International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Comparative Analysis of Hybrid Intrusion Detection System and Intrusion Prevention System for MANET

Pallavi P Puri[1], Nitin R. Chopde[2]

[1]Student of Master of Engineering (Computer Science & Engineering), Raisoni College of Engineering and Management, Amravati, India

[2] Professor, Head of Department of Computer Science & Engineering, Raisoni College of Engineering and Management, Amravati, India

Abstract*: In the entire globe, higher learning institutions, organizations and governments are completely dependent on the computer networks which plays a important role in their day to day operations. So the necessity for protecting those networked systems has also increased. Intrusion Detection System which is increasingly a key element of system security is used to identify the malicious activities in a computer network or system. There are different approaches being employed in intrusion detection systems, but unfortunately none of each of the technique so far is not entirely ideal. Intrusion Prevention Systems (IPS) evolved after that to resolve ambiguities in passive network monitoring by placing detection systems on the line of attack. The main functions of IPS's are, as explained to identify malicious activity, log information about it, and attempt to block or stop and report that activity. IPS in other words is IDS that are able to give prevention commands to firewalls and access control changes to routers. The proposed paper made a survey on the overall progress of intrusion detection systems & intrusion prevention system. It also includes survey of existing types, architectures and techniques of Intrusion Detection Systems & Intrusion Prevention System in the literature.*

Keywords: Mobile ad hoc networks, Intrusion detection system, Intrusion prevention system, Network layer attacks Hybrid Intrusion Detection System, Hybrid Intrusion Prevention System.

1. Introduction

In the 1990's the concept of mobile wireless devices working together was proposed, a significant amount of research has been conducted on mobile ad hoc networks (MANET's).A mobile ad hoc networks (MANET) is a continuously self-configuring, infrastructure-less networks of mobile devices connected without wires. In MANET, the router connectivity may change frequently, leading to the multi-hop communication paradigm that can allow communication without the use of AP/BS, and provide alternative connections inside hotspot cells. All nodes in this network are mobile and they use wireless connections to communicate with various networks. They developed two standard track routing protocol specifications, the reactive and proactive MANET protocols [1]. MANET's are vulnerable in their functionality intruders can compromise the operation of the network by attacking at any of the layers like physical, MAC or network layers. Standard information security measures such as encryption and authentication do not provide complete protection, and, therefore, intrusion detection system (IPS) and intrusion prevention system (IDP) mechanisms are most widely used to secure MANETs [1]. Intrusion Detection is the process of monitoring events occurring in a network or computer system & analyzing them for signs of possible incidents of threats and violations of computer security practices, acceptable use policies or standard security policies. Intrusion Detection System (IDS) is a hardware or software component that automates the process of intrusion detection. It is designed to monitor the events occurring in a network and computer system and responds to events with all signs of possible incidents of violations of network security policies [2]. An Intrusion Prevention System (IPS) is a network device or software that identify and block network threats by assessing each and every packet based on the network protocols in the network layer, tracking each session. It can be considered as an extension of firewalls with extra security. Intrusion Prevention System is a down to business defense mechanisms designed to detect malicious packets within network traffic and stop intrusions dead, blocking the aberrant traffic automatically before it does any damage rather than simply giving an alert as, the malicious load has been delivered. It were invented independently to resolve ambiguities in network monitoring by placing prevention systems in-line on the network monitoring and the incoming packets based on certain prescribed rules and if bad passage is detected, it is dropped in real-time. It helpful to sense and prevent attacks like brute force attacks, vulnerability detection, DoS/DDoS attacks, protocol anomaly prevention and detection unidentified attacks. IPS technologies are session based and traffic flow is examined based on session flow [3].

