DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5213

ISSN No. 0976-5697

Volume 8, No. 9,November-December 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

DETECTIONAND PREVENTIONOF MALICIOUS NODE BASED ON NODE BEHAVIOUR IN MANET

Sibomana Fabrice
Dept. of Computer Science
KarpagamAcademy of Higher Education
Coimbatore-21, India

Dr.E.J.Thomson Fredrik
Dept. of Computer Applications
Karpagam Academy of Higher Education
Coimbatore-21, India

Abstract: The performance of MANET relies on its security. In order to implement MANET network, security issue has to be taken into consideration. As it has been proved by so many studies, MANET is highly vulnerable to so many kinds of attacks due to its characteristics. MANET performance relies completely on the security provided by the network developer. Many researchers are doing research to overcome the loop holes in the security of MANET by implementing lot of techniques and mechanisms. One of the techniques thatis used by the researchers is to detect and prevent the malicious node which is based on node behaviours. There is no single security mechanism that can fit to all networks due to scalability and effectiveness nature of MANET. The use of encryption and authentication system are not sufficient because they can be broken easily therefore by giving chances to different kinds of attack to penetrate in the network. A second level of defence is imminently needed in order to improve the network performance. This paper reviews recent research studies that use node behaviour analysis to detect and isolate malicious node from the network. The goal of this review paper is to find out which study is more effective than others.

Keywords: MANET,AODV,DSR,OLSR,DSD

I. INTRODUCTION

Mobile ad hoc network is a Wireless network that is formed temporally and consists of a set of mobile node connected by wireless links. Nodes in MANET can only have a limited transmission range (single hop approach). MANET uses multi hop approach to transmit a message from the source of the network to the destination through an intermediate node. Node does not only act as a host but as router as well while forwarding the packets through an intermediate node till to the intended destination. Nodes are free to move, join or leave the network at anytime, anywhere [1] in the network which causes the topology of the network to be dynamic. Due to the change of topology,each and every node in the ad hoc network should have a protocol running on it for discovering and maintaining routes between the nodes.

Every node in the ad hoc network has the same power, authority and commitment with each other. Collaboration and cooperation among all nodes are the key to a better performance in ad hoc network. Unlike wired network, Ad hoc network does not possess a central administration point to manage the network.

II. AD – HOC ROUTING PROTOCOL AND MALICIOUS NODE BEHAVIOURS

This section gives a small detail on the routing protocol in MANET and difference between the normal node behaviour and misbehaviour node.

A. Routing protocols

The routing protocols can be classified into three classes

- Demand driven/reactive
- Table driven/proactive
- Hybrid

Demand driven protocols are the routing protocols that aim to eliminate the work that has done for updating the table and tracking every change in the network and update the table according to the change that happened in the network.

Here are some examples: (AODV) ad hoc on demand distance vector, (DSR) Dynamic Source Routing.

Table driven routing protocols exchange the routing information from time to time to make all the routes available at the time of requirement.Here are some examples for table driven routing protocol: (OLSR) Optimised Link State Routing Protocol, Destination Sequenced Distance Vector routing (DSDV) protocol.

Hybrid routing protocols combinethe features of table driven and demand driven. The network is split into two zones, table driven is used in the zone to maintain routing information and demand routing protocol is used to route packet between the different zones

B. Normal node Vs Misbehaviour node

- Normal node

The security purpose in any network is to maintain the security principles of the network which are confidentiality, availability, integrity, authenticity and non-repudiation [2], if any node in the network manages to maintain all these principles then that node is considered as a normal node.

- Misbehaviour Node

A node is called misbehaviour node when one of the security principles is breached by the nodeand that node has to be detected and removed from the network. The types of some malicious behavioursof a node are packet drop, battery drained, delay of packet, stale packets, link break, message tampering, bandwidth consumption, stealing information,

buffer overflow, malicious node entering, denying from sending message, node not available, session capturing and others[2]

III. ATTACKS IN MANET

Providing security in MANET is very challenging. The initial stage in providing security to MANET is to understand all different kinds of attack thatcan attack MANET. These kinds of attacks can be classified into two classes. They are active and passive attacks that areproposed by Reena Sahoo, 2011 [3].

A. Active Attacks

Active attacks are attacks that are able to penetrate the network and then modify, destroy or fabricate data which is transmitted over the network. These attacks disturb the normal operation of the network. Active attack can be classified into internal and external attacks[4][5]. Internal attacks are those that caused by misbehaviour node, these node are the authorised node in MANET. Due to this reason, these misbehaviour nodes are very difficult to detect. External attacks are those that are created by outside node of a particular network region and these attacks can be prevented by using standard encryption techniques. The active attacks are created in the network layer, transport layer, application layer which are proposed by Abhaykumar*et al* 2010 [4][5].

Wormhole attack: It is a powerful attack, creates a tunnel between two malicious nodes. Attacker receives a packet from one particular location in the network and tunnels them to the other location in the network.

Byzantine attack: A compromised intermediate node or set of compromisedintermediate node works in agreement and create attacks. The attacks are creating routing loop, selectively dropping packets and routing path on the non-optimal paths. This kind of attacks fails to bedetected because the network will be looking like a normal one.

