ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 11, November 2017

Study on Malicious Node in MANET and its Defensive Techniques

[[1] Madhavi Dhingra, [2] Dr. S.C. Jain, [3] R.S. Jadon
[1] [2] Amity University, Madhya Pradesh, [3] MITS, Gwalior

***Abstract:*-- Wireless networks work in either ad-hoc manner or in infrastructure mode. Information security is the most important thing in any kind of wireless network. This security depends majorly on the nodes and the path, through which the information passes on. The concept of malicious nodes came when nodes started showing abnormal behavior in the network. These nodes affect the network performance adversely and thus, security of the network involves identification of such nodes and removal of them. This paper has reviewed the concept of normal and malicious node behavior and the various techniques that have been used for mitigating malicious node attacks.**

***Index Terms*— Security of MANET, Malicious, Node behavior.**

I. INTRODUCTION

Mobile ad-hoc network is a network that makes fast communication between different nodes in the direct manner. All the links of the network are wireless. These kind of wireless networks are totally dependent on the nodes irrespective of any infrastructure depending on a central authority. Due to node dependency, each node is equally important in the network for reliable communication. In MANET, the presence of any malicious node can have a major impact on the entire communication. There are several attacks like Blackhole attack, wormhole attack in which a genuine node behaves as malicious node and affects the performance of the network [1]. There have been many researches for detecting the attacks in the wireless system but regarding identifying and determining the behaviour of node, there are very few researches. Thus it is essential to determine the normal and malicious behaviour of the node. When any node becomes malicious, it violate the security principles triad, availability, confidentiality, integrity and non-repudiation. An attacker can take advantages of these security breaches and further breaches the security information of the network. Further, the attacker can launch all kinds of denial-of-service (DoS) attacks by replaying, reordering or/and dropping packets from time to time, and even by sending fake routing messages. In MANET, the nodes are defined as selfish node, malicious node, etc. The nodes can be faulty either by effect of some kind of attack or intentionally to misuse the network. The effects of malicious node are

1. Packet dropping
2. False routing
3. Reduces network connectivity
4. Isolation of nodes
5. Reduces network performance

The security of the information in the wireless network is most important. The attackers change the behaviour of the nodes in network to collapse and degrade the functionality of the wireless networks.

II. STUDY OF NODE BEHAVIOUR

The section focuses on identifying the node behaviour[2]. A node in the wireless network can behave normally or abnormally. Normal behaviour is determined as - when operations are satisfying the security principles in the network. Malicious behaviour is - when a node violates any of the security principles and either is under attack or performs attack by itself.

The presence of malicious node can perform any of the following:

1. Node starts dropping packets instead of forwarding it.

2. Node can start wasting the energy by repeatedly sending unnecessary data.

3.A malicious node can overload the buffer by fake packets and prevent the network from genuine packets.

4. A malicious node when consumes much high bandwidth, it

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 11, November 2017

can affect the whole network.

5. A malicious node can make enter other attacking nodes in the network without proper authentication.

6. Fake packets are introduced in the network to confuse the genuine recipient.

7. This can stop the communication between two legal entities in the network.

8. A malicious node can tamper the packets and then forward it.

9. Malicious node may perform Denial of Service attack.

10. A malicious node can perform wrong routing due to which all the network communication will get disturbed.

11. Information like the content, location, sequence number can be stolen by the malicious node to use it further for attack.

12. A malicious node can capture the information that is being passed between different nodes and can use that information for further attacks.

There are various malicious routing attacks that affect the routing process of the nodes in the network, these attacks are modification, fabrication, impersonation, black hole, gray hole and rushing attack.

