Journal of Advances in Science and Technology
Vol. 12, Issue No. 25, (Special Issue) December-2016, ISSN 2230-9659

Intrusion Detection Techniques in MANET

Prof. Y. M. Naik[1]*, Laxmi Bandakeri[2], Rajeshwari Tigadi[3]

[1]Asst. Prof., Hirasugar Institute of Technology, Nidasoshi, Belgaum, Karnataka, India

[2]UG Student, Hirasugar Institute of Technology, Nidasoshi, Belgaum, Karnataka, India

[3]UG Student, Hirasugar Institute of Technology, Nidasoshi, Belgaum, Karnataka, India

Abstract – The mobile ad-hoc network (MANET) is a new wireless technology, having features like dynamic topology and self-configuring ability of nodes. The self configuring ability of nodes in MANET made it popular among the critical situation such as military use and emergency recovery. But due to open medium and broad distribution of nodes make MANET vulnerable to different attacks. So to protect MANET from various attacks, it is important to develop an efficient and secure system for MANET. Intrusion means any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. Intrusion Prevention is the primary defense because it is the first step to make the systems secure from attacks by using passwords, biometrics etc. Even if intrusion prevention methods are used, the system may be subjected to some vulnerability. So we need a second wall of defense known as Intrusion Detection Systems (IDSs), to detect and produce responses whenever necessary. In this paper we present a survey of various intrusion detection schemes available for ad hoc networks.

Keywords – Ad-Hoc network, Attacks, Bandwidth, Intrusion, MANET, Security.

----------♦----------

I. INTRODUCTION

There has been quick growth in the field of wireless communications since the previous few years, from aircraft communication to wireless personal area networks. The major advantage of a wireless network is the potential of the node to communicate with another node present in the network, while changing their position. Basically there are two types of systems that have been implemented for wireless network. First, is the fixed infrastructure wireless model, this system consists of a number of mobile nodes and comparatively less, but more powerful base stations that remains fixed. These base nodes are wired using modems and landlines. The communication between a base node and a vehicle node takes place via the wireless medium within its range. This model needs a stable infrastructure. Second, is the Mobile Ad hoc Network (MANET), it has been introduced to overcome the problems associated with wired network and implemented only when it is required.

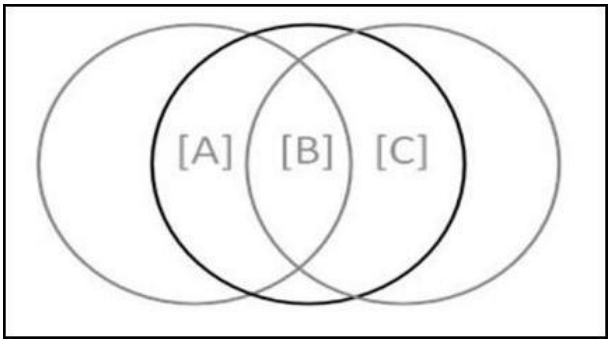

Figure 1: Mobile Ad hoc network with 3 mobile nodes

Although, the communication range of each node is limited to each other's neighbour node, and the nodes that are out of the network's range are routed through intermediate nodes. A MANET is a collection of wireless mobile nodes that are able to communicate with each other without the need of a network infrastructure or any coordinating system. The mobile nodes are independent of any centralized control like base stations or moveable switching centers.

MANET provides infinite mobility and connectivity to the clients. Multiple hops are required for a node to communicate with other node across the network, due to the limited transmission range of wireless

network. In this network, all mobile nodes operates not only as a client only but also works as a router that forwards message packets to the other wireless nodes in the network that may not be present in the same network and not in the transmission network [1]. Figure.1 is an example of ad hoc network consisting of three mobile nodes using wireless system. Nodes A and C are out of range from each other. When transmitting packets from A to C, they use the routing services of host B to forward packets since B is within the transmission range of both of them.

