Intrusion Detection System in MANET : A Survey

S.Parameswari , G.Michael

Abstract— **MANET is a wireless network in where every node is in mobile state that dynamically self-organizes in arbitrary and temporary network topologies. However owing to open medium they are vulnerable to security issues. Security is one of the most important features in MANET. Prevention techniques alone may not be sufficient to make them secure. Therefore detection should also be added as another defensive mechanism. Intrusion detection systems which are used in traditional wireless networks are not well suited for MANET. In this paper we will first analyze the main vulnerabilities and then discuss the security criteria of the mobile ad hoc network and present the main problems associated with it and also will conduct survey of existing Intrusion Detection Systems and analyze the current security solutions.**

***Index Terms*— Mobile Adhoc network (MANET), Intrusion detection system (IDS), watchdog, Enhanced adaptive acknowledgement (EAACK), SACK, MRA, and Mobile agent**

I. INTRODUCTION

MANET is a self-configuring network formed automatically by a collection of mobile nodes without the help of any fixed infrastructure. Due to the mobility and scalability of mobile nodes wireless networks are most preferred. Each node is equipped with a wireless transmitter and receiver, which allow the node to communicate with other nodes and at the same time each node must act as both a host and a router. One of the main advantages of MANET is it allows data to communicate between different parties and still maintain their mobility. MANET is extensively used in military and emergency situations. Some of the applications of MANETS are used in commercial purposes like ecommerce, business, vehicular service etc and used in industrial application also. So security becomes important thing in MANET. [4]Some of the securities issues present in MANET are dynamic in nature so prior trust relationship between the nodes cannot be derived so it is desirable to adapt changes instantly. MANET consists of hundreds or even thousands of nodes so security mechanisms should be scalable to handle such a large network. Limited energy supply and mobility of the nodes makes the wireless link unreliable which is not consistent for the nodes involved in communication. Because of the movement of the nodes the routing information is changed continuously which leads to lack of incorporation of security features. Now let's discuss about the different types of attack that occurs in MANET.

Different types of attacks that can happen in MANET are active attack and passive attack. [2]In passive attack a malicious node either ignores operations purposely which has to be done by it, or packet containing secret information has been dropped which violates confidentiality. In active attack unwanted packets or information is inserted into the network, deleting or modifying the contents of the packet causes harm to the network operations. The preventive mechanisms to overcome this attack, we can use key based cryptography. Key distribution takes place at the center because central authority, trusted third party, and centralized server are not available in MANET. So the key management has to be distributed to all the nodes. The use of complex encryption algorithms are prevented due to Power and computational limitations. To achieve high survivability, Adhoc network should have a distributed architecture with no central entities. So it is necessary for each pair of adjacent nodes to incorporate in the routing issue which helps us to prevent some kind of potential attacks. On the other hand the detective mechanism which is achieved by this is called intrusion detection system (IDS).

Manuscript received April 04, 2014.

S.parameswari is currently pursuing masters degree program in Computer Science at Bharath University , Chennai, India. Worked as Lecturer at SAMS College of Engineering.

G.Michael is currently working as Assistant Professor at Bharath University , Chennai, India.

II. SURVEY OF INTRUSION DETECTION SYSTEM

IDS can be defined as the method, which helps to identify and report any unauthorized or unapproved activities in network or system. It collects and analyses the activity information to determine any unusual activity. If any misbehavior occurs it will generate an alarm to alert the security administrator. The types of IDS are stand alone IDS in which IDS run on each node independently but cooperation between the nodes does not exist. The second one, Distributive and cooperative IDS is more suitable for flat network infrastructure but not suitable for multilayer .Here every node has an individual IDS agent running on them which is responsible for detecting and collecting local data. It is useful to identify possible intrusion; each node participates in intrusion detection system. The third one, hierarchical IDS have been proposed for multilayered network infrastructure. In hierarchical IDS the network is divided into cluster which in turn each cluster has cluster heads. The cluster heads sometimes act as control points similar to routers, switches, gateway in wired network. They have more responsibility and functionality when compared to other members in cluster.

