ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 6, June 2016

A Review on Mobile Ad Hoc Network Attacks with Trust Mechanism

Rinki Bhati[1], Dr. Deepti Sharma[2]

M-Tech Student, Department of CSE, Advance Institute of Technology and Mgt, Palwal, Haryana, India[1]
HOD, Department of CSE, Advance Institute of Technology and Mgt. Palwal, Haryana, India [2]

Abstract:
Mobile ad-hoc network (MANET) is an independent system linked by mobile nodes with wireless connections. Because of unavailability of infrastructure, MANET is utilized in several applications i.e. business applications, battlefield and remote regions. As, communication among the nodes is by the insecure wireless connection, security is very significant issue for this kind of networks. MANET is susceptible to attacks i.e. Gray hole attack, Black hole attack, Sybil attack, wormhole attack and Route table modification attack. Black hole attack has critical effect on delivery ratio and routing of packets. To secure from Black hole attack, a techniques i.e. intrusion detection system, trust based routing, Data Routing Information table (DR!) and sequence number comparison has been suggested. Trust based On Demand routing method identifies and reduces the risks by harmful node in the route. This paper offers a review of preventing and detecting Black hole attack utilizing trust management method in MANET.

Keywords: Trust, black hole attack, reputation, MANET, security.

I. INTRODUCTION

MANET is a decentralized and independent wireless system. It is also known as infrastructure less and self organized networks. Every node not only works as an end system, but also performs as a router to send packets. Nodes cooperate with one another to send the control and the data packets from source node to destination node. Routing in MANET is categorized in two types: reactive (On-Demand) proactive (table-driven). In a table-routing routing protocol, nodes exchange routing information with other nodes periodically. In a On-demand routing protocol, nodes will exchange routing information only when required. Because of dynamic changing configuration, no clear line and open medium defense attacks on MANET are possible. MANET attacks are A passive attack does not interrupt protocol operations, trap the information by the traffic listening. An active attack includes action i.e. deletion and modification of exchanged data. In MANET reactive routing protocol nodes along the route must cooperate with one another to obtain higher packet delivery ratio. If a misbehaved node is in the route the packet delivery ratio decreased. To detect the misbehaved node and to enhance the MANET performance, trust value for node is presented. The trust value of node shows the node behavior. A low trust value detects a malicious node in the network.

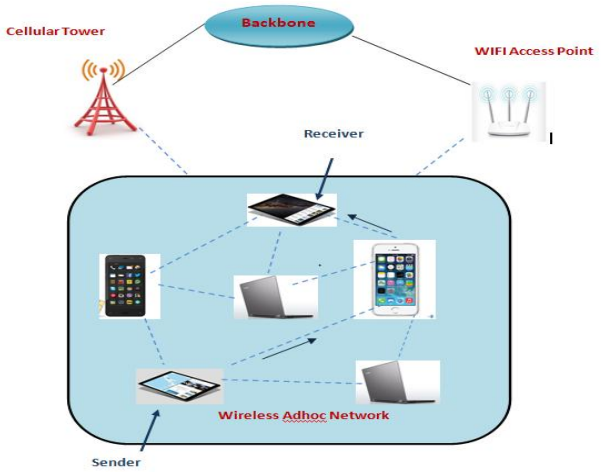

Figure 1: MANET

II. ROUTING PROTOCOLS

The routing protocols are categorized into three main types:

Proactive Routing Protocol: Routing information is exchanged periodically between different mobile nodes. This protocol maintains network topology information in the routing table. Proactive Routing Protocol commonly also known as table driven routing protocol.

Reactive Routing Protocol: In this protocol there is no exchange of routing information periodically. Instead it creates a necessary path when required. It is also known as on demand routing protocol because it obtains on demand routes.

Hybrid Routing Protocol: This routing protocol combines features of both proactive and reactive routing protocols. A table driven or proactive routing approach is used within the routing zone of each node while an on demand or reactive routing approach is used for the nodes that are outside the routing zone.

