International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 3 Issue 6 June 2016

A Survey on Intrusion Detection Techniques in MANET

Sarita[1], Shubha Dubey [2]
Department of Computer Science and Engineering,
Radharaman Institute of Research and Technology, Bhopal [1, 2]
sarita.narwaria93@gmail.com[1]

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 article we present a survey of various intrusion detection schemes available for ad hoc networks. We have also described some of the basic attacks present in ad hoc network and discussed their available solution.*

Keywords: *MANET, IDS , Network Security, Attack, Active IDS, Passive IDS.*

1. 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.

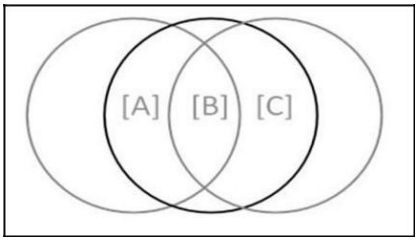

Figure 1: Mobile Ad hoc network with 3 mobile nodes

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 range of each other. In an ad hoc routing protocol each node participates such that multiple hop paths are discovered to other nodes through the 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].

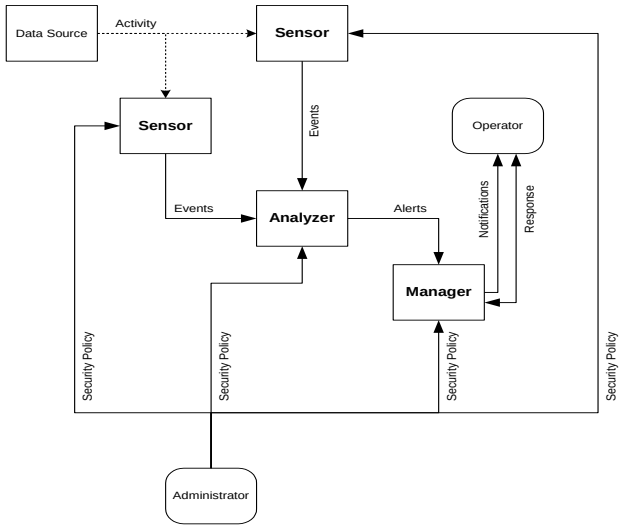

Figure 2 : General IDS Model

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.

2. 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. The concept of multi-layering is applied to intrusion detection systems where hierarchical IDS are proposed. Each IDS agent run's on particular member node and is responsible for its node, i.e. monitoring and deciding on locally detected intrusions. A cluster head is responsible locally for its node as well as globally for its cluster, such as monitoring network traffic and announcing a global response when network intrusion is detected.

3. 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 bedisturbed 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.

4. 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.

5. RELATED WORK

In the intrusion hand side, the attacker must realize the routing protocol mechanism to fake the network, while in the security hand side; the researcher must understand the routing protocol mechanism to protect the network as well. This means that the attacker applies the same type of attack on different protocols using different ways; and hence the researchers use different types of intrusion detection mechanisms on different routing protocols to defend against same attack and/or different types of attacks. In 1980, the concept of intrusion detection began with Anderson's seminar paper [11], in which the author introduced a threat classification model that develops a security monitoring surveillance system based on detecting anomalies in user behaviour.

In 2014, Sumit et al [12] introduced a new technique for intrusion detection. In the proposed IDS, the authors used the Effective K-means algorithm. The centroids of the clusters are constructed using this algorithm. It takes the input as the features of the nodes like total number of RREQ sent by each node or total number of RREP received by each node etc. The desired node features can be picked from the trace file which is obtained on running the simulation in Network Simulator-2. Authors assumed the value of K=2 because, they want to obtain two centroids of highly dense segments. One of these dense segments consists of nodes with normal behaviour and the other consists of abnormal or intrusive behaving nodes. The Effective K-means algorithm runs on a data set which is represented by two centroids of highly dense segments. The IDS is host based and monitors every node in the MANET. If any event is generated by a node, then the selected features of that particular node is fetched. Then the mean square error is calculated and Euclidean distance from the previously constructed centroids is checked. If the result is close to the normal segment centroid, then IDS assumes the node to be normal and allows it to proceed with its normal events. Else, it will not allow the node to proceed with its events. The IDS will simply drop the activity from the queue, which is generated by the node which has been detected as a malicious node [13]. The above process is continued till all the nodes showing intrusive behaviour are detected and separated from the normal nodes. Thus malicious nodes can be separated from the nodes working properly and as a result, our MANET can again get back to its normal functioning i.e. routing packets properly.

In 2014, Indirani and Selvakumar [14] proposed swarm-based efficient distributed IDS for MANET. An artificial intelligence technique that represents the clever activities witnessed in swarms with the help of multi-agent systems (MAS) is termed as swarm intelligence. A MAS is a system that consist multiple interacting intelligent agents. It can be used for solving those problems which are very complex or impracticable for a particular user or a system to solve. In this approach, the swarm intelligence-based ant colony optimization (ACO [15]) is used for selecting the active nodes. In selected route, the parameter to select any node as active node are- maximum trust value, residual bandwidth and energy. This is accomplished to perform the process for detecting intrusion. Every active node checks its neighbour node within its communication range and stores the trust values of all checked nodes. Each active node changes in a timely manner as per the trust parameter. After that active nodes interchange the trust values with its corresponding neighbour active nodes. Once the exchange process done, if any specific node's trust value is less than the minimum threshold, then the node is declared as attacker. After

successfully detecting all attacker nodes, the active node informs to the source node. The source then established a protective mechanism to remove the attacker nodes from the networks. The author used some well defined parameter to select active nodes in the network are- residual energy, bandwidth, coverage and connectivity and trust.