A. Watchdog:

The Watchdog scheme consists of two parts namely watchdog and path rater. Watchdog method detects misbehaving nodes that aims to improve throughput of network. [1] The watchdog identifies the misbehaving nodes by eavesdropping on the transmission of the next hop. If a node does not send a packet in a specified time it is marked as susespeptable node. If the node behaves susceptible several times determined by a Threshold value, it is marked as misbehaving node. The advantages of watchdog are it is very simple and easy to implement and the power consumption is very less. Next one

is path rater which combines knowledge of misbehaving nodes and routing protocols to avoid the reported nodes in future transmission. Every node is maintaining a rating for each other node it knows about in the network and path metric is calculated by averaging the node ratings in the path. If multiple paths exist to the same destination, the path with the highest safety metric is chosen. The drawbacks of watchdog are receiver collision which takes place when two nodes are trying to send packet at the same time to another node. In order to preserve its own battery resources some nodes purposely limited its transmission power .when a node purposely report other node as misbehavior even if the node forward the packet to destination is known as false misbehavior report. The attackers can easily capture and compromise one or more nodes to achieve this attack.

Fig.1 illustrates how watchdog works.

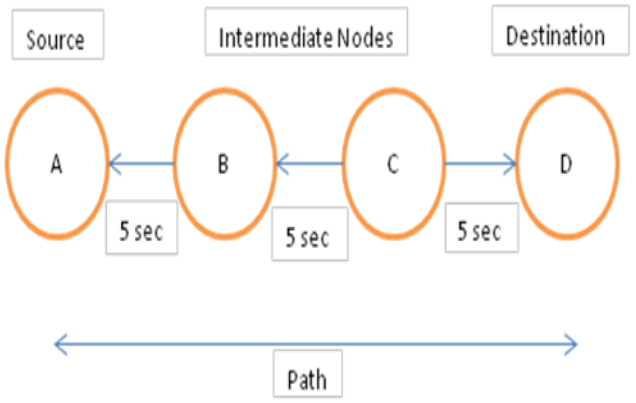

Fig.1. Watch Dog

Let there is path from A to D with intermediate nodes B and C. Consider A is sending packet x to D through the intermediates B, C. Node A cannot transmit the packet directly to Node D, but it can listen in on node B's traffic the same procedure follows node B cannot transmit packet to D but it can listen C's traffic can often say if C transmit the packet to D. Each and every node is maintaining its own buffer of recently sent packets. If a packet remained in the buffer for longer time than a predefined time, it increments a failure counter for the node responsible for forwarding the packet. If the counter exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source intimating that misbehaving node is found.

B. EAACK:

Eaack is ***Hybrid scheme*** which mitigates weaknesses false misbehavior, limited transmission power, receiver collision. [2], [3] it is specially designed for MANET to detect the attackers. Eaack is acknowledgement based scheme which makes use of digital signature. This scheme requires acknowledgement for every packet sent from sender to receiver and all the acknowledgement packets must be digitally signed before sending and verified by the receiver. Eaack consists of three schemes namely ACK, SACK, and MRA.

C. ACK Scheme:

Ack scheme is an end to end acknowledgement scheme. In this scheme when a packet is sent from source to destination, Destination node sends ACK message to Source in reverse order. If Source node does not get ACK packet within specified time Source will assume that there can be misbehaving node and switch to next mode which is explained further. One of the advantages of Ack scheme is routing overhead is reduced when no network misbehavior is found. Fig.2 illustrates the concept of Ack scheme