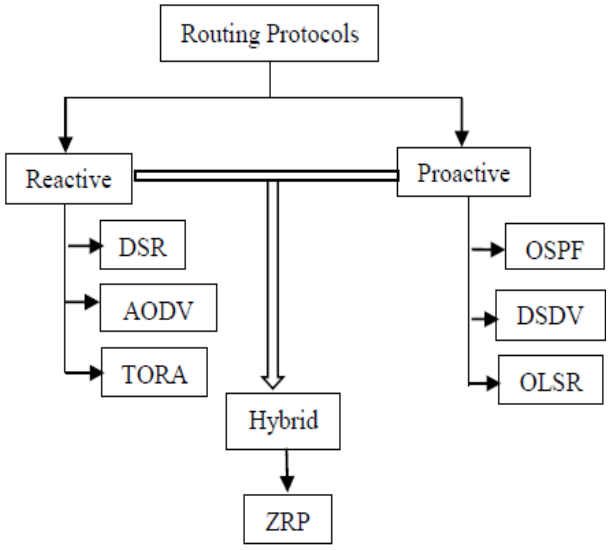

Fig. 2: Types of Routing Protocol

Ad hoc on Demand Distance Vector Routing Protocol AODV) comes under the category of reactive routing protocol and is one of the most popular, widely used routing protocols. Security is a primary concern in MANET which mainly refers to vulnerabilities and threats in the network. Though, there is a huge applicability of MANET, they are also manifest vulnerability to attacks. This vulnerability imposes unreliability, a condition that cannot be compromised even in emergency situations.

III. TYPE OF ATTACKS

Attacks on networks come in several varieties and they can be integrated depending on different features.

a) Availability Attacks: Availability is the most general need of any network. If the networks connection ports are not reachable, or the data forwarding and routing techniques are out of order, the network would stop to present [3].

b) Packet Dropping Attack: In mobile ad hoc networks (MANETs), nodes often cooperate and send each other's packets for enabling out of range communication. Since, in hostile atmosphere, many nodes may refuse to do so, either for saving their own resources or for deliberately interrupting regular communications. This kind of misbehavior is normally known as black hole attack or packet dropping attack [4].

c) Fabricated route Attack: Fabrication attacks produce wrong routing messages. These attacks can be hard to ensure as invalid constructs, particularly in the situation of formed false messages that claim a neighbor cannot be communicated [5].

d) Resource Consumption Attack: In this attack, a harmful node deliberately attempts to consume the resources (for example bandwidth, battery power etc) of network other nodes. The attack can be of several kinds i.e. unessential route discovery, route requests, control messages, or by forwarding stale information [6].

e) Selfishness Attack: Selfishness and harmful nodes play role in route discovery phase suitably to manage their routing table, but as soon as data forwarding phase starts, they loss data packets [7].

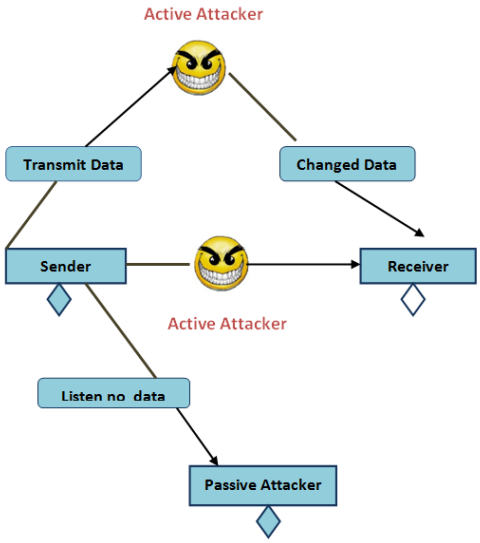

Figure 3: Active and Passive attacks in MANETs

Reactive and Proactive routing protocols require good cooperation between the nodes to route the data from source to destination node. Cooperative nodes never discard the packets or modify the data. Malicious nodes are uncooperative nodes discard the packets and change the data. Misbehaver nodes are of two kinds: malicious node and selfish nodes [2].

Selfish nodes are not fully parting in packets sending service because they are more related about the resources i.e. battery. Selfish nodes discard all data packets that travel through them. A harmful node intentionally discards the packets. Because of this misbehaving node, MANET is vulnerable to various

kinds of routing attacks i.e. Gray hole, Black hole, Sybil attack, Worm hole and resource consumption attack.

GRAY HOLE ATTACK

Gray Hole attack is a special case of the black hole attack in which the malicious node may act as a truthful node first during the route discovery process and then may change its state to malicious and vice versa. This malicious node may then start dropping all or some of the data packets silently as soon as the packets start arriving. Gray Hole attack can be act as a slow poison to the network which shows that the probability of packet loss is undetermined [3]. It is difficult to detect gray hole attack in the network due to congestion, overload and also due to its malicious nature and ability of changing states. The behaviour of gray hole attack is uncertain and unpredicted.

