ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 6, June 2013

A Survey of Attacks on Manet Routing Protocols

Supriya Tayal [1], Vinti Gupta [2]

M.Tech Student, Department of Computer Science & Engineering, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan, India[1]

Assistant Professor, Department of Computer Engineering, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan, India[2]

Abstract: An Adhoc network is a network in which nodes communicate without using any network infrastructure and move in random order. MANET (*M*obile *A*dhoc *NET*work) is an attractive technology for many applications, such as rescue and tactical operations, due to the flexibility provided by their dynamic infrastructure. MANET is an autonomous system of wireless mobile hosts without fixed network infrastructure and centralized access point such as a base station. 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. In this paper we have attempted to represent an overview of AODV, the possible attacks on MANET and some security mechanism to these attacks.

Keywords: Manet, Routing Protocols, AODV, Attacks, Security Mechanisms

I. Introduction

Recent advancement of wireless technologies like Bluetooth introduced a new type of wireless system known as Mobile ad-hoc network (MANETs) which operate in the absence of central access point. Each node operates not only as an end-system, but also as a router to forward packets. It provides high mobility and device portability's that enable to node connect network and communicate to each other. Ad hoc is Latin and means "**for this purpose**". A Mobile Ad Hoc Network is an autonomous system in which mobile host moves in a free and random manner.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. Such networks may operate by themselves or may be connected to the larger Internet. The characteristics of MANETs such as: dynamic topology, node mobility, provides large number of degree of freedom and self-organizing capability of that make it completely different from other network.

MANET is used in applications such as search and rescue, automated battlefields, emergency relief scenarios, law enforcement, public meeting, data network, device network, virtual classroom, disaster recovery, sensor networks and other security sensitive computing environment.

Fig. 1 Example of a typical Manet

The chief characteristics and challenges of the MANETs can be classified as follows:

1) Cooperation: Manets rely on the cooperation of the nodes for routing and packet transmission. If the source and destination node are not in the range of each other then the communication between them takes place with the cooperation of other nodes. All the nodes between them form a optimum chain of mutually connected nodes. In this each node is to act as a host as well as a router simultaneously so this is also known as multi hop communication.

2) *Dynamism of Topology:* The Manet nodes are random and unpredictable and so is the topology. 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.

3) *Lack of fixed infrastructure:* The absence of a fixed or central infrastructure is a key feature of MANETs. There is no centralized authority to control the network characteristics. Due to this absence of authority, traditional techniques of network management and security are scarcely applicable to MANETs.

4) Resource constraints: MANETs are a set of mobile devices which are of low or limited power capacity, computational capacity, memory, bandwidth etc. by default. So in order to achieve a secure and reliable communication between nodes, these resource constraints make the task more enduring.

II. ROUTING PROTOCOLS

Routing is the process of forwarding packets from source to destination using most efficient route. Efficiency of the path/route is measured in various metric like number of hops, traffic, security etc**.** The main goal of routing protocols is to minimize delay, maximize network throughput, maximize network lifetime and maximize energy efficiency.

All MANET routing protocols could be broadly classified into three major categories: Pro-active Routing Protocols, Reactive Routing Protocols, Pro-active Routing Protocols.

1) *Proactive routing protocol:* In proactive routing scheme every node continuously maintains complete routing information of the network. This information is stored in tables. Each node maintains a routing table which contains the list of destinations and routes.
2) *Reactive routing protocol:* The reactive routing protocols are based on some sort of query-reply dialog. In this the nodes do not need periodic transmission of topological information of the network. When there is a need for a route to a destination, route request messages are flooded periodically with new networks status information. Every node in this routing protocol maintains information of only active paths to the destination nodes.
3) *Hybrid Routing Protocols:* Often reactive or proactive feature of a particular routing protocol might not be enough. These protocols combined the features of both reactive and proactive routing protocols.

III. OVERVIEW OF AODV

AODV (Adhoc On-demand Distance Vector) is a reactive routing protocol, but it is basically an improvement of DSDV routing protocol which is proactive protocol. It initiates route discovery process routes only when there is any need to find node. AODV can handle low, moderate, and relatively high mobile rates, together with a variety of data traffic loadings. However, it makes no provisions for security.

In Route Discovery Process of AODV there are types of messages: Route Request (RREQ), Route Reply (RREP), and Route Error (RERR) messages. A source node broadcasts a RREQ message by route discovery process whenever it wants to communicate to destination node but does not have a fresh route to the. All the intermediate nodes that receive this RREQ message either send a RREP to the source node or forward the RREQ message to the other nodes. RREP message is send only when the intermediate nodes have a fresh route to the destination node and the "destination only" flag is not set. If the request packet has been forwarded by this intermediate node before, it is silently dropped. When the destination node receives a RREQ for itself, it sends back a RREP message on the reverse route. The requesting node and the nodes receiving RREP messages on the route update their routing tables with the new route. A route generates a RERR message either a route breaks or it does not have a route to the destination to which the packet is to be send.