Licensed Under Creative Commons Attribution CC BY

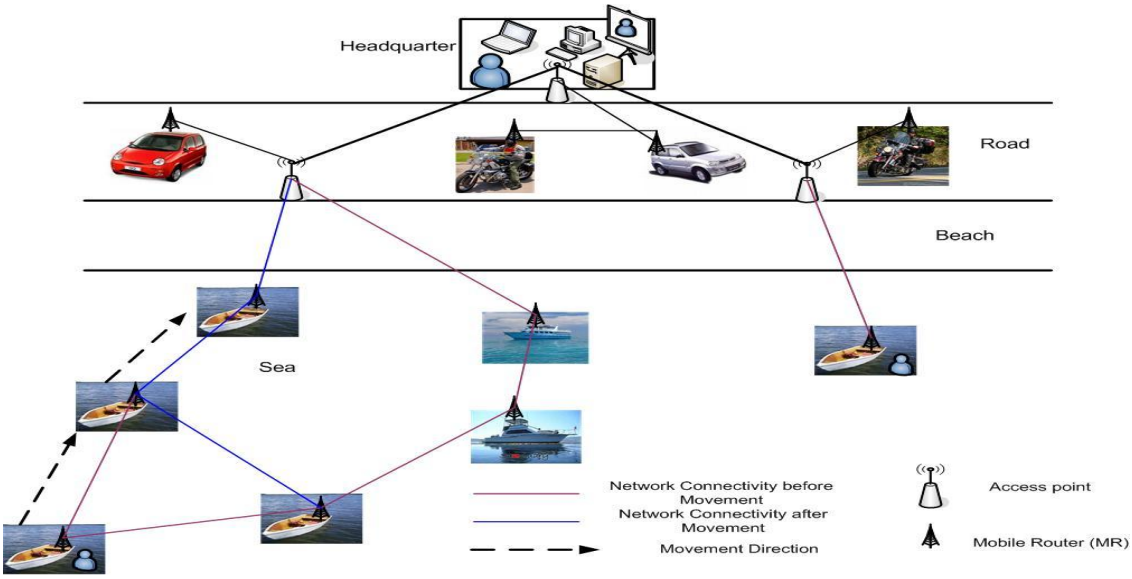

Figure 1: Mobile Ad hoc Network

2. Literature Survey

The studies of Intrusion detection has been progressive field of research from more than three decades now. It started in 1980 with the publication of John Anderson's Computer Security threat surveillance and monitoring, which is one of the latest research papers on this field. Dorothy Denning's important paper, "An Intrusion Detection Model" published in 1987 gives a methodological framework that inspired a number of researchers. After that, for the last two decades, In spite of substantial research and large commercial investments, Intrusion Detection technology is in effective and immature .In the early days, hackers hardly used automated tools to break into systems. They were intelligent with a high level of expertise and followed methodology of their own to perform such an actions. The recent scenario is quite different. A various number of intrusion tools and applications are available that can be used to exploit scripts that capitalize on widely known vulnerabilities. Depicts the relationship between the relative sophistication of attackers and attackers from 1980 to until now. Before the modern IDS, intrusion detection consisted of a manual search for anomalies. Due to the availability of adequate processing speed it now possible to look for attack patterns after the event had occurred and to monitor it in ''real-time'' and trigger alerts if intrusions were detected. In last few years, researchers have been actively exploring many mechanisms to ensure the security of data and control traffic in wireless networks. These mechanisms can be largely categorized into the various classes—authentication and integrity services, protocols that depends on path variety, protocols that use specific hardware, protocols that require explicit acknowledgments or use statistical methods, and protocols that overhear neighbor communication[3]. The unauthorized users are deployed in secure WLANs without permission or knowledge of the network administrator. The presence of such unauthorized users poses severe threats to the WLAN security as it could compromise security of the entire wireless LAN network. This problem has been in existence ever since WLANs have become popular in commercial applications. IPS functions as radar to monitor stream network traffic; recognising, detecting, and identifying any signal that could be considered a security violation. In 2011, Hu [4] declared IPS has correlation between firewall and intrusion detection, also design and implementation of trusted communication protocol based on XML is provided , and then E.E. Schultz and E. Ray, had predicted the future of IPS technology, such as (i) advancement in application-level analysis, (ii) better underlying intrusion detection, (iii) more sophisticated response capabilities, (iv) integration of intrusion prevention into other security devices[5]. The prediction concerns on intrusion prevention technology which are very positive in market. Previously, in 2004 E. Schultz, has predicted IPSs to have a bright future, this technology will continue to be used by a wide number of organizations to the point that it will become a commonplace as intrusion detection technology. More recently, performed work by A. Salah, M. Shouman, and H.M. Faheem describes superior characteristic of host based IPS and use the term detection approach to show how IPSs work. The feature function of IPS is shown Intrusion Prevention provides numerous capabilities at both the network level and the host level, but from a high-level perspective, the capabilities provided by IPSs fall into two main categories: (i) Attack prevention, and (ii) Regulatory compliance [4]. Many types of IPSs potentially avoid the weakness of signature-based intrusion detection systems and it can learn classes of harmful system behaviour and the types of events that they attempt to produce in targeted system. It is much better suited to react appropriately to zero-day attacks. Hence, from this analysis, it is identified that IPS will also become more proficient because IDS, early detection, intrusion response .In this section introduces a classification (Debar *et al.*, in 1999) of intrusion detection systems that highlights the current research status. This classification defines families of intrusion detection systems according to their properties. The intrusion detection approaches can be classified into anomaly based and signature based which any network security tools are mostly using (Ozgur *et al., in* 2005) [6].One more classification can be made by considering source of data used for intrusion detection. The taxonomy can be given based on the information derived from a single host (named as Host based IDS (HIDS)) and

