ISSN:0975-9646

Unwanted Activity Detection System in Wireless Network

Sneha A. Deshmukh [1] , Monika Rajput [2]

[1]*M.E. Student* ,[2]*Professor*
P.R. Pote COET Amravati, India

Abstract **- This paper present how the security can be given to the wireless network with the help of intrusion detection system and firewalls. With the rapid growth of application of Internet in various walks of life, the study of Security has become inevitable. Wireless networks are providing tremendous benefit for a number of industries. This paper focuses different kinds of wireless network i.e. mobile ad hoc network, wi-fi and bluetooth. Although Wireless Networks have appealing features (e.g., low installation cost, unattended network operation), due to the lack of a physical line of defense (i.e., there are no gateways or switches to monitor the information flow), the security of such networks is a big concern.**

Keywords**:-Wireless Network Security, firewall, Intrusion detection system, mobile ad-hoc, wi-fi, bluetooth.**

I. INTRODUCTION

What is security?

"Security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization"[1].Need for security is given by-

- Protects the data that organization collects and uses.
- Safeguards the technology assets in use at the organization.
- Protects the organization's ability to function**.**

II. WIRELESS NETWORK

"Wireless is a term used to describe telecommunication in which electromagnetic wave carry the signal over the part or all of the communication path "[7][8]. Wireless technology has emerged as a very popular alternative to wired technology in recent years and has become more readily available for computer networks anywhere, whether it is for a home, an office, or any size of business. Wireless or WiFi technology is another way of connecting a number of computers to a network without using wires. WiFi uses radio frequency to connect wirelessly, so there is greater freedom to connect computers from anywhere in a home or an office network.1 This technology is similar to how a cordless phone would work, using radio signals to transmit data from one point to another. However, wireless technology has restrictions on accessing a network, such as the network range. Two types of wireless networks are Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN)

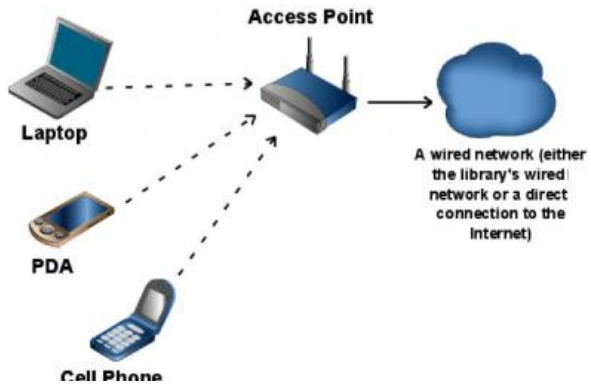

Figure 01 :-An example wireless router, that can implement wireless security features

III. WI-FI

Wi-Fi can also be used to provide wireless broadband Internet access for many modern devices, such as laptops, smart phones, tablet computers, and electronic gaming consoles. Wi-Fi-enabled devices are able to connect to the Internet when they are near areas that have Wi-Fi access, called "hot spots." Hot spots have become common, with many public places such as airports, hotels, bookstores, and coffee shops offering Wi-Fi access[6]. Some cities have constructed free citywide Wi-Fi networks. A version of Wi-Fi called Wi-Fi Direct allows connectivity between devices without a LAN.

Figure 02:-Wi-Fi

IV. MOBILE AD HOC NETWORK

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension .In the mobile ad hoc network, nodes can directly communicate

with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. The following figure shows the mobile ad-hoc network[13]:

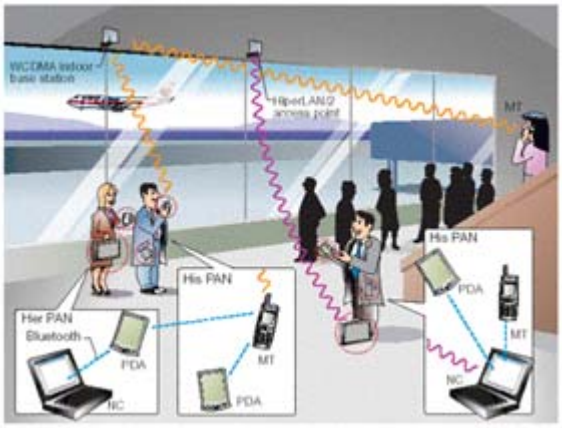

Figure 03 :- Mobile ad-hoc network Airport scenario

The mobile ad hoc network has the following typical features

- Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.
- Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.
- Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