A. Intrusion Detection System

Intrusion detection systems (IDS's) have become most important part in the Security. It is very important element of a complete information security system. Intrusion detection is the process of monitoring computer systems or networks for unauthorized access, activity, or file modification. IDS can also be used to monitor network traffic, so it can detect the system whether it is being targeted by a network attack such as a black hole attack or denial of service attack etc An intrusion detection System can also be defined as a detection system which is of type automated and which is used to alert the available system and security management by generating an alarm at a location where the attack is taken place. If any attack or intrusions have taken place or something different from natural activity happened, IDS come into existence and actions have been taken. IDS achieve detection by continuously monitoring and analyzing the network for abnormal activity, some special attacks and activity which are not same as daily activity [2,3].

B. Types of IDS

IDS can be classified into two types- depending on data collection mechanism and detection techniques. Types of IDS depending on the data collection mechanism includes Network based IDS (NIDS) and Host based IDS (HIDS). Network-based IDS runs on a gateway of a network or on a router and captures and examines all the network traffic that goes through it. It will be useful to detect attack from outside. This is not suitable for MANET since there is no central coordination. A host-based IDS captures local network traffic of a specific host. It is better for detecting attack from inside. While on the other hand, there are mainly three types of IDS that comes under the category of detection techniques [4], are as follows-

a) Anomaly Detection Systems:

In this type of detection system the normal behaviour or daily activities of a user are keeping inside the system. Whenever any activity is performed by the user or attacker, the system compares this activity with the kept data, and then treats that activity based on the evaluation, whether it is an intrusive activity or not, and respond to the system.

b) Misuse Detection Systems:

In the misuse detection system, it holds some well known attack's pattern and their signature. Whenever any activity is performed, it compares this activity with stored pattern or signature and if any match is found then it treated as an intrusive activity. We can take virus detection system as an example of this type. But the main drawback of this system is that it can't identify new types of attack [2].

c) Specification-Based Detection System:

In this type of system it defines a set of rules that describe the procedure of a program or protocol. Whenever any activity is performed, it checks the execution of that activity with defined set of rules.

II. IDS IN MANET

Intrusion are the set of actions that attempt to modify the integrity, confidentiality or availability, and Intrusion Detection System (IDS) is a system or software application that monitors network traffic, and if any suspicious activity is found then it alerts the system or network administrator. [5]. Many intrusion detection systems have been proposed for wired network where all traffic goes through the switches, routers or gateway so that IDS can be easily implemented on these devices. While on the other hand MANET does not have all such devices and any user can access it because of its open medium. Hence current IDS technique on wired network cannot be implemented directly on MANET. There are mainly three types of IDS techniques [6] that can be applied on MANET-

A. Stand Alone Intrusion Detection System:

In this system, an intrusion detection system run's independently on individual node to determine intrusions. All decision taken about a particular activity is depend only on information gathered at its own node, because there is no collaboration among nodes in the network. Therefore, no information is transferred. Even, a node in the same network does not have any information about the other nodes in the network as no alert information is transferred. This model is not efficient because of its limitations, it may be effectively applicable in a network where all nodes already have an IDS installed. This system is also suitable for single layer network as compared to multi-layered network infrastructure. Because the available information on any single node is not sufficient to detect intrusions, this system has not been selected as IDS for MANETs.

B. Distributed and Cooperative Intrusion Detection System

In this architecture, every node has an IDS agent which detects intrusions locally and collaborates with neighbouring nodes for global detection whenever

available evidence is indeterminate and a broader search is required. Whenever the intrusion is captured, an IDS agent can either issue a local response (*e.g.* alerting the local user) or a global response. Each node participates in intrusion detection method and response as having an IDS agent running on them.

The responsibility of an IDS agent is to detect and collect local information and data to identify any attack if there is any attack in the network, and also take a response independently. However, neighbouring IDS agents also cooperates in global intrusion detection when the evidence is inconclusive. Like stand-alone IDS, this system is also more suitable for flat network system, not for the multi-layer system.

C. Hierarchical Intrusion Detection System:

Hierarchical IDS system enlarges the functions of distributed and cooperative IDS system and has been implemented for multi-layer network infrastructures where the network is divided into different small networks known as clusters. Each cluster head usually have more functionality as compared to other members in the cluster, like transmitting the data packets into other cluster. So, we can say that these cluster heads, in some way, perform their working as a central point's which are similar to wired network's controlling devices like routers, switches or gateway.