Licensed Under Creative Commons Attribution CC BY

the information derived from complete segment of the network that is being monitored (named as Network based IDS (NIDS). IDS can be categorized upon its operation as centralized or standalone applications that create a distributed system. Standalone systems will be working individually without any agents but centralized applications work with autonomous agents that are capable of taking pre-emptive and reactive measures.

3. Attacks in MANET's

Various types of network layer attacks are known for MANETs. Classification of major network layer attacks and introduce some individual attacks. Some major network layer attacks are as follow.

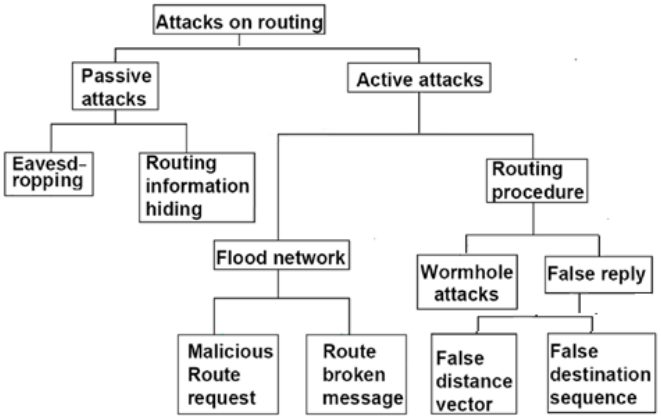

Figure 2: Attacks in MANET

Types of Network Layer Attacks
Network layer attacks in MANETs can be divided into two major categories, as passive attacks and active attacks

A. Passive Attacks:
Passive attacks are those where the attacker does not disturb the operation of the routing protocol but attempts to grab some valuable information through traffic analysis. This can leak critical information about the network or nodes such as the location of nodes, the network topology or the identity of important nodes. Examples of passive attacks are eavesdropping and traffic analysis & location disclosure.

1) **Eavesdropping:**
In MANETs as links are wireless, a message sent by a node can be heard by every device equipped with a transceiver and within that radio range, and attacker can get useful information. Without being known to the sender and receiver. It is also known as disclosure attack. The attacker collects information e.g. Private key, public key or even passwords of the nodes and analyzes broadcast messages to reveal useful information about the network.

2) **Traffic Analysis & Location Disclosure:**
In this the network traffic and messages are examined to find out information. It is performed on encrypted messages Attackers can listen to the traffic on wireless links to discover the location of target nodes by analyzing the communication pattern, the characteristics of the transmission and the amount of data transmitted by nodes.

