# LITERATURE SURVEY ON IDS IN MOBILE AD HOC NETWORK

**Ganesh J. Solanke, Prof. Chandre P.R.**

*Abstract*— A Mobile Ad hoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. But this MANET is too much vulnerable to attack so there is need to implement Intrusion detection system (IDS) in this network. In this paper, we will study different IDS used in MANET.

***Index Terms*—IDS, MANET, wireless network.**

## INTRODUCTION

### A Mobile Ad hoc Network

A Mobile Ad hoc Network is a collection of different co-operating mobile nodes. In a MANET do not have a fixed infrastructure to which you could connect. Because certain infrastructure components as routers can move along with the nodes, there is nothing you can rely on. So nodes are connecting spontaneously with each other in order to form a network .There is even the possibility that no fixed infrastructure is available so that the nodes must do tasks like routing and address management on their own. Because of the attributes described above there arise some defining characteristics of MANETs. These networks are bandwidth constrained, because wireless links still have a lower capacity than wired links. Furthermore you have to take care of the energy management of all components. These networks are used in environments that usually have no energy supplier. Because of this the nodes have to rely on their batteries which rules out CPU-expensive routing algorithms or other complex activities. Last but not least, MANETs have highly dynamic topologies because of the movement of the nodes. Mobile ad hoc networks are also known as infrastructure less networks. These types of networks do not have fixed router, every node in this network can work like a router. All nodes present in the network are accomplished of movement and they can communicate or connect with each other dynamically in random order. The responsibilities like organizing and controlling the network are given to the terminals. The whole network is mobile in nature and all the terminals exclusively permitted to move randomly and freely. In this kind of network, few pairs of mobile nodes cannot communicate with each other indirect manner, and they have to rely on some intermediate terminals so as to transfer messages to the intended destinations. These type of networks are often called as multi-hop or store and forward networks. Every node present in this network can work like a router, which performs, discovering and maintaining routes to the other nodes present in the network. The nodes may be positioned in or on different vehicles like trucks, cars or on air-planes, ships or possibly even on the body of persons. These are very small devices. These ad hoc networks are used for different purposed like disaster recovery, rescuing operations, battle field interactions in between soldiers where wired network is not existing. It can give a possible ways for the ground communications and access of information [2].

Main facts of MANETs:

- Facts
  - Mobile nodes
  - Dynamic topology
  - No fixed infrastructure
  - Bandwidth and CPU constraints
  - Limited battery power

- Threats
  - Easy faking of identity
  - Battery exhaustion
  - falsifying routes
  - Selfish and malicious nodes
  - rely on cooperation

- Difficulties
  - Limited battery capacity
  - Low false positive rate
  - Interoperability
  - Limited bandwidth
  - Dynamisms and mobility
  - Event correlation

### Intrusion detection System (IDS)

The most important component of the computer security is intrusion detection. The intrusion detection avails an additional layer of defense for computer which can be used after physical, authentication and access control [1]. A mobile ad hoc network is a combination of wireless mobile hosts which are forming a dynamic network infrastructure without any use of standard infrastructure or any centralized administration. The flexibility in the parameters like space and time brings new challenges towards the infrastructure security. The mobile nature of the nodes produces new vulnerabilities because of the open medium, continuous and dynamic changes in the network topology, also the lack of centralized monitoring and managerial points and lots of



ISSN: 2278 – 7798 

proven security procedures turn out to be ineffective. Because of these reasons the conventional way of securing wired or wireless networks with the help of firewalls and encryption techniques is not that much sufficient. Military, University campuses and conference settings uses this kind of network because it is the easy way of collaboration and efficient communication which is having no need of costly network infrastructure. According to [3], IDS is a (software-) system, which monitors events in order to detect incidents. In this context, an incident is a violation to the security policy of the system. The software automates the intrusion detection process. An important component of IDS is the logging facility, which is used to analyze the events or even to detect unusual activity by the user. When an IDS is capable of preventing attacks, it is often called IDPS (intrusion detection and prevention system) [4], but mostly IDS is used as a generalization of both functionalities. An IDS uses three main functions. First of all, it records information about what is happening in the network. Next, the system will notify the administrator, if something unusual happens or if human consultation is needed. The third component is the report component, which generates assessments of the situation in regularly intervals. These reports are very important for arguing with the management about the security situation of the company. In addition to that, these reports give the administrator a feeling for the situation and are an advice, whether he should be more careful or not. Because of the dynamic topology of ad hoc networks, they do not have a definite boundary, and therefore the mechanism like firewalls cannot be applied to them. Different vulnerabilities in ad hoc network are like:

1. Dynamic topology: Because of continuous changes in the topology, ad hoc networks usually requires well defined routing protocols. The main obstacle is that the misbehaving nodes in the ad hoc network can produce incorrect routing information which is very hard to find. The mobility of the nodes can also create a problem.
2. Absence of infrastructure: Ad hoc networks are not having any predetermined infrastructure which makes the conventional security mechanism of cryptography and certification inapplicable.
3. Vulnerability of nodes: Physical protection of nodes cannot be feasible therefore they can be easily find out and can fall under the control of an attacker.
4. Vulnerability of channels: Message eavesdropping and inoculation of forged messages into the network is quite easy in case of wireless networks without having the actual physical access to network components.

## Literature Survey

There are four main IDS architectures [5], [6], [7] and [8], as follows: First is Standalone IDS; Second is Distributed and collaborative IDS; Third is Hierarchical IDS and Fourth is Mobile agent IDS; based on these architectures we have found the different detection systems (IDS) during the literature survey.