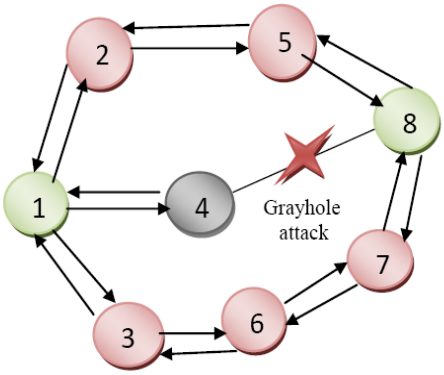

Fig. 4: Gray Hole Attack

There are two phases of gray hole attack. In the first phase, a malicious node in the network exploits the AODV protocol to publicise itself as having a valid route to the destination node, with the purpose of intercepting packets, even though the route is fake. In the second phase, the malicious node drops the intercepted packets with some certain probability. Gray hole attack is more difficult to detect as compared to the black hole attack in which the malicious node drops the received data packets with certainty [4]. A gray hole node may show its malicious behavior in many different ways. It may drop packets either coming from or destined to a certain specific node in the network while forwarding all the packets to some other nodes. Another type of gray hole node may behave as malicious node for some specific period of time by dropping packets but may switch to normal behaviour later. A gray hole node may also exhibit a behaviour which is a combination of the above two situation, hence making its detection even more difficult [5].

IV. TRUST MANAGEMENT

The trust of specific node depends on subjective assessment by peer/agent node on reliability and obtaining information from and (or) traversing through the node provided situation and time. The primary features of trust in MANET have subjective, dynamic, context dependency and asymmetry. Trust can be evaluated in continuous value in between [0,1]. Trust in Ad-hoc networks are categorized into two types, one is identity trust and another is behavior trust. Identity trust depends on the node identity. This can be obtained by digital signature, encryption mechanism and authentication technique. Behavior trust depends on the node behavior and is utilized to differentiate between malicious and authorized node. Behavior trust can be demonstrated in two ways in and directly. A direct trust is observation that is directly built by the node itself. Indirect trust is measured utilizing advice from other nodes, and suggests trust from third party in MANET. Trust management is to measure the neighboring nodes behavior, and allocates a trust value for each node depending on the behavioral assessment result. Trust models are carried out for trust management. These trust models are categorized as distributed models and centralized models. In centralized models, trust values are saved in trusted third party server or centralized server. Since this model is not proper because of dynamic changing configuration as MANET. In decentralized models every node allocates trust values to its neighboring nodes to communicate with other node. Nodes in the communication areas of nodes are taken to be the neighboring nodes. In starting, a node is not known of all the nodes in the communication area. To demonstrate trust in MANET a node must aware all the other neighboring nodes in the network.

As illustrated in Fig. 5, Trust Management System (TMS). Trust management improves the privacy and security of mobile ad-hoc networks and also enhances the communication quality among devices. TMS composed of two parts, Watchdog and Reputation System (RS). The service of Watchdog is to monitor routing nature of a node, and then feed the information into Reputation System (RS) to maintain the node reputation.

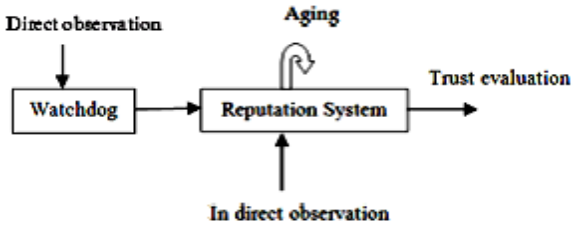

Fig. 5 trust management system

RS primarily has three tasks: (1) manage reputation value by direct observation obtained from Watchdog, (2) integrate reputation value by combining the indirect information obtained from other members with direct observation, and (3) aging reputation which is a technique when fresh direct observation is not existed for a long time period.

V. RELATED WORK

Shivani Uyyala et al [6] proposed anomaly based intrusion detection mechanism for the detection of gray hole attack in the network. The author uses monitoring nodes which have unique id and can never behave as malicious node. The sender sends the packets until the attack is detected and once the attack is detected the monitoring node broadcast an alert message and ID blocks the route and chooses another route for data transmission. This method increases the network performance for AODV with intrusion detection technique. But this method fails when the attacker modifies the data packet without dropping the packets.

Megha Arya et al [7] uses AODV routing protocol to discover route, an Intrusion detection system (IDS) to monitor the network for malicious activities and gives reports to a Management Station. The author has designed AODV and grayhole AODV protocols to transfer packets and uses three performance metrics: throughput, routing load, packet delivery ratio. Results show that throughput and packet delivery ratio have been increased to 92.69% and 80.40% respectively and routing load has been decreased to 75.22 %.