B. Active Attacks
An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Intruders launch intrusive activities such as modifying, injecting, forging, fabricating or routing packets or dropping data, resulting in various disruptions to the network. Active attacks interrupt the operations of the network and can be so strong that they can bring down the entire network or degrade the network performance remarkably , as in the case of denial of service attacks. Some of these attacks are caused by a single activity of an intruder and others can be caused by a sequence of activities by colluding intruders. Active attacks can be further divide into flood network attacks and routing attacks.

1) **Flooding Attack:**
In flooding attack , attacker use up the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance.

2) **Malicious Route Request:**
A path between a destination node and a source node in a MANET is established using a route discovery process. The source node starts sending the data packet to the next node with the path; then this intermediate node identifies the next hop node towards the destination along the established path and forwards the data packet to it. This process continues till the data packet reaches the destination node. To achieve the desired operation of a MANET, it is significant that intermediate nodes forward data packets to each and all source nodes. However, a malicious node might decide to drop these packets instead of forwarding them; this is known as a data packet dropping attack, or data forwarding misbehaviour. In some cases nodes are unable to forward data packets because they are overloaded or have low battery reserves.

3) **Routing Attacks:**
Both the reactive and proactive routing protocols are vulnerable to routing attacks as they route based on the assumption that all nodes cooperate to search the best path. Malicious node can utilize the vulnerabilities of the cooperative routing algorithms and the lack of centralized control to launch routing attacks. In particular, the on-demand (reactive) MANET routing protocols, such as AODV and DSR, allow intruders to launch a wide variety of attacks. In the following we give examples of how different intrusive activities can cause various attacks in MANETs, illustrating them with AODV as the routing protocol.

4) **Worm Hole Attack:**
The tunnel exist between two malicious nodes is referred to as a wormhole .In wormhole attack, malicious node receive data packet at one point in the network and tunnels them to another malicious node [8]. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Wormholes are hazardous because they can do damage without even knowing the network. Attackers use wormholes in the network to make their nodes appear more attractive so that more data is routed through their nodes [9].When the wormhole attacks are used by attacker in routing protocol such as DSR and AODV, the

Licensed Under Creative Commons Attribution CC BY

attack could block the discovery of any routes other than through the wormhole.

5) False Reply:
A reply attack is a form of network attack in which a valid data transmission is fraudulently or maliciously delayed or repeated. This is performed either by the originator or by an adversary who intercepts the data and retransmits it. These replay attacks are later misused to disturb the routing operation in a MANETs.

6) False Distance Vector Attack:
In both Ad Hoc On-demand Distance Vector (AODV) and Destination Sequence Distance Vector (DSDV) the hosts collect routing information solely from direct neighbours. The incomplete understanding of global topology leads to false distance vector attacks. The malicious host can claim that the destination is one (or a few) hop(s) from it in the routing update packets or RREP even if it does not have any available path in its routing table. If no other replies provide a shorter or fresher route, the source will select the path provided by the malicious host, and the data packets will be either dropped or compromised.

7) False Destination Sequence Attack:
Both AODV and DSDV employ destination sequence to identify the freshness of routing information. When multiple routes are unoccupied , the source host always chooses the one with the largest sequence number. By assigning a large false destination sequence in the routing update packets or RREP, the attacker's reply can easily beat other replies and attracts the data traffic. Even worse, the deceived hosts will propagate in good faith the false route to other hosts, thus strengthening the impacts of the attack.

4. Intrusion Detection System

Intrusion Detection is divided into three categories
(a) anomaly-based detection (b) misuse-based detection
(c) hybrid-based detection shown in below figure.

