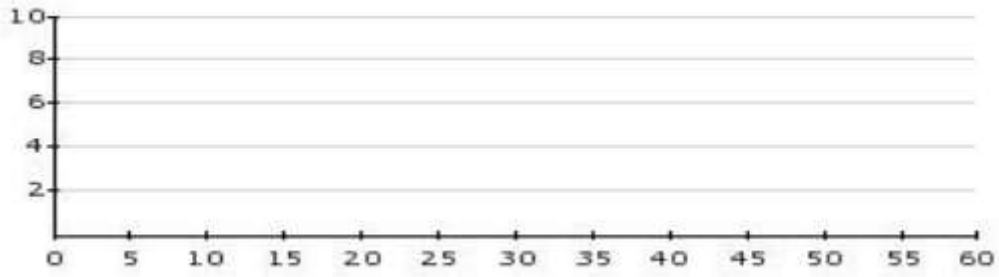
flow matrix uniquely detect attacks. They are unable to track assaults on other network networks. The displays the IDS focused on "Flow matrix" anomaly detection that identifies all forms of network assaults.



Anomalous behavior capture by Flow Matrix

The thorough review of the effects proceeds

Incongruity Events Calculation–
This shows the cumulative amount of the time period with event alarms. The execution time is 1 minute in the normal flow matrix. The last 60 minutes are seen in this table. Alarms and not alerts are displayed only in the table. No anomaly warning was observed at 9:52-10:52 am on 7 April.



count of Anomaly Event

Anomaly Proceedings
Growing alarm can be monitored by clicking on the overview alarm label. This will offer the pages some detail about the alert which discusses whether alerts or notifications were regarded. If required, the classification details of the alert are identified as belonging to a specific category of anomaly. We will obtain most of the information on site, and further determine, accept and investigate alerts, or ignore false alarms or known anomalies. Since there were no other extreme anomalies from 9:52-10:52 on April 7th, should be regarded as a blank row.

Table: occurrence of Anomaly event

Within the map of subspace #1, deviation identification is provided with statistics linked to the relevant thresholds. The statistical model divides network traffic into individual network clusters and network clusters and subspaces across network clusters. In Subspace ° 1 graph disturbances in minor magnitudes (low intensity assaults, search, etc.) are usually apparent, although in both Subspace # 2 or much of the time broad scale deviations can be observed (worms, alpha flashes, etc.). When applied to several traffic clusters, all subspaces will concurrently and separately identify volume and function abnormalities.

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.

[21] Prof. Smita Jawale et. at. : Intrusion Detection System using Virtual Honeypots, International Journal of Engineering Research and Applications, Mar 2012, pp 275-279.