V. BLUETOOTH

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength radio waves in the ISM band from 2.4 to 2.485 GHz and mobile devices, and building personal area networks (PANs). Bluetooth is a high-speed, low-power microwave wireless link technology, designed to connect phones, laptops, PDAs and other portable equipment together with little or no work by the user. Unlike infra-red, Bluetooth does not require line-of-sight positioning of connected units. The technology uses modifications of existing wireless LAN techniques but is most notable for its small size and low cost

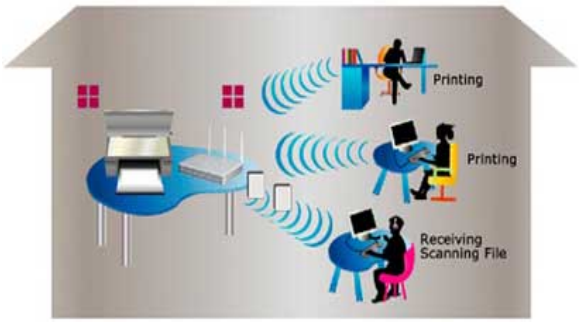

Figure 04: Bluetooth

Feature of Bluetooth Technology:

- Bluetooth technology is a wireless communications technology that is simple, secure, and everywhere. You can find it in billions of devices ranging from mobile phones and computers to medical devices and home entertainment products. It is intended to replace the cables connecting devices, while maintaining high levels of security.
- The key features of Bluetooth technology are ubiquitousness, low power, and low cost. The Bluetooth Specification defines a uniform structure for a wide range of devices to connect and communicate with each other.
- When two Bluetooth enabled devices connect to each other, this is called pairing. The structure and the global acceptance of Bluetooth technology means any Bluetooth enabled device, almost everywhere in the world, can connect to other Bluetooth enabled devices located in proximity to one another.
- Connections between Bluetooth enabled electronic devices allow these devices to communicate wirelessly through short-range, ad hoc networks known as piconets. Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave radio proximity meaning that you can easily connect whenever and wherever it's convenient for you.

VI. BASICS OF INTRUSION DETECTION SYSTEMS

An intrusion is when anyone, usually a hacker, attempts to break into or misuse a computer system. An Intrusion Detection System is a system for detecting such intrusions. A network IDS will continually monitor packets on a network wire and attempt to discover whether a break into the system has been attempted. The IDS can also try to determine other intrusions such as an attempt to cause a 'denial of service' attack to freeze the ability of the network

to handle data traffic. In some cases, an IDS may be able to respond to anomalous or malicious traffic by taking action, such as reconfiguring a remote firewall in order to block a user IP address or port from gaining access into a network.

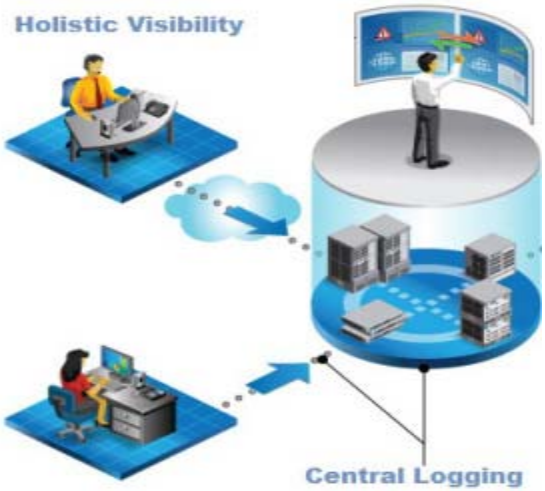

Figure 05 :- Intrusion Detection System

VII. FIREWALL

A firewall is a software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on applied rule set. Firewalls can be defined in many ways according to your level of understanding. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted. Most firewalls will permit traffic from the trusted zone to the untrusted zone, without any explicit configuration. However, traffic from the untrusted zone to the trusted zone must be explicitly permitted. Thus, any traffic that is not explicitly permitted from the untrusted to trusted zone will be implicitly denied (by default on most firewall systems). A firewall is not limited to only two zones, but can contain multiple 'less trusted' zones, often referred to as Demilitarized Zones (DMZ's)