III. LITERATURE SURVEY

Initially, two methods have been used for detection of malicious node [3]. First is watchdog technique that determines the node behaviour by continuously sensing the network for all the communications. This technique is passive and does not directly interfere with the nodes. It can only detect whether the next hop has sent the data. Second is the pathrater technique that instruct nodes not to send their packets across misbehaving nodes.. Two methodologies were used, namely, watchdog and pathrater, to detect and mitigate the effects of the routing misbehaviour due to the malicious nodes in the wireless networks, respectively[4]. Reputation based technique[5] uses the concept of central authority network that maintain the entity of each node by assigning it a value. A positive and negative signal feedback is noted for each node of the network. When ever a node want to send data to other node, it can check the current status of the other node by inquiring central authority. But this approach requires the continuous updation of the values, as well as for large sized distributed networks, it is very difficult for central team to assign and manage the node reputation values. Future reputation values can not be determined prior to sending. Incentive and Eigen Trust Technique is used that is based on incentive and eigen trust. Every node that transmit the packets to others, is charged and compensated when it forwards the packet to other nodes. To decrease the charge, the node can take packets from other nodes also so as to forward it and reduce their own charge. The node with maximum charge will be examined for malicious node, Punishment based technique, another technique is based on intimating the the neighbouring nodes about the presence of malicious nodes. and assigning the reputation values to all the nodes. Also, the best path is defined for routing avoiding the malicious node. This method is also not feasible with large networks as continuous updation of reputation values is required. COOPMAC with ARQ, This method works on Automatic repeat request protocol. It identifies whether the receiver has received the packets successfully , it sends the signal to source to retransmit the packets. This method is used in the MAC layer in wireless networks. One of the major drawback of any malicious node detection or intrusion detection system is determining a legitimate node as malicious node. This is also known as false alarm. The consensus method detects the malicious node and compute the false alarm probability by using maximum cardinality approach. An adaptive acknowledgement technique [6] was proposed to identify the malicious nodes in the wireless sensor networks. The process reduces the overhead of acknowledgement by sending the AACK signal only after the packets has been reached at the final destination. If the sender does not receive the signal within the fixed time interval, it send the packet again. This method has reduced the network overhead and achieved the same throughput. A dual busy tone multiple access technique was used by Haas and Deng [7] to eliminate the exposed and hidden nodes from the network. This technique transmits two tones of narrow bandwidth to inform its neighbours about the signal. Another method was used to study the performance of wireless networks with hidden nodes [8]. The authors showed that the hidden nodes barely affect the network performance in low traffic conditions.

A queuing theory based analysis method was also

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 11, November 2017

presented for computing the performance of wireless networks [9]. They provided an approximate results for linear topology at low load. In wireless networks, CSMA protocol plays an important role regarding transmission of packets. The hidden node problem of CSMA protocol was solved with Busy Tone Multiple Access protocol. In their paper, the analysis of the protocols has been carried out under the assumption that the inter-arrival times of the point process defined by the start times of all the packets plus retransmissions are independent and exponentially distributed, i.e. they follow the Poisson process. Various other active and passive detection methodologies have reduced the hidden node problem in wireless networks by using Request t o S e n d / C l e a r t o S e n d (RT S / C T S) mechanism[10]. But these methods have major drawback of introducing high overhead over the network. Later on, a hybrid approach was also proposed to solve this issue.

IV. SOLUTION TO MALICIOUS NODE PROBLEM

A Misbehaving Node Detection (MIND) mechanism, for identifying misbehaving and malicious nodes must consider the following major considerations[11] :

1. The system must use a specified policy for identifying malicious nodes based on some parameters.

2. The system must be capable of detecting the misbehaving nodes.

3) The system must have capability of recovering from attacks.

4) The system should not overload the network with additional messages or bandwidth consumption.

5) The system must be error free while malicious activities are being performed.
Different Intrusion detection systems are used to determine the malicious behaviour in the network. Each system has considered few parameters to detect the abnormality in the network, these parameters include:

1. Miss - The value depend on the trial of the suspicious node to access the data packets.

2. Hit - The value depends on the authorised node number of access to the data packets.

3. Total Tries - The value depends on the number of packets that are sent over the network.

4. Miss Ratio - Number of misses by total tries.

5. Hit Ratio - Number of hits by total tries.

6. Prt Address - The final destination address specified in the packets.

7. Threshold - This value is the computed value according to the algorithm used in the mechanism.

8. Suspicious nodes - Number of nodes identified as suspicious node.

The performance of the proposed methodology is determined through the following important parameters:

1) Packet delivery ratio: It is defined as the ratio between the numbers of packets correctly received to the total number of packets sent.

