Scientific Journal Impact Factor (SJIF) : 3.518
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Survey on Detection and Prevention Techniques for Malicious Node in MANET

Mr. Virendra Patil[1] and Mr. Rajendra Patil[2]
[1]*PG Student, SSVPS COE, Dhule, Maharashtra, India*
[2]*Asst. Professor, SSVPS COE, Dhule, Maharashtra, India*

Abstract— Wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. Due to lack of a defined central authority, MANETs are more vulnerable to security attacks and thus security is essential requirement in MANET as compared to the wired network. The nature and structure of MANET makes it attractive to various types of attackers. In this paper the principal focus is on routing and security issues associated with mobile ad hoc networks which are required in order to provide secure communication. On the basis of the nature of attack interaction, the attacks against MANET may be classified into active and passive attacks. In this paper we discuss mobile ad hoc network security issues and there detection techniques. We first analyze the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks, then we discuss the security criteria of the mobile ad hoc network and present the main attack types that exist in it. Finally we compare the current security detection techniques for the mobile ad hoc network.

Keywords— Mobile Ad Hoc Network, Security, Malicious Node, Secure Routing

I. INTRODUCTION

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections. Means, wireless communication there is no require physical network in which used cables. Wireless technologies use the radio frequency for transmission of data, whereas wired technologies use cable. Wireless networks are classified into two categories; Infrastructure networks and Ad Hoc networks as shown in Figure 1.

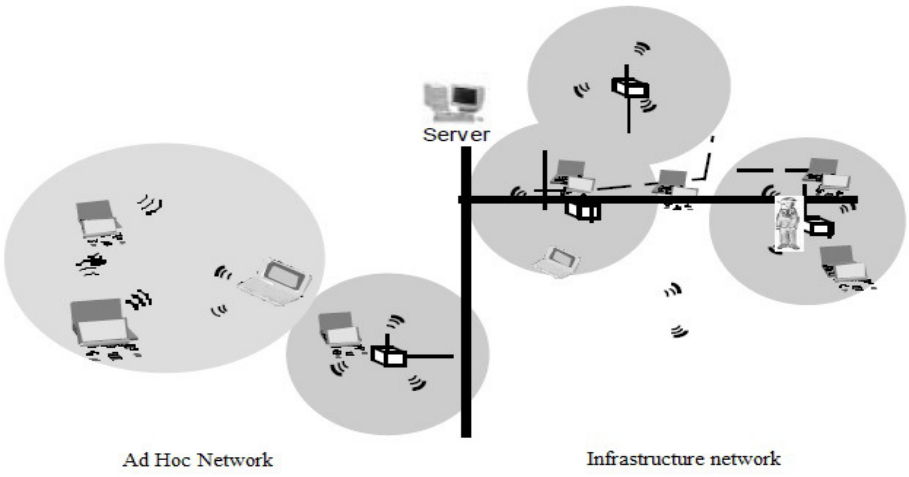

Figure 1 Categories of wireless network

1) Infrastructure networks: An Access Point (AP) represents a central coordinator for all nodes. Any node can be joining the network through AP. In addition, AP organizes the connection between the Basic Set Services (BSSs) so that the route is ready when it is needed. However, one drawback of using an infrastructure network is the large overhead of maintaining the routing tables.
2) Ad Hoc networks: A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks [1]. Ad Hoc networks do not have a certain topology or a central coordination point. Therefore, sending and receiving packets are more complicated than infrastructure networks.

MANET is a collection of independent mobile nodes that can communicate to each other via radio waves with no fixed base station. Means its self-configurational network of mobile node connected by wireless link. Mobile means 'Moving' and ad hoc means 'temporary' without any infrastructure. Due to infrastructure less nature of the network, routing and network management is done cooperatively by the nodes i.e. the nodes themselves are responsible for the creation, operation and maintenance of the network.