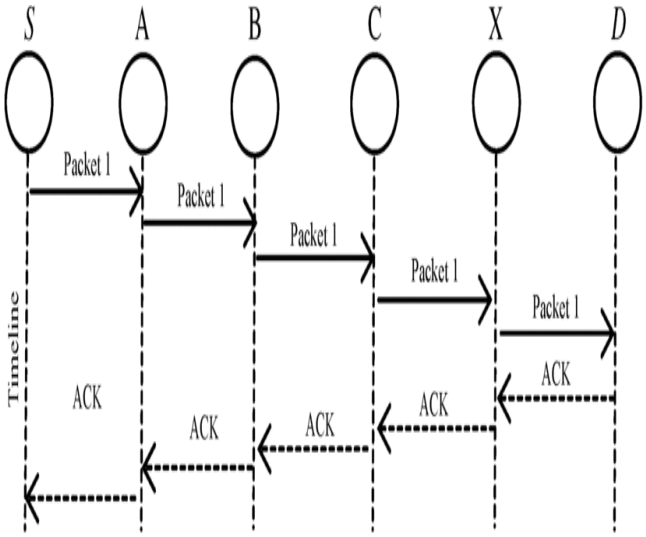

Fig 2.ACK scheme

D. SACK Scheme:

SACK packets have a very similar functionality as the ACK packets on the Medium Access Control (MAC) layer or the TCP layer. [5]The main aim of SACK scheme is to detect the misbehaving node in presence of receiver collision and limited transmission power. In this scheme Data is sent from source to destination if packet transmission is success no issues, Else it will switch to SACK mode by sending SACK data packet to find which is the malicious node in the route. In SACK mode every three consecutive node work as group to detect malicious or misbehaving node in the route and the third node is required to send SACK packet to the first node. If the sender/forwarder of a data packet does not receive a SACK packet within predefined time, nodes are reported as malicious and the misbehavior report is generated and sends to source node. Then the forwarding link is claimed to be misbehaving and the forwarding route is broken. Advantage of SACK scheme are the misbehavior report generated is not trusted immediately by the source node it will switch to next mode to confirm the misbehavior report which is explained further. The concept of SACK is explained with the below example shown in fig.3

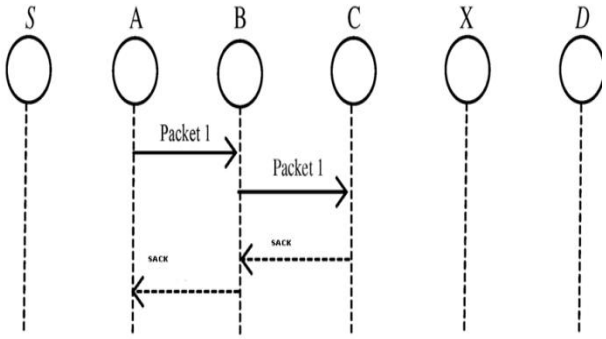

Fig 3.SACK scheme

In the above figure consider A, B and C are the three consecutive nodes in the network. Source sends data to destination node through these intermediate nodes A, B, and C. After receiving the data packets, the destination node will send acknowledgement to source node. If A does not receive acknowledgment within specified time A will send misbehavior report to source node indicating B and C are malicious. So receiver collision and limited transmission power is avoided using this scheme.

E. MRA Scheme:

In this scheme which mitigates weaknesses of false misbehavior, limited transmission power, receiver collision. [5]MRA is used to authenticate whether the destination node has received the reported missing packet through a different route. Attackers falsely generate misbehavior report to make innocent nodes as malicious. To verify false Misbehavior Report Analysis (MRA) packet is sent. If destination is already received the packet, we conclude that this is a false misbehavior report. Otherwise, the misbehavior report is trusted and accepted. MRA will send the missing packet through a different route. If there is no alternate path then source node initiates DSR request to generate new path. One of the advantages of MRA scheme is confirmation and authorization of data present in destination is achieved. And the drawback is time complexity is increased.

Fig.4 illustrates the concept of MRA

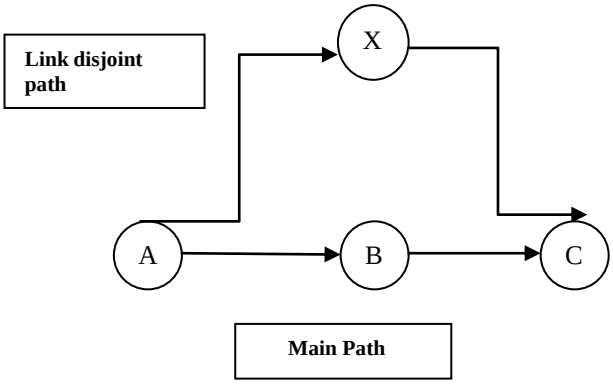

Fig.4. MRA Scheme

The concepts of MRA are explained with the suitable examples. The disadvantages of Eaack are complexity, routing overhead. This is overcome by using mobile agent.

III. MOBILE AGENT

Mobile Agent is distributed and centralized in MANET. [6]A mobile agent controls the communication flow between the nodes and it simplifies the exchange of services and cooperation between nodes. It has ability to move and cover large area of networks. Each mobile agent is allowed to perform only one function which is assigned to them. The mobile agents are used in applications such as network and system administration, process management, monitoring, security etc. Some of the advantages of mobile agent are used to reduce power consumption which is scarce is MANET. It also provides fault tolerance, and allows the mobile agent to work continuously even if the network is partitioned or even some agents are destroyed and it also used to reduce the data load over the network. Mobile agents are independent of platform architectures and must protect themselves from secure modules on remote host.