In 2013, Bhavsar and Waghmare [15] proposed a system, in which the author constructed a SVM model for classification. Whenever any intrusive activity happens, SVM detects the intrusion. A classification task involves training set and testing set which consist of objects. Each object in the training set contains one "target value" (class labels: Normal or Attack) and several "attributes" (features).The goal of SVM is to produce a model which predicts target value of data object in the testing set which gives only attributes. To achieve this goal, the author used kernel functions available with SVM. There are 3 major SVM kernel functions [16]:

(I) Gaussian Kernel Function
(II) Polynomial Kernel Function
(III) Sigmoid Kernel Function

In the same year 2013, Abirami et al [17] proposed anIDS which is based on Sentinel Protocol. Sentinel Protocol. It is an efficient approach to detect replica nodes when the IDS inform it by an alert value. Replica detection is based on an interactive time and global information about the node. Whenever two nodes communicate during the packet transmission, each node will exchange some information such as time and global information with another node. This confidential information exchange process should do with all nodes in the network during the transmission. If any node fails to perform this activity, then from the knowledge of the neighbourhood node, it can easily detect the abnormal silence of the replica node. Nodes also exchange the challenge key which contains least and unused index of the node. With this detection scheme the geographical range of replica nodes are detected easily. The author used five simple steps to form the proposed IDS, are- Network formation, Route discovery, Protocol implementation, Route maintenance and Analysis. In the protocol implementation phase, the author believed that the attacker has the potential to agree a few number of nodes, control on the agreed nodes, and build many copies of agreed nodes to enlarge the possibility of attack. The assumption is that the attacker can't compromise enough number of nodes to have a remarkable effect on the network, but it can take full control on the network by inserting many copies of replica node. Hence the motivation of the Sentinel Protocol is to discover and reject all alias nodes with the same identity to make sure the security of the network. If the alias is constructed in an area where the distance between any two alias node exceeds some predefined value and if they do not interchange information with other node during the data transmission process then it's the responsibility of neighbour node to detect Attacker Node (AN) present in the network. The neighbour node implements the Sentinel Protocol.

In 2011, Abdelhaq et al [18] approached a new technique for detecting intrusion in MANET, known as Local Intrusion Detection (LID). The LID secure routing technique allows the diagnosis of the attacker node to be locally; it means that when the suspected intermediate node unicast the RREP message towards the source node, the preceding node to the intermediate node performs the process of detection and not the source node. The detection process is as follow- First, the previous node buffers the RREP packet. Second, it uses a new route to the next hop node and sends FRREQ packet to it. When the previous node receives the FRREP packet from the next hop node, it extracts the information from the FRREP packet and behaves according to following rules:

(i) If the next node has a route to intermediate node and destination node, the previous hop node discard the FRREP, and unicast the RREP to the source node.

(ii) If the next hop has no route to the destination node or the intermediate node or both of them, the previous node discards the buffered RREP and the FRREP as well, at the same time broadcasts the alarm message to announce there is no secured enough route available to the destination node. The last case includes another scenario such as; the case in which the previous hop node does not receive any FRREP from the next hop node. So, here the source node will discover a new route to the destination. This will decrease both routing overhead packets and .end-to-end delay, and increase the network throughput at the same time.

6. 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. Bhavsar and Waghmare [15] introduced a new IDS based on SVM, which uses gausian radial basis function, which improves the attack detection accuracy. But the only disadvantage of this technique is its large training time. Abirami et al [17] proposed an enhanced IDS which uses sentinel protocol to detect replica node easily using predefined time and global information. But this technique is susceptible to node compromise attack. There is one more technique known as Local IDS introduced by Abdelhaq et al [18] that reduces the delay as it performs attacker node detection process locally, but it become unseful once the link to the attacker's previous node is break.

REFERENCES

[1] 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.

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

[3] 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).

[4] 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.

[5] 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):

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

[7] 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.

[8] Vesa Kärpijoki. Security in ad hoc networks. 2000.

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

[10] 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.

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

[12] 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.

[13] Preetee K. Karmore , Smita M. Nirkhi, Detecting Intrusion on AODV based Mobile Ad Hoc Networks by k-means Clustering method of Data Mining. International Journal of Computer Science and Information Technologies, 2011. 2(4): 1774-1779.

[14] 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.

[15] 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.

[16] Panwar, S.S. and Y.P. Raiwani, Data Reduction Technique to analyze NSL-KDD set .Journal Impact Factor, 2014. 5(10): p. 21-31

[17] Abirami, K.R., M.G. Sumithra, and J. Rajasekaran. An enhanced intrusion detection system for routing attacks in MANET. 2013. IEEE.

[18] Abdelhaq, M., et al. A local intrusion detection routing security over MANET network. 2011. IEEE.