2) Latency: It is the time required to receive the packets from the transmitter through the number of nodes.

The different IDS that have been used for detection of malicious node. Each technique have their own benefits and drawbacks[12].

1. Watchdog and Pathrater IDS - This method uses dynamic source routing protocol. It improved the throughput of the network even in the presence of malicious nodes. But it fails to detect misbehaving nodes in case of collisions and limited transmission power. In some cases, the probability of false alarm is also high.

2. Twoack IDS resolves the problem of collusion but the acknowledgement involved at every phase of transmission has added an significant amount of overhead on the network.

3. AACK has reduced this problem and maintained the same throughput while there is still the problem of authenticity in the transmission of packets.

4. EAACK is another technique based on Digital signature algorithm that solves the problems of collision, and false

alarm. But when number of malicious nodes are more, this method produces more burden on the network. Hybrid cryptography technique depending on Blowfish, elliptic curve and Diffie hellman algorithms provide much more security as compared to other schemes.

V. CONCLUSION

Security of information in the any wireless network is the most important. Apart from various attacks, the malicious node attacks are of major concern. This paper has presented the aspect of node behaviour in context of wireless mobile adhoc network. Different kind of node behaviour exhibit different results. Malicious nodes either formed intentionally or unintentionally have an adverse impact on the performance of the network. Different techniques are discussed that have their own mechanism for identification and removal of malicious nodes. Different Intrusion detection systems have been developed to overcome this issue. But more efficient techniques and frameworks are required in this area since the probability of false malicious node detection rate is still high.

REFERENCES

[1] B. Wu et al, ―A Survey of Attacks and Preventions in Mobile Ad Hoc Networks,‖ Wireless/Mobile Network Security, Springer, Vol 17, 2006.

[2] R. Gopal, V. Parthasarathy, A.Mani,“ Techniques toIdentify and Eliminate Malicious Nodes inCooperative Wireless Networks”, IEEE InternationalConference on Computer Communication andInformatics (ICCCI -2013), Jan 2013.

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

[4] . RadhikaSaini and ManjuKhari , “ Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network” International Journal of Computer Applications, Volume 20– No.4, April 2011.

[5]. G.S. Mamatha and Dr. S.C. Sharma, “ Network Layer Attacks and Defense Mechanisms in MANETS- A Survey” International Journal of Computer Applications (0975 – 8887),Volume 9– No.9, November 2010.

[6]. Jaswinder Singh and Ramandeep Kaur, “Towards Security against Malicious Node Attack in Mobile Ad Hoc Network”, IJARCSSE Volume 3, Issue 7, July2013.

[7] S. Dehnie and S. Tomasin, “Detection of selfish nodes in networks using CoopMAC protocol with ARQ," IEEE Trans. Wireless Commun., vol. 9, no. 7, pp. 2328–2337, July 2010.

[8] T. Fahad & R. Askwith, “A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks,” Liverpool John Moores University, 2006.

[9] P.K.Suri, K.Taneja,”Exploring Selfish Trends of Malicious Mobile Devices in MANET,” Journal of Telecommunications, May 2010, Volume 2, Issue 2.

[10] G. Soni and K. Chandrawanshi, “A Novel Defense Scheme Agaisnt Selfish Node Attack in MANET,” International Journal on Computational Sciences & Applications, June 2013,Vol.3, No.3.

[11] John, R. P Haroon,”Selfish Node Isolation & Incentivation using Progressive Thresholds”, International Journal on Network Security, (January 2014)Vol.5, No.1.

[12] M.S.Subbulakshmi, S.J.Mohana, A Survey on Malicious Nodes in Mobile Ad hoc Network, International Journal of Computer Science & Communication Networks,Vol 4(4),137-142