Malicious Nodes and its defending mechanisms in Wireless Adhoc Network

Madhavi Dhingra
Department of Computer Science and Engineering, Amity University Madhya Pradesh, Maharajpura Dang, Gwalior (MP)-474005
Email: madhavi.dhingra@gmail.com

Abstract-Maintaining Security in the wireless networks is a major concern of issue in todays era. Many approaches are suggested and implemented such as VPN, Personal Area networks and Firewall.But each of the techniques have some or other issues due to which it wont be called as effective and efficient technique. In wireless network, security is not only done within the connections over the network, but its also important to do on the nodes separately. The networks and the nodes must be monitored for the particular set of selected metrics and on the basis of it, further actions can be planned for it. Nodes can behave in malicious manner and disturb the working of the network. This paper covers the vulnerabilities in the wireless ad hoc mobile network due to which malicious nodes effect the network. It also highlights the major preventive mechanisms that have been developed to avoid the malicious nodes.

Index Terms-Malicious Node; Intrusion Detection;Intrusion Prevention;Wireless Mobile Adhoc network

1. INTRODUCTION

Wireless networks are commonly used in all the IT infrastructures for sharing and retrieving useful information. Mobile ad hoc networks play a major role in establishing connected networks. MANET is commonly used and popular as either with or without infrastructure.

Mobile adhoc network is a temporary network that contains multiple number of wireless mobile nodes.MANET uses the multiple node approach to transmit the messages between nodes in the network. Nodes can be the source node, destination node or even an intermediate node that simply transfers the packets to another destination. Nodes can enter and exit the network whenever they want. The structure and organization of the nodes in the network vary from time to time due to mobility of nodes within and outside the network. Each node is responsible for sending the data to other nodes and have their own approach regarding rules and protocols for data transmission. The routes and the routing protocols need to be updated from time to time due to dynamic environment of the network. All nodes in the network share information with each other and cooperate to perform the desired task. This network does not have a central accessing point like the wired networks.

2. NEED OF SECURITY IN AD HOC NETWORK

Mobile ad-hoc networks have few vulnerabilities due to which attackers can easily enter into the network. An attacker take advantage of these weaknesses and violate the security of the network. these vulnerabilities are as follows [1] -

1. Mobility feature of Adhoc network - the nodes in the network are mobile in nature. They can enter and exit the network whenever they wish. This is the biggest problem in the network. This will generate the opportunity for the attacker to enter into the network and have all the information about the network.
2. Open Wireless connection - A wireless connection is fast but less secure than the wired connection. The attacker can easily access the network and take advantage of it.
3. Limited Resource constraints - Nodes of the wireless network have limited amount of resources like bandwidth, battery, etc. Thus intruder can waste these resources after entering the network and make them unavailable for intended users.
4. Dynamic Network Structure - The movement of nodes inside and outside the network makes a dynamic structure of the network. The transmission of packets follow different routes each time a node enter or exit the network. There is no definite static path for it. Thus, an attacker can easily make its way to enter the selected route in order to disturb the network.
5. Scalability - Adhoc network has no limitation on the number of nodes. This feature gives the attacker an advantage tented the network without any restriction.

6. Limited Range - Adhoc network works in limited range, due to which all the nodes must be in that range for doing communication.
7. Quality of Service - A network performance depend on the quality of service provide by it. Malicious node can easily affect this factor by performing several kinds of attacks.

The security principles must be maintained by the networking system to have successful and error free operations. Security is a broad area which encompasses the following major parameters to ensure the working of a particular system[2].

- Confidentiality - All the communications that are done between the different systems in the network must preserve the confidentiality of the messages and the identity of the communicating nodes.
- Integrity - The originality of the message must be secured during transmission of the packets.
- Availability - The message and data must be available to the genuine intended users that require it.
- Authenticity - Only authentic users have access to the system and its resources. The authentication process identifies the validity of the user that wants to gain the access to the resources.
- Non Repudiation - The sender and the destination must not deny the transmission of packets sent by them.