1.1. Security issues in MANET

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

- Wireless Links: First of all, the use of wireless links makes the network susceptible to attacks such as eavesdropping and active interference. Wireless network work on lower bandwidth which is useful for the attackers to consuming bandwidth and prevent communication among nodes.
- Dynamic topology: Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The nodes may leave or join the network at any point of time also the topology is vulnerable to link failure, all these affect the status of trust among nodes and the complexity of routing.
- Cooperativeness: MANET's rely on the cooperation of the nodes for routing and packet transmission. In MANET each node is to act as a host as well as a router simultaneously so this is also known as multi hop communication. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.
- Lack of a Clear Line of Defense: MANETs do not have a clear line of defense; attacks can come from all directions. The boundary that separates the inside network from the outside world is not very clear on MANETs.
- Limited Resources: Resource availability is a major issue in MANET. MANETs are a set of mobile devices which are of low or limited power capacity, computational capacity, memory, bandwidth etc. by default. Such resource constraint make the task more difficult.
- Lack of fixed infrastructure: There is no centralized authority to control the network characteristics. Due to this absence of authority, it is very difficult to make monitoring and controlling the traffic in MANET. Lack of centralized management will impede trust management for nodes.
- Scalability: Due to mobility of nodes, scale of ad hoc network changing all the time. So scalability is a major issue concerning security mechanism should be capable of handling a large network as well as small ones.

1.1. Security goals

Security involves a set of investments that are adequately funded. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-

organizing manner. For these reasons, securing a mobile ad hoc network is very challenging. The goals to evaluate if mobile ad hoc network is secure or not are as follows:

- Availability: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.
- Confidentiality: Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is only those who should have access to something will actually get that access. To maintain confidentiality of some confidential information, we need to keep them secret from all entities that do not have privilege to access them. Confidentiality is sometimes called secrecy or privacy.
- Integrity: Integrity means that assets can be modified only by authorized parties or only in authorized way. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never corrupted.
- Authentication: Authentication enables a node to ensure the identity of peer node it is communicating with. Authentication is essentially assurance that participants in communication are authenticated and not impersonators. Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key.
- Nonrepudiation: Nonrepudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such a message .This is helpful when we need to discriminate if a node with some undesired function is compromised or not.
- Anonymity: Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

II. SECURITY ATTACKS

MANET are vulnerable to various attacks not only from outside but also from inside the network itself. So attacks are occurs on the ad hoc network by mainly two different levels. The first level of attack occurs on basic mechanisms of the ad hoc network such as routing and second level of attack occurs on security mechanism of network. The attacks in MANETs are divided into two major types.

2.1. Location base attacks

A. External attacks

External attacks are mainly carried out by node that does not belong or outside the network. They get access to the network by some means and once they get access they try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc.

B. Internal Attacks

In internal attack, the attacker has normal access to the network as well as participates in the normal activities of the network. Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them [1]. It is very difficult to identify the wrong route information generated by internal attackers nodes like compromised nodes or malicious nodes, because this attack are occurs due to more trusted nodes they able to generate the valid signature using their private keys.

2.2. Behavior base attacks

A. Passive attacks

MANETs are more susceptible to passive attacks. A passive attack does not alter the data transmitted within the network. But it includes the unauthorized listening to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic. Detection of such type of attacks

is difficult since the operation of network itself doesn't get affected. In order to overcome this type of attacks powerful encryption algorithms are used to encrypt the data being transmitted.

B. Active Attacks

Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks. These attacks generate unauthorized access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc. The active attacks are generally launched by compromised nodes or malicious nodes. Malicious nodes change the routing information by advertising itself as having shortest path to the destination.

III. LITERATURE SURVEY

In [2], Bansal and Baker developed OCEAN scheme for malicious node detection that is based on direct observations. OCEAN stand for an **O**bservation-based **C**ooperation **E**nforcement in **A**d-hoc **N**etworks. In which rating of node is depend on the behavior of the node. If the node behavior is positive then the rating of the node increased otherwise if the observed behavior is negative the rating of node is decreased by more value than that is used for increment. If the rating of a node decreases beyond faulty threshold then it is added in faulty list. This list is broadcasting to be used as the list of nodes to be avoided. A route is rated good or bad depending on whether the next hop is on faulty list or not. Also used a chance mechanism which is remove the node from the faulty list after an idle period with its rating remaining unchanged.