The most favorable IDS architecture for ad hoc network may rely on infrastructure of the network itself. Wireless ad hoc networks can be designed or configured in either multi-layered or flat network infrastructure. In case of flat network infrastructure, all nodes in the network are treated at the equal level and they all can take part in the function of routing. This kind of infrastructure can be suitable for the civilian application, like a classroom or conference. In case the case of multi layered network infrastructure, all nodes in the network are not treated in the equal. Whereas the nodes within transmission range are prearranged into a cluster, and cluster head is to be get elected from them to centralize the routing information for the particular clusters. The cluster head nodes are forming a virtual backbone for the existing network, and according to the protocol, the packets can be relayed in between cluster head nodes by intermediate gateway nodes. This kind of infrastructure is appropriate for the military applications.

### 1. Stand-alone IDS Architecture

In this kind of architecture, for the determination of intrusions, an intrusion detection system is run on each node independently [5]. There is no cooperation among the nodes in the network, because of this every decision made is depend only on the information collected at its own node. Besides, nodes belonging to the same network do not know anything about the nodes which are present in the same network because no alert information is passed in between them. Even though there are some limitations with this architecture like it may be convenient in a network where not all the nodes are able to have IDS with them or IDS installed. This kind of architecture is more appropriate for flat network infrastructure than that for the multi-layered network infrastructure. As the information on each separate node might not be adequate to find intrusions, this type of architecture has not been selected in most of the intrusion detection systems for MANETs.

### 2. Distributed and cooperative Intrusion Detection Systems

As the basic nature of MANETs is distributed and it has need of cooperation of all the other nodes present in the network, [6] have proposed that the intrusion detection system and the response system in MANETs should also have these properties of cooperativeness and they must be distributed. Every node is participating in the process of intrusion detection and response system with the help of an IDS agent running on them [6]. The functionality of an IDS agent is to detect and collect local events and data to find out possible intrusions, along with initiating a response independently. However the other neighboring IDS agents are cooperatively participating in global intrusion detection actions when evidence is full of loopholes. As compared to the stand alone IDS architecture, this distributed and cooperative IDS is more appropriate for network infrastructure and not for the multi layered infrastructure.

### 3. Hierarchical Intrusion Detection Systems

Hierarchical IDS architectures [7] enlarge the distributed and cooperative IDS architectures and have been projected for the multilayered network infrastructures where the existing network is get divided into the number of clusters. The cluster head in each particular cluster have more work than that of the



ISSN: 2278 – 7798 

other members of the clusters, like routing of packets across the clusters. Because of these duties, these cluster heads works like control points which are very much resemble with switches, routers or gateways used in wired networks. Similar concept of multilayered infrastructure is claimed to intrusion detection systems where hierarchical IDS architecture is projected. Each and every IDS agent is running on every member of node of the cluster and is responsible locally for that cluster's node means that IDS agent is monitoring and deciding on locally identified intrusions. A cluster head is accountable locally for its node similarly, globally for its cluster, for example, monitoring of the network packets and starting a global response after detection of the network intrusion.

### 4. Mobile Agent for Intrusion Detection Systems

In the several techniques for intrusion detection systems for MANETs a concept of mobile agents has been used in [5]. Due to the capability of the mobile agent to move across the large network, each mobile agent has given only one specific task to perform and thereafter one or more number of mobile agents is distributed into each node in the network. This permits the division of the intrusion detection tasks. There are so many advantages of using mobile agents [9]. Some functions which are assigned to the mobile agents are not assigned to every node, resulting in reducing the consumption of power, which is considered as scarce in ad hoc networks. Mobile agents are providing fault tolerance in the circumstances like if the network is partitioned or some agents are get damaged, they are still able to work. More to this, mobile agents are scalable in large and diverse system environments, as the nature of mobile agents is tend to be independent of platform architectures. However, these systems would need a secure environment or secure module where these mobile agents can be stationed. Furthermore, mobile agents must be able to defend themselves from the secure modules which are on the remote hosts.

## CONCLUSION

In this paper we have summarized the research work that has been done related to the various intrusion detection system in mobile Ad hoc network and their similarity measure or differentiation in functionality. We focused on advantages, disadvantages and key factors which are responsible for providing security mechanism of each existing IDS in MANET

.

.

## REFERENCES

[1] Teresa F. Lunt, "A survey of intrusion detection techniques, "Computers and Security, Elsevier science publishers, 1993.

[2] Victor Govindaswamy, "Recent Position Based Routing Mobile Ad-hoc Network Protocols,"UKSim 13th International Conference, 2011.

[3] Scarf one Karen, Mell Peter, Guide to Intrusion Detection and Prevention Systems (IDPS) - Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-94, February 2007.

[4] Tapan P. Gondaliya1, Maninder Singh, "Intrusion detection System for Attack Prevention in Mobile Ad-hoc Network,"International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.

[5] Tiranuch Anantvalee, Jie Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, 2006.

[6] H.N.Pratihari, "Intrusion Detection System (IDS) for Secure MANETs: A Study,"International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 2, Issue 1, Jan-Feb 2012.

[7] Fattah, Dahalin and Jusoh, "Distributed and Cooperative Hierarchical Intrusion Detection on MANETs, "International Journal of Computer Applications (0975 A ,S 8887) Volume 12 A ,S No.5, December 2010 .

[8] Zhang Y, Lee W, "Intrusion Detection in Wireless Ad Hoc Networks, "In Proc of the 6th International Conference on Mobile Computing and Network (MobiCom): 275-283, 2000.

[9] Wayne A. Jansen, "INTRUSION DETECTIONWITH MOBILE AGENTS, "National Institute of Standards and Technology, 2004.



ISSN: 2278 – 7798 