III. SECURITY ISSUES IN MANET

Security always plays a vital role to identify various types of attacks, security threats and different vulnerabilities present in a system. Vulnerability could be a weakness in security system of any network. A particular system may be prone to unauthorized access to manipulate data because the system does not verifies a user's authenticity before permitting it to access into the network. Wireless ad hoc network like MANET is more vulnerable than wired network. Some of the major issues [7] regarding vulnerabilities in mobile ad hoc network are as follows:-

A. Lack of Centralized Management:

There is not any concept of centralized coordinating system in the mobile ad hoc network. Because of the absence of central management system it is very tough task to detect attacks present in the network, since it is not easy to observe the traffic in a movable and very big ad hoc network. Lack of centralized coordinating system may break trust among nodes in the network.

B. Resource Availability:

Availability of resources is a big issue in MANET. Establishing secure communication path in such dynamic network and protect the network from various attacks, ends up to the development of different security approaches and systems. Cooperative ad hoc network always permit development of self organized security systems.

C. Scalability:

Because of the moving nature of nodes, era of ad hoc network changes all the time. Therefore scalability is an important issue regarding security of ad hoc network. Hence security system should be able to manage a large scale network as well as small ones.

D. Cooperativeness:

Some routing algorithm for MANET like AODV normally assumes that nodes are cooperative in nature and non-attacker. As a result an attacker node may become main routing agent very easily and manipulate network functions as not following the protocol rules.

E. Dynamic Topology:

Dynamic nature and movable nodes relationship can break the trust between nodes. The trust of a node can also be disturbed if few nodes are detected as agreed. This dynamic or changeable nature can be better protected with distributed and cooperative security systems.

F. Limited Power Supply:

The power supply for any node in mobile ad hoc network is limited, which causes many problems. A node in mobile ad hoc network could behave in a selfish manner once it's realized that there is limited power supply.

IV. ATTACKS IN MANET

Karpijoki [8] and Lundberg [9] presented few attacks that can be easily attacked mobile ad hoc network. Mainly there are two types of attack present in ad hoc network are-Active and Passive attacks. A passive attack never disturb or manipulate the functions of a routing protocol, but it only try to get the valuable information by just looking and analyzing the network traffic, which makes user complex to detect it. On the other hand an active attack is an attempt to unauthorized access and manipulates data, gain authentication, or obtain accessibility by injecting wrong packets into the system. Active attack can also be divided into two types- External attacks and Internal attacks. An external attack is one that is produced by the nodes that is not from the same network, while an internal attack is done by the nodes that belong to the same network. As compared to external attack, internal attacks are more difficult to detect, because the attacker nodes already belong to

the same network as authorized parties. Therefore, to protect the system from these types of attack we need the principals of network security. There are some major active attacks [8,9] presented, that can be easily performed in mobile ad hoc network-

A. Black Hole Attack:

A black hole node exploits a routing protocol. In black hole attack, the attacker node may or may not be authorized in the network i.e. it may be authorized in some other network. When the attacker node receives a route request packet (RREQ) from a neighbouring node it immediately sends route reply (RREP) as having a valid route and a shortest path to the required destination even though the route is fake thus creating confusion. In this way the attacker node attacks all the route requests. Thus the information packets being received at the attacker node are either being dropped or sent to network where the attacker node is authorized, without informing the source node that the data did not reach its required destination.

B. Wormhole Attack:

The most powerful attack now a day's present in the ad hoc network is wormhole attack. This type of attack requires the collaboration of two attacker nodes that take part in the ad hoc network. In this type of attack, an attacker, e.g. node A, captures a specific path traffic at one place of the network and underpasses them to another place in the network, to node B, which shares a personal communication link with node A. Now node B selectively sends channeled traffic back into the network. The nodes that have created connectivity across the routes over the wormhole link are fully under the control of the two collaborated attackers.

C. Denial of Service:

Another type of attack is denial of service, which focus to capture the availability of a particular node or even the functions of the whole ad hoc networks. In the simple wired network, the DoS attacks are performed by inserting some specific network traffic to the goal node so as to consumes the energy of the node and make the services provided by that particular node become unavailable. But, it is not practically possible to implement the normal DoS attacks on the mobile ad hoc networks because of the decentralized nature of the nodes. Besides that, the mobile ad hoc networks are too weak as compared to the wired networks because of the interference-prone radio channel and the limited power supply [10]. In the practice, the attackers mainly use the radio jamming and battery exhaustion methods to implement DoS attacks on the mobile ad hoc networks.