In [3], Michiardi and Molva proposed **Co**llaborative **Re**putation mechanism (CORE). In which they used a collaborative monitoring techniques and reputation mechanism. Reputation is a measure of someone's contribution to network operation and three types of reputation are defined: (i) subjective reputation, (ii) functional reputation and (iii) indirect reputation. CORE is based on watchdog mechanism. Calculate a reputation value for every neighbor of each node using a sophisticated reputation mechanism that differentiates between the tree types of reputation. Members that have a good reputation can use the resources while members with a bad reputation are gradually excluded from the community. It can be integrated with any network function like forwarding of packets, route discovery, network management and location management and is mainly an extension to the DSR protocol.

In [4], Buchegger and Boudec proposed **C**ooperation **o**f **N**odes: **F**airness **i**n **D**ynamic **A**d-hoc **N**etwork (CONFIDANT). It aims at detecting and isolating uncooperative nodes so that to make it unattractive for nodes to deny cooperation. With Confidant, each node has the following four components: monitor, trust manager, reputation system and path manager. These components interact with each other to provide and process protocol information.

Each node monitors the behavior of its neighbors by monitor component. If a suspicious event is detected, the information is given to the reputation system. If the monitored event is significant for the node, it is checked for its occurrence for more than a predefined threshold that is high enough to distinguish deliberate malicious behavior from simple coincidences such as collisions. If a certain threshold exceeds, the reputation system updates the rating of the node that caused the event. If the rating turns out to be intolerable, the information is sent to the path manager, which deletes all routes containing the misbehaving node.

In [5], Qu He Presents a **S**ecure **O**bjective **R**eputation based **I**ncentive (SORI) scheme to encourage packet forwarding and discipline selfish nodes. This scheme consists of three components. First, neighbor monitoring component monitors packet forwarding behavior of the neighbor nodes and a neighbor node list (NNL) which consists of details for all the neighbors of a node is maintained by each node. Second Reputation Propagation is build record of reputation by using the NNL and shared this reputation with the all nodes to identify the selfish node. Finally a punishment scheme is used by punishment component to penalize selfish nodes. The unique feature of this scheme is that

reputation is secured by one-way hash based authentication scheme and communication overhead is less since reputation is propagated to neighbor nodes only.

In [6], Khalil et al. proposed Lightweight counter measures for **W**ormhole attack (LITEWORP) that provides detection of attack by using secure two hop neighbor discovery with isolation of malicious nodes by local monitoring. They introduced concept of guard node, a node is a common neighbor of two nodes to detect a legitimate link between them. Guard nodes increment the counter by one if malicious action is detected. After the counter reaches beyond threshold value, the node is identified as malicious. It is suitable for resource constrained multi hop wireless networks.

In [7] Swadas PB proposed a scheme **D**etection, **P**revention & **R**eactive **AODV** (DPRAODV) in which used concept of dynamic threshold value and added a new control packet called ALARM. A threshold value is calculating by taken the average of the dest_seq_no between sequence number and RREP packet. If the RREP seq_no is higher than the threshold value then the sender node is consider as an attacker and added it to the black list and also ALARM is send to the neighbors who update (include) the black list. The dynamic threshold value is changed in each slot. By this scheme, the black hole attacks not only be detected but also prevented by updating threshold which responses the realistic network environment and achieves higher packet delivery ratio.

In [8], Saurabh Gupta et. al. proposed Blackhole Attack Avoidance Protocol (BAAP) is avoiding malicious nodes in the routing path by using legitimacy table which is maintained by each node in the network. In BAAP, **A**d-hoc **O**n-demand **M**ultipath **D**istance **V**ector (AOMDV) is used to form link disjoint multi-path during path discovery. When intermediate node replies to source node, few nodes in the routing path may have more than one path to the destination but it chooses only one path to destination node. In BAAP, a legitimacy table is maintained by each node to choose the most legitimate node to source node and next hop to destination node while sending RREP back to source node. Path count field and the send count field are used to define the Legitimacy Ratio of a Node ID which indicates the confidence of node in performing its function of correct routing. A higher legitimacy ratio has higher possibility of a node being non-malicious.