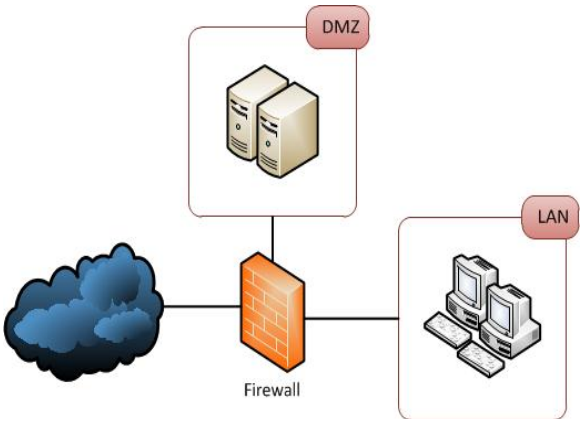

Figure 06 :-Firewall

Feature of Firewall

They can control access to other services e.g.

- bar callers from certain IP addresses,
- filter the service operations (both incoming and outgoing), e.g. stop
- FTP writes
- hide information e.g. by only allowing access to certain directories or systems

They are more cost effective than securing each host on the corporate network since there is often only one or a few firewall systems to concentrate on.

They are more secure than securing each host due to:the complexity of the software on the host - this makes it easier for security loopholes to appear.

VIII. WIRELESS NETWORK RISKS

Having a wireless network set up has made life a lot easier by getting rid of the annoying wires and cables that may lie across the room, over the ceilings, and under the floors. Today's network marketplace indicates that wireless networking has been installed in many businesses, even in preference to the wired networks that have been commonplace for many years. By just about any measure, WLAN usage is growing at a rapid pace worldwide. However, this has also created an environment where there is great chance for intrusion, such as people being able to see each other's files and personal information. Therefore, Wireless LAN's still have their share of problems, with security playing a major part.The following characteristics must be provided if security is desired for a WLAN3:

- Confidentiality: Assurance that the message sent is readable only by the intended recipient (i.e., protection against interception, or eavesdropping)
- Authenticity: Assurance that the message originates from the claimed entity (i.e., protection against spoofing, or impersonation)
- Integrity: Assurance that the message has not changed in transmission (i.e., protection from transmission errors and/or intended modification of message)
- Availability: Assurance that the data will be available whenever and wherever required (i.e., protection against denial of service or poor reliability)

IX. VULNERABILITY MOBILE AD HOC NETWORK

Mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. In this section, we discuss the various vulnerabilities that exist in the mobile ad hoc networks.

i. Lack of Secure Boundaries

There is not such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network[13].

ii. Lack of Centralized Management Facility

Ad hoc networks do not have a centralized piece of management machinery such as a nameserver, which lead

to some vulnerable problems**.**First of all, the absence of centralized management machinery makes the detection of attacksa very difficult problem because it is not easy to monitor the traffic in a highly dynamic andlarge scale ad hoc network .It is rather common in the ad hoc network that benign failures,such as path breakages, transmission impairments and packet dropping, happen frequently.Therefore, malicious failures will be more difficult to detect, especially when adversarieschange their attack pattern and their attack target in different periods of time.

iii. Threats From Compromised Nodes Inside The Network

We mainly discuss the vulnerability that there is no clear secureboundaries in the mobile ad hoc network, which may cause the occurrences of various linkattacks. These link attacks place their emphasis on the links between the nodes, and try toperform some malicious behaviors to make destruction to the links. However, there are someother attacks that aim to gain the control over the nodes themselves by some unrighteous means and then use the compromised nodes to execute further malicious actions. This vulnerability can be viewed as the threats that come from the compromised nodes inside the network[13].

iv. Restricted Power Supply

The first problem that may be caused by the restricted power supply is denial-of-serviceattacks . Since the adversary knows that the target node is battery-restricted, either it can continuously send additional packets to the target and ask it routing those additional packets, or it can induce the target to be trapped in some kind of time-consuming computations. In this way, the battery power of the target node will be exhausted by these meaningless tasks, and thus the target node will be out of service to all the benign service requests since it has run out of power.