Resource consumption attack: In this attack malicious node tries to consume away the resources of the other nodes present in the network. Resources that can be consumed are battery power, computational power and bandwidth which are only limited in MANET.

Manipulation of data: Malicious node that is presented in between the source and destination node will receive the data packet from a forwarder node. And then it modifies the content of packet and forwards the modified data packets to the next node.

Grey hole attack: An attacker node will broadcast itself as having a very shortest path to any node from the entire mobile node in the network. As the result it will affect the concrete path to destination node

Eclipse attack: The malicious node presents in the network can perform the network partitioning. The attacker nodes monitor and control the data flow between the partitioned networks.

Session attack: This attacker takes control over a session between the two nodes. Since the most authentication processes are carried out only at the start of a session. Once a session between the two is established, the attacker node masquerades as one of the end nodes of the session and hijacks the session.

Jamming attack: Jamming attack is the particular class of DoS attacks. Jamming attack interferes with the legitimate wireless communication by preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets.

Routing attack: All attacks that are fixed on the routing protocol are routing attacks. These are routing table overflow, routing table poisoning, packet replication, route cache poisoning, rushing attack.

B. Passive attack

Passive attack is opposite to active attack because passive attacks do not involve in the operation of the network. Passive attack monitors the data and path regularly. It isalso used to transmit the data packet without altering the content of the data packet. Passive attack will not disturb the data transmission.It is very difficult to detect passive attack. The best way of preventing passive attack in MANET is by using effective encryption technique to encrypt and decrypt the data being transmitted. Examples of passive attack are eavesdropping, traffic analysis and monitoring [5].

IV. LITERATURE REVIEW

In this section, six different recent methods for detecting and preventing malicious nodes are reviewed. All the methods arebased on node's behaviours analysis in MANET.

In[6],VIDHYA.K,*et al*, 2016 introduce an approach called collaborative contact based watchdog to detect and isolate malicious node and selfish node from the network. The isolation is done by choosing a safe route to destination.

Unlike the ordinary watchdog, the approach introduced by K.VIDHYA *et al*, 2016 has an improvement feature in adding the algorithm called chord algorithm. Normal watchdog detects the malicious node by observing the node whether the sending time of the packets is greater that the storing time of the packet and some other node's activities, if so it sends the alarm message in the system then the node is considered as a malicious node. Another drawback of the watchdog approach is that it does not support a very large number of nodes with a high speed movement.

The drawbacks possess by watchdog are solved by adding a chord algorithm that support a large number of nodes and high speed movement and at the top of that the problem of false detection is solved by using chord algorithm alongside with watchdog.

But even though chord algorithm possesses all those features (good result in throughput, packet delivery ration, end to end delay) it alsohas somedisadvantages that it does not take decision easily about node because packet loss can also happen due to the network congestion.

In [7],Nidhi Lal *et al,*2015introduced a mechanism to improve the watchdog which is called as I-watchdog with destination sequenced distance vector routing protocol that provides efficient and secure routing with prevention of denial of service attack as well as detection of congestion in the network background.
The mechanism works in two steps. First step allows the nodes to authenticate the other node that sends the updated routing table information and in the second step nodes measures the activities of the next working node. If the measurements do not match with the predefined value, then the node reports its next working node as the malicious node.
The disadvantage of this approach lies in that it works only on the DSDV [Destination Sequenced Distance Vector] routing protocol and it has a fault alarm.

In [8], Sruthi R and Vijayakumar R, 2015 introduced a trust based approach to detect and eliminate malicious node for the network. The trust mechanism evaluates the trust value along with the reputation score and eliminate malicious from the active path.
The trust has three modules and each has its own specific role

1. Monitor module
2. Trust module
3. Reputation module.

Monitor module is responsible for collecting information about the neighbouring nodes in order to infer their behaviour

Trust module is responsible for rating the behaviour of the node. The evidences are sent periodically when the trust level of a given neighbouring node which is proved to be lower than a predefined value defined as the lowest tolerated trust in the network

Reputation is responsible for assessing the reputation of nodes. Once reputation value and trust value fall below a predefined value,then the node with that value is considered asmalicious nodeandis eliminated from the network by sending an alert message to all nodes

The assumption on this approach is that it provides a strong security but suffer from time consuming

In [9] ChinthanaiChelvan,K., *et al,* 2014introduced an approach called EAACK- A secure intrusion detection system for MANET to improve the security of the watchdog to detect and eliminate malicious node in the case of receiver collision and false misbehaviour report. This EAACK has two parts namely Secure ACK (S-ACK) and Misbehaviour Report Authentication (MRA) and each part perform its specific role.
S-ACK: It is the part that solves watchdog's weakness when it fails to detect malicious node with the presence of receiver collision. The system is to build a group of three consecutive nodes in route and the third node in that route is responsible to send a S-ACK acknowledgment back to the first node that will ensure that no collision happened. If the first node fails to receive S-ACK acknowledgment within a predefined time and has overheard its next hop forwarding the packet to third node. The First node will report to the third node as malicious node.