In [9], Jian-Ming Chang et. al. proposed **C**ooperative **B**ait **D**etection **S**cheme (CBDS) which is able to detect and prevent malicious nodes launching cooperative black hole attacks. It integrates with the proactive and reactive defense architectures and the source node randomly cooperates with a stochastic adjacent node. When source node initializes Route Discovery, it sends out the bait RREQ' and then source node receives RREP. If RREP is from not existed destination node or intermediate node then trace which node sends back the RREP according to RREP packet's Record address field. The location of black hole is recognized and detected by source node when receiving the fake RREP. Then the detected black hole node is listed in the black hole list and noticed all other nodes to revoke the certificates of black hole by propagating Alarm packets through the network. Ignore any responses from black hole are discarded.

IV. COMPARISON OF THE TECHNIQUES

Table 1. Comparison of malicious node detection techniques

Detection Technique	*Protocol Name and its type*	*Basic concept*	*Mobility*	*Attack type*	*QoS parameter*	*Change in routing protocol, false detection*
OCEAN [2]	DSR, Reactive	Based on direct observation	Considered	Selfish Node	Throughput	Components system is used, Handled
CONFIDANT [4]	DSR, Reactive	Based on passively Observed behavior	Random Way Point Model	Cooperative misbehaving node	Packet Drop rate and throughput	Components system is used, Handled
SORI [5]	DSR, Reactive	Neighbor monitoring and	Random Way Point	Selfish Node	Packet drop rate and	Yes(NNL list is maintained), Not

		reputation propagation	Model		throughput	Handled
LITEWORP [6]	DSR, Reactive	Guard node can detect the wormhole.	Not Considered	Worm hole	Packet loss	No, Handled
DPRAODV [7]	AODV, Reactive	Dynamic threshold value which is changed in each time slot.	Considered	Single Black hole	Packet delivery ratio and delay	No, Not Handled
BAAP [8]	AOMDV, Reactive	Use legitimacy ratio for detection	Considered	Cooperative Black hole	Packet loss increases with mobility	Yes(legitimacy table), Not handled
CBDS[9]	DSR, Reactive	Baiting and reverse tracing.	Considered	Cooperative Black hole	Packet delay and extra overhead	No, Not Handled

V. CONCLUSIONS

In this paper we have (described) analyzed the various security threats in MANET and some defensive techniques. In literature survey we have described the malicious node detection techniques, with problem of secure routing in MANET and various issues involved in the process. In tabular form we briefly summarized the malicious node detection techniques for MANETs. Thus, it is concluded that MANETs are more prone to malicious node attacks. Thus malicious node detection and its removal are the two main issues that need to be resolved by maintaining the throughput, detection rate, etc.

REFERENCES

[1] Mohammad Ilyas, "The handbook of ag hoc wireless network".
[2] S. Bansal and M. Baker, "OCEAN: Observation based cooperation enforcement in ad hoc networks," *Technical Report*, Stanford University.
[3] Michiardi P, Molva R., "Core: a collaborative reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks," in Proc. of the sixth IFIP Conf. on Security Communications and Multimedia (CMS), 2002.
[4] S. Buchegger, "The CONFIDANT Protocol," NCCR MICS Kick - off Meeting, February, 2002.
[5] Q. He, D. Wu, P. Khosla, "SORI: A secure and objective reputation-based incentive scheme for ad hoc networks," IEEE Wireless Communications and Networking Conference 2004.
[6] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, "LITEWORP : A Lightweight Countermeasure for the Wormhole Attack in Multi-hop Wireless Networks," in Proc. of the International Conference on Dependable Systems and Networks (DSN), 2005
[7] Raj P.N., Swadas P.B., "DPRAODV: A Dynamic Learning System against Black hole Attack in AODV based MANET," International Journal of Computer Science, pp. 54–59, 2009.
[8] Saurabh Gupta, Subrat Kar, S Dharmaraja, "BAAP: Black hole Attack Avoidance Protocol for Wireless Network," IEEE proceedings of the International Conference on Computer & Communication Technology (ICCCT), 2011.
[9] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao, Jiann-Liang Chen, "CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture," IEEE 2011.