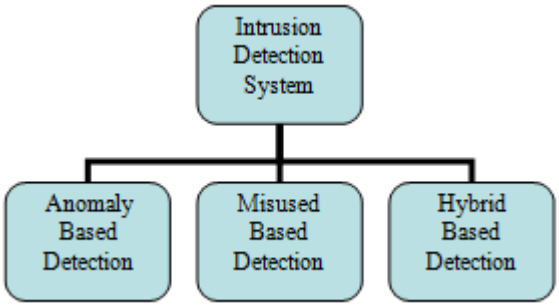

Figure 3: Intrusion Detection System

A. Anomaly-Based Detection
Anomaly-based detection, the key to the application of anomaly detection methods to the field known as threat consists in a simple but critical hypothesis. Hence, anomaly detection has the capability of detecting new types of intrusions and need list of profile data as a normal data, builds model of normal behaviour and automatically detect any violation of it can generate alarm. In anomaly detection the measure and techniques used are (a) statistical measures, (b) threshold detection, and (c) other technology (i.e. data mining, neural network, genetic algorithm and immune system model .In 2010 Wu and Banzhaf said that , anomaly detection searches for intrusive activities by comparing network traffic to those established acceptable normal usage patterns learned from training data, and refers from work, they divided three classifications of the anomaly detection techniques according to the nature of the processing, such as (a) statistic based, (b) knowledge based, and machine learning based. Advantage this approach is ability to detect novel attacks for which signatures have not been defined yet. Unfortunately, this approach produces many false alarms and dally time consuming for research intensive to obtain update accurate and comprehensive profiles of normal behaviour. This means, it requires a large set of training data with consist network environment system log.

B. Misuse-Based Detection:
Misuse detection identifies intrusions by matching observed data with pre-defined description of intrusive behaviour. It find threat by examining the network traffic in search of direct matches to known pattern of packet. Disadvantage of this approach is that it can only detect intrusion that match a previously defined rule, the set of signature require to be constantly update manually to known the new threat. This method can be highly accurate to increasingly precision identify known attack and their variations. Misuse based produce low false alarm.

C. Hybrid-Based Detection:
This section includes the design of hybrid intrusion prevention approach, and describe its basic concepts from previously research work. More recent research explored the deployment of hybrid intrusion detection and prevention to enhancement network security there are some hybrid approaches have been proposal to combine this advantage of both misuse-based and anomaly-based. Both systems have advantages and disadvantages. They need for the solution to overcome security violation was recognizes by researcher to provide system, by combining currently approaches.

Intrusion Detection System of Hybrid structure separates the whole MANET into multiple IDS clusters; and the intrusion detection activity is executes by cluster head. Hybrid structure of IDS system has excellent network extensibility and little network control overhead, which can realize distributed intrusion detection and is appropriate for network characteristics of the MANET. The host IDS can effectively distinguish and report information of attacks in the system.

5. Intrusion Prevention System

IPS design is to enhance data processing ability, intelligent, accurate of itself. Features of IPS are as follows

Signatures Action
- Recognize attack pattern.
- Blocking & response action.
- Stateful pattern matching.
- Protocol decode-based analysis.

Licensed Under Creative Commons Attribution CC BY

- Heuristic-based analysis.

Activity
- Reactive response security solution.
- Early Detection, proactive technique, early prevents the attack, when an attack is identified then blocks the offending data.

Component
- Can be detecting new signatures or behaviour attack.
- Handling alert to trigger false positive or false negative alarm.

Blocking future traffic
Have the capability to chunk and can apply policy at perimeter router or firewall.

Event Response
- Have mechanism allow, block, log, and report.
- Integrated mechanism threat management to security operator

Sensor
- Enable to integrate with other platform.
- Have the ability to integrate with heterogeneous sensor.

Hybrid Intrusion Prevention System

More recent research explored the deployment of hybrid intrusion prevention to enhancement network security their performed work have been proposed to combine this advantage of both misuse-based and anomaly-based. In 2000, A. Seleznyov and S. Puuronen [5], proposed a basis beginning of hybrid intrusion research work, they introduce the earliest method of hybrid, their present architecture of a hybrid intrusion prevention based on real time user recognition. They combines anomaly and misuse based approach. This approach is adapted and implications to other subsequent researchers. With respect to previously proposed work they clearly describe review algorithm approach, such as fuzzy logic, artificial neural networks, evolutionary computation and artificial immune system. Thus, propose hybrid detection system model by combining with neural network IDS and immune system. The idea of this work is a more accurate detection rate of immune system and the powerful learning ability of neural networks.