V. CONCLUSION

Ad hoc networks are an increasingly and promising area of research with lots of practical applications. However, MANETs are vulnerable to attacks, due to their dynamically changing topology, absence of centralized infrastructures and open medium of communication. Due to this vulnerability, intrusion prevention methods such as authentication and encryption are not able to eliminate the attacks, it only reduces the attacks. Intrusion detection system (IDS) is one of the most active fields of research in MANET, many author has proposed their work on IDS using different techniques. In 2014 Sumit et al [12] defined a new IDS based on effective k-means algorithm. This technique detects malicious node easily because it checks every node individualy, but in this system overhead would be increased once the number of nodes increases. In the same year Indirani and Selvakumar [14] approaches a new system- A swarm-based efficient distributed intrusion detection system for mobile ad hoc networks (MANET). It has some extra advantages like it reduces packet drop ratio and energy consumption is less because the selection of active nodes depende on their residual energy. This system also has the same problem like if the network size grows, the packet drop ratio may increased.

REFERENCES

Pooja Jaiswal and D.Rakesh Kumar. Prevention of Black Hole Attack in MANET. IRACST– International Journal of Computer Networks and Wireless Communications (IJCNWC); ISSN; 2012; p. 2250-3501I.

Neethu B. Classification of intrusion detection dataset using machine learning approaches. International Journal of Electronics and Computer Science Engineering; 2012; p. 1044-1051.

Shailesh Kumar Gaikwad, Prof. Vijay Shah, Yogendra Kumar Jain. A Secure Network Detection System against Noisy Unlabeled Data. International Journal of Computer Applications, 2010. 9(9).

Mishra A., K. Nadkarni and A. Patcha. Intrusion detection in wireless ad hoc networks. Wireless Communications; IEEE; 2004. 11(1): p. 48-60 %@ 1536-1284.

BalaGanesh M. and M.M. Faisal. Enhance the Security Level of MANET's Using Digital Signature. IEEE Transactions on Networking, 2004. Electronic Publication: Digital Object Identifiers (DOIs):

Tiranuch Anantvalee, Jie Wu A survey on intrusion detection in mobile ad hoc networks, in Wireless Network Security. 2007; Springer; p. 159-180 %@ 0387280405.

Priyanka Goyal., Sahil Batra, and Ajit Singh. A literature review of security attack in mobile

ad-hoc networks. International Journal of Computer Applications; 2010; 9(12): 11-15.

Vesa Kärpijoki. Security in ad hoc networks. 2000.

Janne Lundberg. Routing security in ad hoc networks. Helsinki University of Technology, http://citeseer.nj.nec. com/400961. html, 2000.

Wenjia Li and Anupam Joshi, Security issues in mobile ad hoc networks-a survey. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, 2008: p. 1-23.

Anderson, J.P., Computer security threat monitoring and surveillance. 1980, Technical report, James P. Anderson Company, Fort Washington, Pennsylvania.

Sumit, S., D. Mitra, and D. Gupta. Proposed Intrusion Detection on ZRP based MANET by effective k-means clustering method of data mining. 2014. IEEE.

Indirani, G. and K. Selvakumar, A swarm-based efficient distributed intrusion detection system for mobile ad hoc networks (MANET). International Journal of Parallel, Emergent and Distributed Systems, 2014. 29(1): p. 90-103 %@ 1744-5760.

Yogita B. Bhavsar, Kalyani C.Waghmare, Intrusion Detection System Using Data Mining Technique: Support Vector Machine. International Journal of Emerging Technology and Advanced Engineering, 2013. 3(3): p. 581-586.

Mohit Soni, et al. A Survey on Intrusion Detection Techniques in MANET. 2015 International Conference on Computational Intelligence and Communication Networks

Corresponding Author

Prof. Y. M. Naik*

Asst. Prof., Hirasugar Institute of Technology, Nidasoshi, Belgaum, Karnataka, India

E-Mail – ymnaik.cse@hsit.ac.in