A. Mobile Agent with Eaack:

In this scheme mobile agent assigns buffer level, TTL and key. Source node transmits data to destination node via intermediate nodes. Before transmitting the data to the destination node we are encrypting the data packets using [8] RSA algorithm which enhances the security level. One of the major advantages of RSA is more secure and convenient. [7] Each and every node in MANET will continuously update its location to the mobile agent; simultaneously each node will send time to live (TTL) message to mobile agent. So the mobile agent will have accurate information about the location of each node. Key is generated by using fast randomized algorithm. If any of the node which drops the packet or not cleared the buffer within the predefined time while travelling in network, the mobile agent who is monitoring the nodes will intimate to source node that some misbehaving node is found. Here the misbehaving node is find out directly with the help of the key. So the time is saved instead of switching to SACK and MRA mode, the data is send to destination node via alternate path. Security is increased by key generation. If the source chooses the same path again to send the data means the key will automatically changed.

Fig.5 illustrates the concept of mobile agent.

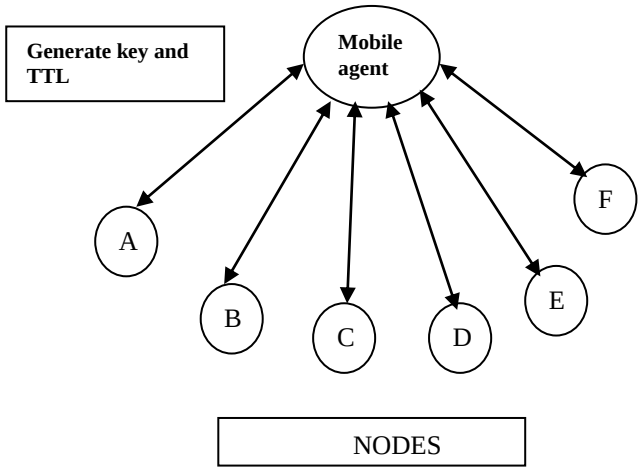

Fig.5 Mobile agent

IV. CONCLUSION:

In this paper we conducted survey for detecting malicious nodes in MANET. This paper presented the overview of various intrusion detection systems like watchdog, EAACK, ACK, SACK, and MRA. This is used to detect the malicious nodes in presence of receiver collision, limited transmission power and false misbehavior report. We analyzed the attacks in the networks and also provided security against those attacks by using efficient intrusion detection system. So we introduced mobile agent with Eaack here the misbehaving node is directly removed from the network. But still there are tradeoffs between each scheme which has to be evaluated further. Further research has to be done to measure the efficiency of mobile agent based IDS.

REFERENCE:

[1]. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-4, September 2011 Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks Dipali Koshti, Supriya Kamoji.

[2]. A Survey on Intrusion Detection System in Mobile Adhoc Networks Arockia Rubi.S1, Vairachilai.S2 International Journal of Computer Science and Mobile Computing, Vol.2 Issue. 12, December- 2013, pg. 389-3939.

[3]. IEEETRANSACTIONSONINDUSTRIALELECTRONICS,VOL.60, NO.3,MARCH2013EAACK—ASecureIntrusion-DetectionSystemfo rMANETS ElhadiM.Shakshuki,SeniorMember,IEEE,NanKang,andTarekR.Shel tami,Member,IEEE.

[4]. Security Issues in Mobile Ad Hoc Networks - A Survey Wenjia Li and Anupam Joshi Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County.

[5]. A Survey on Secure Intrusion Detection for Detecting Malicious Attackers in MANETS c.logeshwari and professor n.gugha priya"IRACST – International Journal of Advanced Computing, Engineering and Application (IJACEA), ISSN: 2319-281X, Vol. 2, No. 5, October 2013.

[6]. AsurveyonIntrusionDetectioninMobileAdHocNetworksTiranuchAna ntvaleeWireless/MobileNetworkSecurity Y.Xiao, X.Shen, andD.-Z.Du (Eds.) pp.170-196 c2006Springer.

[7]. A.Mishra,K.Nadkarni,andA.Patcha, "IntrusionDetectioninWirelessAdHocNetworks,"IEEEWirelessCom munications, Vol.11, Issue 1, pp.48-60, February2004.

[8]. AMethodforObtainingDigitalSignaturesandPublic-KeyCryptosystem sR.L.Rivest, A.Shamir, andL.Adleman.

S.parameswari is currently pursuing masters degree program in Computer Science at Bharath University, Chennai, India. Worked as Lecturer at SAMS College of Engineering

G.Michael is currently working as Assistant Professor at Bharath University, Chennai, India.