3. NEED OF SECURITY IN AD HOC NETWORK

The Mobile ad hoc networks have two kinds of nodes based on their behaviour [3]-

1. Normal node - A node that performs the task according to the defined protocol and maintains the security of the network is considered as a normal node.
2. Malicious node - A node which violates any of the security principles is known as malicious node. Such node can affect the network adversely thereby degrading the performance of the network. Thus several algorithms have been used for identification and removal of the malicious node. Malicious or susceptible behavior can be of several kinds like packet drop, battery drained, bandwidth consumption, linkage problem, denial of resources, modification of data, insertion of duplicate packets etc.

A normal node maintains and follow all the security principles. Malicious nodes act as normal nodes in the network and violate the security parameters in active or passive manner. Malicious behaviour has several forms which are explained below [1]-

1. A malicious node captures the packet that are transferred in the network and drops it so that it never reaches the original destination.
2. A malicious node can waste the power of the battery by performing unnecessary tasks like holding the network data for long, sending the duplicate data etc.
3. A node can fill the network with abnormal data so that normal data cannot be transferred.
4. A malicious node tries to hold the bandwidth of the network by continuously engaging it and denying the use of the legitimate nodes.
5. A malicious node can disturb the network without giving any authentic details.
6. The malicious node can enter duplicate fake packets so as disturb the network.
7. Any malicious node can intentionally delay the packet before sending it in the network.
8. The linkage between the nodes can be broken which will affect the communication between the nodes.
9. The packet data can be modified by the malicious nodes.
10. The malicious node can forge the existing routes by creating new fake routes so as to send the packets on wrong paths.
11. An attacker node can make the node isolated while making delays in its path so that The source node selects another path to send the packets.
12. A malicious node can store al the information about the transfer of packets for future attack.
13. A malicious node can hack the session between the two genuine nodes thereby stealing the information and disturbing the communication process.

4. ATTACKS DUE TO MALICIOUS NODES

The presence of malicious nodes introduces internal attacks. These internal attacks are type of active attack as they disrupt the message and the network directly.

Misbehaving nodes are difficult to detect as they are also part of the network. These attacks are done at network, transport and application layer of the network. These attacks include [3,4]-

1. Wormhole attack: The malicious node creates a tunnel between the far nodes by creating an illusion that they are neighbouring nodes and thus it affects the choice of the path for data transmission which will not involve honest nodes.

2. Byzantine attack: This attack is done by a compromised node that create attacks by performing certain tasks like creating a loop in the routing, dropping the packets, and sending the packets on non efficient paths over the network. This category of attack is difficult to find out as all the nodes look normal in this kind of network.
3. Resource consumption attack: In this attack, the attacker waste the limited resources of the network so that genuine users cannot utilise it.
4. Manipulation of data: One simple attack is modification of the data which is done by malicious nodes.
5. Grey hole attack: An intruder broadcast the information that it is having shortest distance to the destination which result in rerouting of the path to send the packets. The invalid path will result in unsuccessful transmission of data.
6. Eclipse attack: The malicious node divide the network into multiple partition and monitors the data flowing between the partitions. It can also control the data flowing between the networks.
7. Session attack: The attacker can take over the control of the session once the session authentication is over. The malicious node can obtain the confidential information and use the information for performing other attacks.
8. Jamming attack: The malicious node will jam the network so that the sender cannot send the data packets and the receiver cannot receive the packets. The network is flooded by unnecessary data so as to flood the overall network.
9. Routing attack: Attacks related to routing protocol are routing attacks. These are routing table overflow, routing table poisoning, packet replication, route cache poisoning, rushing attack.

5. DEFENSIVE TECHNIQUES IMPLEMENTED

Many researchers have focused on this problem and invented some mechanisms to deal with the problem.

Vidhya.K has implemented collaborative contact based watchdog technique for identification of he malicious node and isolation of it from the network[6]. The secure route is selected by choosing the normal nodes of the network. This mechanism is an improved version of watchdog technique. In general, the watchdog technique observes the time of sending packets and storing packets and if the former is more than latter then it gives a warning to the network that the respective node is malicious. This technique also does not work for large umber of nodes. The improved version works for larger number of nodes as well as it can match with the movement of the nodes within the network. The problem of false node detection is also solved by this method. Apart from all the advantages, the approach has some limitations like its working process is not that fast at the time of network congestion due to which packets start dropping.