Deepali A. Lokare et al [8] proposed a credit based approach on AODV routing protocol (CBAODV) for the discovery and elimination of cooperative gray hole attack in MANET. Every node in the network assign a credit value to which the route request is to be send and subtracting the credit value after a reply comes from them. The performance metrics used are: throughput, packet loss rate, normalized routing overhead, packet delivery ratio and end-to-end delay. Simulation results show that the proposed method gives good performance in terms of better throughput and minimum packet loss percentage over AODV without attack and AODV with attack.

Shalini Jain et al [9] proposed an algorithm to detect a chain of cooperative black/ gray hole nodes. The technique is based on sending data in terms of equal but small sized blocks instead of sending whole of the data in one continuous stream. The complexity of the proposed algorithm is O(n) which is half of the previous complexity $O(n^2)$. Using this algorithm, each node creates its own table of black listed nodes whenever it tries to send data to any destination node. This list of black listed nodes can be applied to discover secure paths from source to destination by avoiding multiple black/ grayhole nodes.

Garima Neekhra [10] gives IDS aodv technique to improve the performance of the network. AODV routing Protocol is used for route discovery and intrusion detection system (IDS) is used to report violation of policy and for the nodes whose packets are dropped again and again and these nodes try to establish new paths using Route Requests (RREQ) messages. Result shows that after applying IDS technique performance of the network gets improved. For comparison the author has taken throughput, sending packet, receiving packet, PDF, dropped packet, dropped bytes etc. as parameters metrics.

In his work the author simulate that Network under the presence of packet dropping attacks, the performance of the network degrades but after setting up IDS , a secure route is created by isolating the black hole and gray holes so that we can able to improve the network performance

Into the method proposed by author we can detect and isolate black hole and gray hole attack that is if the attacker is dropping the packets but if the attacker modifies the data packets without dropping the packets then this proposed method cannot detect these kind of attacks so we can extend the proposed methodology by using cryptographic hash function to detect and isolate packet modification attacks.

CONCLUSION

A review of trust based routing protocol in MANET to protect black hole attack that is caused by a misbehaved node is talked about in this paper. A misbehaved node decreases end to end delivery of packet ratio. To increase packet delivery ratio there is requirement for detecting the misbehavior nodes dynamically depending on trust value. From the review it is discovered that there are no mechanisms to deal with the colluding two or more harmful nodes in MANET, which importantly decreases the network performance. Taking the above limitations we would like to introduce a new efficient trust based routing mechanism to enhance cooperation among the nodes depending on efficient trust calculation. In future we plan to carried out and examine the performance of the introduced trust based routing mechanism.

REFERENCES

[1] Seryvuth Tan, Keecheon Kim "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs", *IEEE International Conference on High Performance Computing and Communications*, 2013.

[2] Radityo Anggoro, Teruaki Kitasuka" Performance Evaluation of AODV and AOMDV

with Probabilistic Relay in VANET Environments", *Third International Conference on Networking and Computing*, 2012.

[3] Meenakshi Patel, Sanjay Sharma" Detection of Malicious Attack in MANET A Behavioral Approach", *IEEE Conference on Networking*, 2012.

[4] H. Deng, H. Li, D.P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Communications Magazine*, October 2002, Vol. 40, No. 10,.

[5] Jaydip Sen," A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", *IEEE ICICS*, 2007.

[6] Shivani Uyyla, Dinesh Naik, "Anomaly based Intrusion Detection of Packet Dropping Attacks in MANET", *IEEE International conference on Control, Instrumentation, communication and Computational technologies*, 2014, pp.1137-1140.

[7] Megha Arya, *Yogendra* Kumar Jain, "Grayhole Attack and Prevention in Mobile Adhoc Network", *International Journal of Computer Applications*, August 2011, Vol.27, pp.21-26.

[8] Deepali A. Lokare, A.M Kanthe, Dina Simunic, " Cooperative Grayhole Attack Discovery and Elimination using Credit based Technique in Manet ," *International Journal of Computer Applications*, February 2014, Vol. 88, pp.13-22.

[9] Shalini Jain, Mohit Jain, Himanshu Kandwal, "Advanced Algorithm for Detection and Prevention of Cooperative Black and Grayhole Attacks in MANET", *International Journal of Computer Applications*, 2010, Vol. 1, pp.37-42.

[10] Garima Neekhra, Sharda Patel, " Effect of Grayhole Attack with IDS Techniques for AODV Routing Protocol using Network Simulator", *International Journal of Advanced Research in Computer Engineering & Technology*, December 2014, Vol. 3, pp.4184-4190.