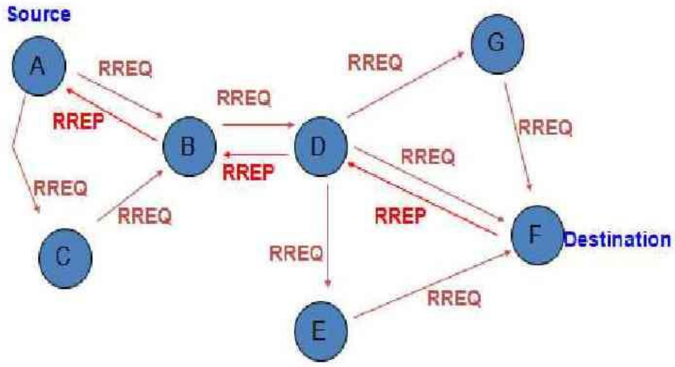

Fig. 2 Example of a AODV Routing Protocol

A. *Security Threats in AODV*

Title AODV has no/less security mechanisms, so the malicious nodes can perform many attacks. A node is compromised if a node behaves maliciously. It happens when an legitimate node behaves maliciously but the network can not identified it. The types of malicious activity depend on the functioning of the protocols. A node is called selfish when it tends to deny its own resources for the benefits of other nodes in order to save its own resources. Since AODV has no security mechanisms several attacks can be launched against the AODV routing protocol: denial of service, impersonation, distributed false route request.

The attacks can be classified as passive attacks or active attacks.

1) *Passive attacks:* In a passive attack an unauthorized node continuously monitors the network and willing to get the information. In this the communications is not interrupted. There is no direct damage to the network. The attacker can read the information which can be used for future harmful attacks. Examples of passive attacks are eavesdropping and traffic analysis.

- *Eavesdropping Attacks:* It is also known as disclosure attack. These are passive attacks by external or internal nodes. The attacker gathers information e.g. Private key, public key or even passwords of the nodes and analyzes broadcast messages to reveal some useful information about the network.
- *Traffic Analysis:* In this the network traffic and messages are examined to find out information. It can be performed on encrypted messages. In this the attackers use techniques such as traffic rate analysis, and time-correlation monitoring etc.

2) *Active Attacks:* These attacks cause unauthorized state changes in the network such as denial of service, modification of packets etc. These attacks are generally launched by users or nodes with authorization to operate within the network. The active attacks can be classified into four groups: dropping, modification, fabrication, and timing attacks. An attack can be classified into more than one group.

- *Dropping Attacks:* It is a kind of denial of service attack and most difficult one to detect and prevent. Malicious or selfish nodes drop all packets that are not destined for them. While malicious nodes aim to disrupt the network connection, selfish nodes aim to preserve their resources. Dropping attacks can prevent end-to-end communications between nodes, if the dropping node is at a critical point. It might also reduce the network performance by causing data packets to be retransmitted, new routes to the destination to be discovered, and the like.
- *Modification Attacks:* Insider attackers after reading the data in the packet modify it to disrupt the network. For example modifying the hop-count value of a routing packet to a smaller value. By decreasing the hop count value a malicious node can attract more network communication.
- *Black Hole Attack:* The black hole attack is a kind of denial of service attack. In this attack, the malicious node sends false route replies to the source node claiming to have the shortest path to the destination node. When the source node established the route through the malicious node, the malicious node then misuse or discards any or all of the network traffic being routed through it.
- *Grey Hole attack:* It is a special type of black hole attack in which the attacking node first agrees to forward packets and then fails to do so. In this the selected packets are dropped. Gray Hole attack may occur due to a

malicious node which is deliberately misbehaving, as well as a damaged node interface.

- *Wormhole attack:* It is also known as tunneling attack. In this an attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

3) Other Attacks:

- *Timing Attacks*: In this an attacker attracts other nodes by causing itself to appear closer to those nodes than it really is. DoS attacks, rushing attacks, and hello flood attacks use this technique.
- *Sleep Deprivation:* In sleep deprivation attack, the attacker interacts with the target node in a manner that appears legitimate but the resources of the nodes of the network are consumed by constantly keeping them engaged in routing decisions. The attacker node continually requests for either existing or non-existing destinations, forcing the neighboring nodes to process and forward these packets and therefore consume batteries and network bandwidth obstructing the normal operation of the network.
- *Impersonation Attack:* These are also called *spoofing* attacks. The attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes. The attacker nodes impersonates a legitimate node and joins the network undetectable, sends false routing information, masked as some other trusted node.
- *Routing Table Poisoning Attack:* Different routing protocols maintain tables which hold information regarding routes of the network. In poisoning attacks, the attacker node generates and sends fictitious traffic, or mutates legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. Another possibility is to inject a RREQ packet with a high sequence number. This causes all other legitimate RREQ packets with lower sequence numbers to be deleted. Routing table poisoning attacks can result in selection of non-optimal routes, creation of routing loops, bottlenecks and even partitioning certain parts of the network.
- *Location Disclosure Attack:* In this attack, the privacy requirements of an ad hoc network are compromised. Through the use of traffic analysis techniques or with simpler probing and monitoring approaches an attacker is able to discover the location of a node, and the structure of the network.
- *Rushing Attack:* In this attack the attacker (initiator) node initiates a Route Discovery for the target node. If each neighbor of the target node receives these RREQ messages first, then the route discovered by this route discovery process will include a hop through the attacker. Then the neighbor forwards that REQUEST to the target node. When non-attacking REQUESTs arrive later at these nodes, they will discard those legitimate REQUESTs. As a result, the initiator will be unable to discover any usable routes (i.e., routes that do not include the attacker) containing at least two hops (three nodes).

B. Securing Routing Protocols in MANET

There are number of security mechanisms as authentication, access control, confidentiality, Data Integrity, Non-Repudiation, Availability. Many of the attacks can be avoided by using these mechanisms. Some approaches are used for these mechanisms. Digital Signatures are used for authentication, encryption is used for confidentiality, and integrity of data is achieved by hash functions. Integrity is used so that any malicious node cannot be able to alter data while access control controls the access of data, not all nodes have rights to access information. Authentication is used to ensure that the nodes are those which they claim to be i.e. to ensure the identity of nodes authentication is used; confidentiality is used to prevent the unauthorized access of data [7]. Non-repudiation prevents sender and receiver from denying messages [19]. Authentication should be enforced during all routing phases, thus preventing unauthorized nodes (including attackers) from participating in the routing and so from launching routing attacks. Digital Signatures can be verified by any node, providing a secure proof of the identity of the sender [10].

To defend against passive attacks conventional approaches like Digital signature, encryption, authentication and access control and defend against active attacks intrusion detection systems and cooperation enforcement mechanism are very useful [15].

Apart of these mechanisms there are few more security techniques such as secure key management, intrusion detection etc. As for encryption and digital signature secure key distribution is also very necessary. Key management is the necessity for secure key distribution. It is the mechanism for issuing, exchanging, and revoking keys. Key management in MANETs is generally more difficult due to the absence of any infrastructure or central administrative authorities. [10].

Since new intrusions continually emerge, an intrusion detection system (IDS) is an indispensable part of a security system. IDS deals with attacks by collecting information from a variety of systems and network sources, and then analyzing the information for possible security problems introduced to detect possible violations of a security problems[13]. IDS architecture can be categorized into three types: *Signature based IDS*, *Anomaly based IDS* and *Specification based IDS* [14]. There has been a lot of research done on preventing or defending attacks through IDSs for MANETs, or on modifying current IDSs to be applicable to MANETs.

IV. COUNTERMEASURES AGAINST AODV

Lots of researches have been done to provide security on AODV against threats. One of the most threats is Black hole Attack. There are a number of solutions have been suggested for detection and prevention from black hole attacks in AODV. Some of them are as follows:

Sanjay Ramaswamy et al. [16], proposed a solution for cooperative black hole attacks by slightly modified AODV Routing Protocol by introducing Data Routing Information (DRI) Table and Cross Checking. This algorithm is based on a trust relationship between the nodes.

Vishnu K et al. [17], Discussed a Backbone Network which is based on selecting some trustworthy and powerful nodes in terms of battery power and range. These nodes which are referred to as Back Bone Nodes (BBN) will form a Back Bone network and have special functions unlike normal nodes. This algorithm detects black hole as well as gray hole attack in AODV.

Deng et. al. [18] has proposed an algorithm to prevent black hole attacks in ad hoc networks. According to the algorithm, any node on receiving a RREP packet, crosschecks with the next hop on the route to the destination from an alternate path. If the next hop either does not have a link to the node that sent the RREP or does not have a route to the destination then the node that sent the RREP is considered as malicious. This solution cannot prevent cooperative black hole attacks. Apart of that there are many techniques which are used for the security of AODV.