Nidhi Lal has given another technique to improve the watchdog technique by adding the destination sequenced distance vector routing protocol that gives more secure route[7]. It is known as I-watchdog which is helpful in avoiding DoS attack as well as congestion over the network. The process has two phases, First phase involves authenticating the nodes that are sending the updated information of the routes. In second phase, the nodes will analyse the working and events of the other working nodes. If the events were different from the prescribe events, then that node is declared as malicious. The main drawback of this mechanism is that it generates false alarm for malicious nodes and don’t support any other routing protocol other than distance vector routing protocol.

Sruthi R and Vijayakumar have given a trust based mechanism for detection and removal of malicious nodes[8]. This method depends on the calculated value of trust and the reputation value of the nodes and identify the malicious nodes. There are three modules, monitor module, trust module and reputation module. Monitor module collects the information regarding the neighbouring nodes, trust module rate the behaviour of the nodes and reputation module analyse the trust value and reputation value of the nodes and determine the misbehaving nodes. The report of the malicious nodes are sent to the network so as to remove those nodes from the network. The normal reputation value and trust value has been predefined by the system. If any neighbouring node trust value or reputation value comes below the predefined value, then alert is sent for the corresponding node. This approach considers all the aspects of the node but it consume a large amount of time.

Chinthanai Chelvan,K. had proposed EAACK, an intrusion detection system to improve the security of the network by using the watchdog improved version to detect and eliminate the abnormal nodes whenever such report is received[9]. This approach has two modules Secure acknowledgement and misbehaviour report authentication(MRA). Both modules perform their specific responsibility.

The secure acknowledgement (s-ack) approach solves the problem of failing to detect the malicious nodes in case of receiver collision. The network makes the group of three nodes, where third node is responsible for sending the s-ack to the first node, this process ensures the safe network without collision. If the first node dint receive the s-ack until the specified limit of time, then it declare the receiver collision.The MRA part solves the watchdog problem where malicious nodes are not detected due to false acknowledgement report. In this case, the malicious node itself sends the acknowledgement report. The report is checked by the algorithm to verify that the packets sent were received by the genuine destinations. By verifying it, the validity of the acknowledgement report can be determined.

Mamatha S. and A.Damodaran provided the method for detecting and isolating malicious node by using an anomaly based IDS that monitors the node behavior to avoid the occurrence of the attacks[10]. Data transmission quality function is used for identification of normal nodes with malicious nodes. IDS agent is the major module that checks on each node of the network. This agent has four separate modules. The first module data collection module collects the information of each node and computes the quality of data transfer for them in the network. The intrusion detection module takes the information of data collection module and verify it with the standard values, if it does not matches, then the corresponding node is termed as malicious. The voting module will verify whether the malicious node is really malicious or it is falsely detected. This module take the votes of the other nodes which can confirm the misbehaviour. After the node is confirmed as malicious, the last module segregation removes the node from the network.

This mechanism has an advantage of no communication overhead. The drawback is that this approach can only be performed with Adhoc on demand distance vector algorithm due to which it can prevent very few attacks.

Vijayakumar 2015 had given a Reputed packet delivery approach that involved audit misbehaviour detection and monitoring method[11]. The main task of this method was to detect and remove the malicious node from the mobile ad hoc networks. The node behaviour is monitored for each packet transferred over the network. Misbehaviour node's detection and prevention is done within the following three major parts audit monitoring, reputation and route discovery. The system evaluates the reputation among nodes in the network. Each node has its own view over the other node in the network. The first and second hand information are used to evaluate the reputation of each node and then according to the result from the evaluation the node is determined to be the misbehaviour node or a legitimate node. Once misbehaviour node is identified, then enhance the additive increase/multiplicative decrease principle is used to isolate them from active path.