v. Scalability

Finally, we need to address the scalability problem when we discuss the vulnerabilities in the mobile ad hoc network . Unlike the traditional wired network in that its scale is generally predefined when it is designed and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because of the mobility of the nodes in the mobile ad hoc network, you can hardly predict how many nodes there will be in the network in the future. As a result, the protocols and services that are applied to the ad hoc network such as routing protocol and key management service should be compatible to the continuously changing scale of the ad hoc network, which may range from decades of nodes to hundreds of nodes, or even thousands of nodes. In other words, these protocols and services need to scale.

Attack Mobile Ad Hoc Network

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types :

a) External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

b) Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

i. Denial of Service (DoS)

The first type of attack is denial of service, which aims to crab the availability of certain node or even the services of the entire ad hoc networks. In the traditional wired network, the DoS attacks are carried out by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and make the services provided by the target become unavailable.

ii. **Impersonation**

Impersonation attack is a severe threat to the security of mobile ad hoc network . As wecan see, if there is not such a proper authentication mechanism among the nodes, the adversary can capture some nodes in the network and make them look like benign nodes.

iii. Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks.The goal of eavesdropping is to obtain some confidential information that should be kept secret during the communication. The confidential information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

X. SECURITY THREATS AND VULNERABILITIES IN BLUETOOTH

Bluetooth technology and associated devices are susceptible to general wireless networking threats, such as denial of service (DoS) attacks, eavesdropping, MITM attacks, message

modification, and resource misappropriation. They are also threatened by more specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Attacks against improperly secured Bluetooth implementations can provide attackers with unauthorized access to sensitive information and with unauthorized use of Bluetooth devices and other systems or networks to which the devices are connected

XI. SECURITY SCHEMES IN THE MOBILE AD HOC NETWORKS

Intrusion Detection Techniques

Intrusion detection is not a new concept in the network research. According to the definition in the Wikipedia, an Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems [17]. Although there are some differences between the traditional wired network and the mobile ad hoc network, intrusion detection technique, which is developed first in the wired network and has become a very important security solution for the wired network, has also gained some attentions from the researchers when they explore the security solution for the

mobile ad hoc network. In the following, we discuss some typical intrusion detection techniques in the mobile ad hoc networks in details.The first discussion about the intrusion detection techniques in the mobile ad hoc networks was presented in the paper written by Zhang et al. This is a general intrusion detection framework in MANET was proposed, which was distributed and copperative to meet with the needs of MANET. The proposed architecture of the intrusion detection system is shown below in figure. The internal structure of an IDS agent is shown in Figure below.

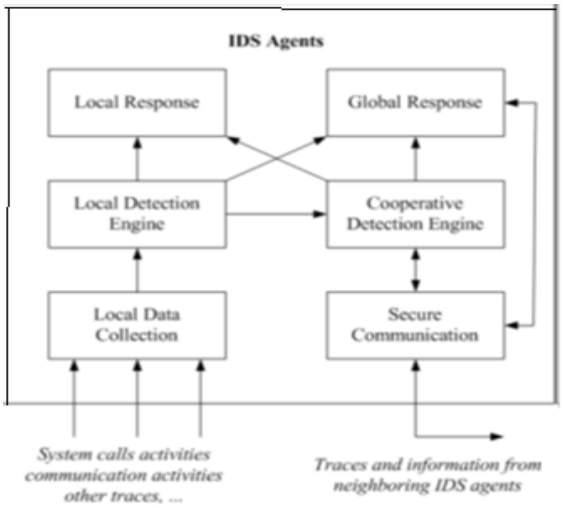

Figure 07:-Conceptual model for IDS

In the conceptual model, there are four main functional modules:

- Local data collection module, which mainly deals with the data gathering issue, in which the real-time audit data may come from various resources.
- Local detection engine, which examines the local data collected by the local data collection module and inspects if there is any anomaly shown in the data. Because there are always new attack types emerging as the known attacks being recognized by the IDS, the detection engine should not expect to merely perform pattern recognition between known attack behaviors and the anomalies that are likely to be some intrusions: instead of the misuse detection technique that cannot deal with the novel attack types effectively, the detection engine should mainly rely on the statistical anomaly detection techniques, which distinguish anomalies from normal behaviors based on the deviation between the current observation data and the normal profiles of the system.
- Cooperative detection engine, which works with other IDS agents when there are some needs to find more evidences for some suspicious anomalies detected in some certain nodes. When there is a need to initiate such cooperated detection process, the participants will propagate the intrusion detection state information of themselves to all of their neighboring nodes, and all of the participants can calculate the new intrusion detection state of them based on all such information they have got from their neighbors by some selected algorithms such as a distributed consensus algorithm with weight. Since we can make such a reasonable assumption that majority of the nodes in the ad hoc network should be benign, we can trust the conclusion drawn by any of the participants that the network is under attack.
- Intrusion response module, which deals with the response to the intrusion when it has been confirmed. The response can be reinitializing the communication channel such as reassigning the key, or reorganizing the network and removing all the compromised nodes. The response to the intrusion behavior varies with the different kinds of intrusion.

A. Advantages of Intrusion detection system:

1. This is especially true if the network administrator has not granted the user access to files in other departments. IDS can also detect fake and stolen accounts, and take immediate action on such intrusions.
2. An IDS can also detect when individuals within the network misuse network resources. Users find ways to circumvent network security policies. An IDS makes it possible to detect which specific user or computer violated security policies.

Advantages of Firewall

1. Some firewalls but not all can detect viruses, worms, Trojan horses, or data collectors.
2. All firewalls can be tested for effectiveness by using products that test for leaks or probe for open ports.
3. A feeling of increased security that you're PC and contents are being protected.
4. Relatively inexpensive or free for personal use**[1]**.

XII. CONCLUSION

This paper present the importance of wireless network security. Then we focus on what is mean by Wireless and mobile ad-hoc network.The brief description can be given for the wi-fi and MANET. This paper represent how the attack can be occurred on that syatem. Then we see how the security can be given to these systems.We provide security with the help of Intrusion Detection System and Firewall.We see that what are the advantages of IDS, firewall ,we also study how that wireless network can be secured with the firewalls, IDS. Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network. With all its capabilities along with assistance with policy enforcement, the advantages of the wireless IDS can be significant. Keep in mind however that the wireless IDS is only one part of a potential greater solution to wireless security. Other security measures may be deployed to reach the level of security desired for the entire WLAN, but the wireless IDS, can greatly enhance the Network security.

REFERENCES

[1] William Stalling (Computer Network & Security}

[2] Shuyao Yu Youkun Zhang Chuck Song Kai Chen A Security Architecture For Mobile Ad Hoc Networks. Technical Report Institute Of Computing Technology Center Of Chine's Academy Of Science.

[3] J. Kong, P. Zerfos, H. Luo, S. Lu, And L. Zhang, "Providing Robust And Ubiquitous Security Support For Mobile Ad Hoc Networks", Proc. Ninth Int'l Conf. Network Protocols(ICNP), Nov. 2001.

[4] Intrusion Detection: Challenges And Myths By Marcus J. Ranum Http://Secinf.Net/Info/Ids/Ids_Mythe.Html

[5] Y. Zhang, W. Lee, And Y. Huang, \Intrusion Detection Techniques For Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003..

[6] Special Issue On Wireless Com6puting. Commun. ACM 37, 10 (Oct.1994).

[7] Tanenbaum, A. Computer Networks, 3d Ed. Prentice Hall.

[8] Varshney, U. Supporting Mobile Computing Using Wireless ATM. IEEE Computer (Jan. 1997).

[9] Building Internet Firewalls Second Edition, O'Reilly - A Thorough Reference And Tutorial.

[10] Internet: Welcome to MagicLAN, WLAN Introduction; Retrieved 12/2004;

[11] Address http://www.magiclan.com/en/about/KmlMLanIntro_03.jsp

[12] Stanley, Richard A., Internet: Wireless LAN Risks and Vulnerabilities; Retrieved 1/2005; Address http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=13592

[13] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.

[14] Intrusion-detection system, from Wikipedia, the free encyclopedia,http://en.wikipedia.org/wiki/Intrusion-detection_system.