V. CONCLUSION

Security of routing protocols in Manet is a challenging task as the nodes are mobile and self-organized. There are a number of security threats against AODV. To design such a technique which prevents the AODV routing protocol from all the threats is very difficult. Although many researchers have worked through the security of AODV but the area of research in this is still open. Many techniques have been designed to provide security in AODV against some specific attacks. Not all the attacks can be prevented by using a single technique. So a combination of number of techniques should be used to fully secure the AODV Routing Protocol. In this paper we have described some of the possible attacks on AODV and some defensive techniques.

ACKNOWLEDGMENT

Many people have contributed to this research, either directly or indirectly. To start with, we must thank all the researchers who have contributed to the fields of MANET because their work enabled us to do further enhancement in this area. Finally, we would like thanks to our parents and our friends for their support and understanding.

REFERENCES

[1] Sevil Sen, John A. Clark, Juan E. Tapiador, “Security Threats in Mobile Adhoc Networks”, http://web.cs.hacettepe.edu.tr/~ssen/papers/Survey_SecThreatsMANETs.pdf

[2] KUTE D.S., PATIL A.S., PARDAKHE N.V. AND KATHOLE A.B., “A Review: Manet Routing Protocols and Different types of attacks in Manet”, International Journal of Wireless Communication ISSN: 2231-3559 & E-ISSN: 2231-3567, Volume 2, Issue 1, 2012

[3] Mishra, Alekha Kumar,“Analysis of Secure Routing Scheme for MANET”, M.Tech Thesis. (2009).

[4] PALANISAMY1, P.ANNADURAI, “IMPACT OF RUSHING ATTACK ON MULTICAST IN MOBILE AD HOC NETWORK”, (IJCSIS) INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND INFORMATION SECURITY, VOL. 4, NO. 1 & 2, 2009

[5] G.Vijaya Kumar, Y.Vasudeva Reddyr, Dr.M.Nagendra, “Current Research Work on Routing Protocols for Manet: A Literature Survey”, (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 706-713

[6] Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong, “A New Routing Attack in Mobile Ad Hoc Networks”, International Journal of Information Technology Vol. 11 No. 2.

[7] “Rutvij H.Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah, “Manet Routing Protocol and Wormhole Attack against AODV”, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[8] Karlsson, Jonny; Dooley, Laurence S. and Pulkkis, Goran, “Routing Security in Mobile Ad-hoc Networks”. Informing Science and Information Technology Education 2012 Conference (InSITE’12), 22-27 June 2012, Montreal, Canada (Forthcoming), 2012.

[9] Ashwani Garg, Vikas Beniwal, “A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, pp.145-148, September-2012.

[10] Preeti Bathla, 2Bhawna Gupta, “Security Enhancements in AODV Routing Protocol”, IJCST Vol. 2, Issue 2, June 2011.

[11] Adnan Nadeem and Michael Howarth, “Protection of MANETs from a range of attacks using an intrusion detection & prevention system”, Springer.

[12] K. SIVAKUMAR, Dr. G. SELVARAJ, "OVERVIEW OF VARIOUS ATTACKS IN MANET AND COUNTERMEASURES FOR ATTACKS", Vol 2, Issue 1, ISSN 2278-733X, January 2013.

[13] http://www.sans.org/reading_room/whitepapers/detection/understanding-intrusion-detection-systems_337.

[14] Mohammad Saiful Islam Mamun, A.F.M. Sultanul Kabir, "Hierarchical design bases IDS for Wireless Adhoc Sensor Network", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010.

[15] Praveen Kumar, Jatin Sharma,Kriti Saini, "A survey on AODV routing protocol for Ad-hoc network", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013.

[16] Sanjay Ramaswamy; Huirong Fu; Manohar Sreekantaradhya; John Dixon; and Kendall Nygard (2003). Prevention of cooperative black hole attack in wireless Ad hoc networks. In Proceedings of 2003 International Conference on Wireless Networks, (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.

[17] Vishnu K and Amos J Paul, "Detection and Removal of Cooperative Black/Gray hole Attack in Mobile Adhoc Networks", International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 22, 2010.

[18] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol. 40, pp. 70-75, 2002.

[19] Stallings W., "Cryptography and Network Security", Prentice Hall, pp. 12-20, 2007,

BIOGRAPHY

Supriya Tayal received her B.Tech degree in Computer Science and Engineering from Shobhit Institute of Engineering & Technology, Saharanpur, in 2011, and pursuing M.Tech in Computer Science & Engineering from Jayoti Vidyapeeth Women's University, Jaipur, at present.

Vinti Gupta received her B.Tech degree in Computer Science and Engineering from Shobhit Institute of Engineering & Technology, Saharanpur in 2009, and M.Tech degree in Computer Science & Engineering from Jayoti Vidyapeeth Women's University, Jaipur. She is Asst. Professor in Jayoti Vidyapeeth Women's University, Jaipur.