6. IPS vs IDS

Deciding between intrusion detection systems (IDS) and intrusion prevention systems (IPS) is a particularly challenging and time consuming task for most security pros. Both systems provide similar benefits. They sit in line between two networks and control the traffic going through them. IPS is the way they handle network traffic. IPS accepts all the requests except those whose contents seem to be malicious and threatening to the system. IPS is control device . If an IPS acts as a control tool, then IDS acts as a visibility tool. Intrusion Detection Systems sit off to the side of the network, controlling and observing traffic at many different points, and gives visibility into the security posture of the network. A good analogy is to compare IDS with a protocol analyser which is a tool that a network engineer uses to look deep into the network and see what is happening. An ID is a "protocol analyser" for the security engineer. The IDS goes deep into the network and sees what is happening from the security point of view. From their definitions itself, we can say that IPS starts functioning at the point where IDS stops. IDS can only detect an error, but IPS not only detect it, but also rectify the incurred problem.

Table 1: Comparison HIDS and HIPS

Parameters	Intrusion Prevention System	Intrusion Detection System
Placement In Network Infrastructure	Part of the direct line of communication	Outside direct line of communication
System Type	Active and, or Passive	Passive
Detection Mechanism	1) Statistical Anomaly-based Detection 2) Signature Detection: • Exploit-facing signatures • Vulnerability-facing signatures	1.Signature Detection: -Exploit-facing signatures

7. Conclusion

Many technologies are there in the market to help companies fight the inevitable network and system attack in MANET. But IPS and IDS technologies are only two of many resources that can be deployed to increase visibility and control within a corporate computing environment. So, we have compare and contract both IDS and IPS in MANET based on some parameters shown in table 1 to find which one is better and found that IDS are to provide a foundation of technology that meets the need of tracking, identifying network attacks to which detect through logs of IDS systems and prevent an action through IPS systems.

References

[1] Adnan Nadeem And Michael P. Howarth ,"A Survey Of MANET Intrusion Detection & Prevention Approaches For Network Layer Attacks," IEEE Communications Tutorials and Surveys ,Volume 15, No. 4, Fourth Quarter 2013.
[2] Nilotpal Chakraborty," Intrusion Detection System And Intrusion Prevention System: A Comparative Study," International Journal Of Computing And Business Research, Volume 4 Issue 2 May 2013.
[3] Prof Dr D N Chaudhari , Prof S V Athawale ,"IPS For Wireless Lans At Layer 3," International Journal Of Advanced Research In Computer Science And Software Engineering, Volume 3, Issue 9, September 2013.
[4] Kamarulnizam Abu Bakar, Abdul Hanan Abdullah, Ala' Yaseen Ibrahim Shakhatreh Mohd. Yazid Idris, Deris Stiawan, "Intrusion Prevention System: A Survey," Journal Of Theoretical & Applied Information Technology 15 June 2012. Vol. 40 No.1 © 2005 – 2012.
[5] Deris Stiawan, Abdul Hanan Abdullah, Mohd. Yazid Idris ,"Characterizing Network Intrusion Prevention System," International Journal of Computer Applications (0975 – 8887) Vol. 14– No.1, January 2011.

Licensed Under Creative Commons Attribution CC BY

[6] Norbik Bashah Idris, Bharanidharan Shanmugam, "Hybrid Intrusion Detection Systems Using Fuzzy Logic," www.Intechopen.Com.
[7] Sampada Chavan, Khusbu Shah, Neha Dave And Sugata Sanyal, Sanghamitra Mukherjee , Ajith Abraham ,"Adaptive Neuro-Fuzzy Intrusion Detection Systems," The International Conference On Information Technology: Coding And Computing (ITCC'04) 0-7695-2108-8/04 © 2004 IEEE.
[8] Manjeet Singh, Gaganpreet Kaur, "A Surveys of Attacks in MANET," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.
[9] Pawan Kumar, Gagandeep, Aashima," Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review," International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

Licensed Under Creative Commons Attribution CC BY