MRA: The Second part solves watchdog's weakness when it fails to detect malicious node with the presence of false acknowledgment report. A malicious node overheard its next hop forwarding the packet but still report it as a misbehaving node. In this case, the second part of EAACK has MRA scheme that determines whether misbehaviour report is genuine one or false one. When destination node receives a MRA packet, it checks in its local knowledge base and compare if reported missing packet was received, if it is received then the destination node will know that it is a false misbehaviour report and whoever reported that is considered as a malicious node and removed from the network.

In [10],Mamatha S. and A.Damodaran, 2014has proposed the way to detect and isolate malicious node based on the anomaly based intrusion detection system that works by checking the behaviour of the nodes in order to overcome the different kind of attacks.
Data transmission quality function is used as the parameter to distinguish betweenthe misbehavingnode and legitimate node. The main function of this distributed and cooperative approach is performed by the IDS agent that is running on every node in the network. IDS agent running on every node monitors the activities of their neighbours. This IDS agent consists of four modules which are data collection module, intrusion detection module, voting module and intrusion response module that perform their task respectively. Data collection is responsible for collecting all data and calculates data transmission quality for each node in the network, intrusion detection module uses the information collected by the data collection module if the information does not match with the predefined condition set for legitimate mode. And then the node is marked as the misbehaving node but this node will not immediately be perished from the network because it might be the fault detection due to malfunction. The voting module will come in for the approval where the node is accusing another as the misbehaving is required to get the conformation from the other and confirms whether the node is really misbehaving. Segregation module eliminates the misbehaving node based on the outcome from voting module.
The approach overcomes the issue of fault detection in using voting module and there is no communication overhead that finds in the acknowledgment based approach but it has a drawback of protecting against few kind of attack and it can be implemented on AODV only.

In [11] Vijayakumar. A *et al,* 2015introduced an approach called reputed packet delivery using the efficient audit misbehaviour detection and monitoring method in the mobile ad hoc network and their aim is to detect and eliminate misbehaviour node from the packet transmission in multi hop mobile ad hoc network.
Behaviours of the node are simply evaluated based on the per packet basis and this is done without any energy expensive overhearing technique or intensive acknowledgment technique. 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 ownview over the other node in the network. The first and second hand information are used to evaluate thereputation ofeach 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 enhancethe additive increase/multiplicative decrease principle is used to isolate them from active path.

In [12],AnithaG., andHemalatha,M., 2014proposed an intrusion prevention and message authentication protocol for detecting malicious node by sending the ID of this malicious node to all the remaining node in VANET.**In[13],ThirumalaiSelvi,V., and ThomsonFredrik,E.J.,2016** proposed a secure on demand distributed protocol for identifying malicious node in spontaneous adhoc network. They concentrate on routing techniquesusing AdhocOn Demand Distance Vector (AODV) avoiding the malicious nodes for secure transmission Adhoc Network.

VI. CONCLUSION

Detection of Malicious node is a main security issue in MANET because malicious node can disrupt the operation of the network and it paralyses the whole network. Many studies have been conducted proposing different types of technique to detect and prevent the malicious node in mobile ad hoc network. There is not a single security mechanism that can fit in all networks, especially MANET due to its mobility nature, but it is an extremely important to keep this area of research open in order to create the new and powerful technique to detect and prevent different new emerging attacks. The approach proposed by S Manatha,S., and Damodaram,A.,2014 stand out to be the strongest among the approaches which are reviewed, due to the fact that it eliminate the malicious node as well as tackling the issue of fault alarm,false detection and no overhead issues which are usually found in the acknowledgment approach.

VII. REFERENCES

[1] Jayashree.A.Patil, NandiniSidnal " survey – Secure routing Protocols of MANET", International journal of Applied information systems, Vol 5, No 4, (2013), pp 8-15

[2] Radhika Saini and Manju khari, "Defining malicious behaviour of node and its defensive methods in ad hoc network", International journal of computer application, Vol 20, issue 4, (2011), pp 18-21

[3] Reena Sahoo and Dr. P. M. Khilar "Detecting malicious nodes in MANET based on cooperative approach", IJCA, Special issue on "2nd national conference- computing, communication and sensor network,(2011), pp 46-51

[4] Abhaykumar Rai , Rajiv RanjanTewari and Saurabh Kant Upadhyay, "Different types of attacks on integrated MANET- internet communication",International journal of computer science and security,vol 4, issue 3, (2010), pp 265-275

[5] Vidhya.S.V., Deepa A.J, "A survey on securing MANETS from malicious behaviour by detection mechanism", International journal of computer science and information technologies, Vol 5, issue 10,(2014), pp 969-977

[6] Vidhya. K, Sundhar. U, Anantharaj. B "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, (2016 June), pp 22-30

[7] Nidhi Lal, Shishupal Kumar, Aditya Saxena, Vijay Km. Chaurasiya " 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, (2015), pp 264-273

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

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

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

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

[12] Anitha G, Hemalatha " 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, (2014), pp 663-672

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