Anitha G. and Hemlatha. M. have used the approach of sending the ID of the malicious nodes to all the existing nodes over the network[12]. This approach helped in intrusion prevention and message authentication in the network.

ThirumalaSelvi.V. and ThomsonFredrik,E.J., have provided an on-demand distributed protocol for determining malicious node in ad hoc network[13]. They have also used AODV routing protocol for security of nodes in the network.

Apart from these, several other intelligent defence mechanisms have also been implemented.

6. DEFENSIVE TECHNIQUES IMPLEMENTED

Mobile Ad-hoc wireless networks has been dealing with several security problems from last few years. One of the major area of research is in identification and removal of malicious nodes. Various techniques have been developed till now which are working on different concepts. Every technique has its own benefits and limitations. This paper has covered various defence techniques for determining the malicious nodes and removing them. There is still lot of scope of research in this area

REFERENCES

[1] Saini Radhika; Khari Manju.(2011): Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network, International journal of computer application, Vol 20, issue 4, pp 18-21.

[2] Jangra1; A. Goel; N. Priyanka; Bhati,K. (2010): Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture, International Journal of Electronics Engineering, pp 189- 196.

[3] Abhay kumar Rai; Rajiv Ranjan Tewari; Saurabh Kant Upadhyay (2010): Different types of attacks on integrated MANET- internet communication, International Journal of computer science and security, vol 4, issue 3, pp 265-275.

[4] Vidhya.S.V.; Deepa A.J(2014): A survey on securing MANETS from malicious behaviour by detection mechanism, International journal of

computer science and information technologies, Vol 5, issue 10, pp 969-977.

[5] Sibomana Fabrice; Dr. E.J.Thomson Fredrik (2017):Detection And Prevention of Malicious Node Based on Node Behaviour in MANET, International Journal of Advanced Research in Computer Science, Vol. 8, No. 9, pp 774-777.

[6] Vidhya. K.; Sundhar. U; Anantharaj. B (2016) :Detection of Node Activity and Selfish & Malicious Behavioural Patterns Using Watch Dog-Chord Algorithm, International journal of emerging technology in computer science and electronics, Vol 23, issue 1, pp 22-30.

[7] Nidhi Lal; Kumar Shishupal; Saxena Aditya; Chaurasiya Km. Vijay (2015): Detection of Malicious Node Behaviour Via I-Watchdog Protocol in Mobile Ad hoc Network With DSDV Routing Scheme, International conference on Advances in Computing, Communication and Control, Vol 49, pp 264-273.

[8] Sruthi R.;Vijayakumar R. (2014): Prevention of MANETS from Malicious Node Attacks, International Journal of Computer Applications, Vol 112, issue 14, pp 23-25.

[9] Chinthanaichelvan K.; Sangeetha T.; Prabakaran V.; Saravanan D. (2014): EAACK-A Secure Intrusion Detection System for MANET", International journal of Innovative Research in Computer and Communication Engineering, Vol 2, issue 4, pp 3860-3866.

[10] Mamatha S.; Damodaram A. (2014): Intrusion Detection System for Mobile Ad hoc Networks Based on the Behaviour of Nodes, International Journal of Grid Distribution Computing, Vol 7, issue 6, pp 241-256.

[11] Vijayakumar. A; Selvamani K; Pradeep Kumar Arya (2015): Reputed Packet Delivery Using Efficient Audit Misbehaviour Detection and Monitoring Method in Mobile Ad hoc Networks, International Conference on intelligent Computer, Communication and Convergence, Vol 48, pp 489-496.

[12] Anitha G; Hemalatha (2014): Intrusion Prevention and Message Authentication protocol(IMAP) Using Region Based Certificate Revocation List Method in Vanet ,International journal of Engineering and Technology, Vol 6, issue 2, pp 663-672.

[13] Thirumalai V. Selvi; Thomson Fredrick E.J (2016) : Secure on Demand Distributed Protocol for Spontaneous Wireless ad hoc network, International Journal of Computer Science and Information Technology & Security, Vol 6, issue 6, pp 21-24.