Study on Sinkhole Attacks in Wireless Ad hoc Networks

GAGANDEEP
Department of Computer Science & Engineering,
Shaheed Bhagat Singh College of Engineering & Technology,
Ferozepur, Punjab (India)
gaganluthra85@gmail.com

AASHIMA
Department of Computer Science & Engineering,
Shaheed Bhagat Singh College of Engineering & Technology,
Ferozepur, Punjab (India)
aashima_kataria@ymail.com

Abstract-Wireless ad hoc network is a collection of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. As compared to conventional network, wireless ad hoc network are more vulnerable to the security attacks. The nature and structure of wireless ad hoc network makes it very attractive to attackers, because there is no fixed infrastructure and administrative approach in it. "Sinkhole attack" is one of the severe attacks in this type of network; this makes trustable nodes to malicious nodes that result in loss of secure information. This paper focuses on sinkhole attacks on routing protocols such as DSR, AODV. To overcome the problems occur due to sinkhole we discuss about Security-aware routing (SAR) which helps to reduce the impact of such attack.

Keywords: DSR, AODV, SAR, wireless ad hoc network, Sinkhole attacks

I. INTRODUCTION

A. Structure of wireless ad hoc network

Wireless Ad hoc Network consists of autonomous mobile nodes interconnected by wireless multi hop communication paths. They can communicate and move at the same time. Wireless Adhoc networks have no fixed network infrastructure or administrative support, unlike other conventional network that requires fixed network infrastructure [1]. The topology of an ad hoc network can change because nodes may not be fixed i.e. it changes dynamically as mobile node join or depart the network. Ad hoc networks can also be defined as self creating, self organizing, and self administering [1]. There are no routers or other base stations to route packets from source to destination .So wireless ad hoc network is a kind of self-configuring network of mobile nodes connected by wireless links – the union of which forms an arbitrary topology. The participating nodes act as router are free to move randomly and manage them arbitrarily, such a network may operate in a standalone fashion or may be connected to the larger Internet [1, 2].

The figure 1 shows the interaction among three nodes. To make communication between A and C must discover the route through B. The circle in the figure represents the nominal range of each node's radio transceiver. A wireless ad hoc network is much more flexible than wired network. It does not required complex wired structure and other network equipments.

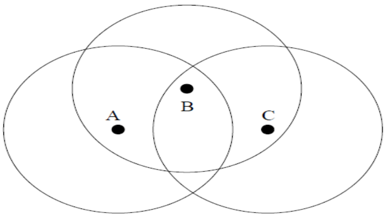

Fig .1 A Simple Wireless ad hoc network with three participating nodes

B. Security in Wireless Ad hoc Network

From a security point of view, there are lots of reasons why wireless Adhoc networks are at risk. The links required between nodes in wireless networks are highly susceptible to link attacks or routing attacks. Link attacks further leads to Route Disruption, Active Interfering, Loss of Secret Information, Message distortion, Denial of Service (DoS), Data Tempering etc[2].Wireless Ad hoc networks are also susceptible to the problems related to the compromised nodes, the compromised nodes works in such a way that seems like work correctly but the same time they may make use of the flaws and inconsistencies in the routing protocols (DSR, AODV).The compromised node can become malicious node and create new routing messages and advertise itself in a existing links and start producing incorrect link state information that results in network delay, energy consumption and finally makes the network disabled. Some Reactive (On-Demand) and proactive (Periodic) routing protocols are vulnerable to these attacks.

II. Sinkhole Attack

Sinkhole attack is one of the severe attacks in wireless Ad hoc network. In sinkhole Attack, a compromised node or malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic. After receiving whole network traffic it modifies the secret information, such as changes made to data packet or drops them to make the network complicated. A malicious node tries to attract the secure data from all neighboring nodes. Sinkhole attacks affects the performance of Ad hoc networks protocols such as AODV by using flaws as maximizing the sequence number or minimizing the hop count [4]. In this way the path presented through the malicious node appears to be the best available route for the nodes to communicate. In DSR protocol, sinkhole attack modifies sequence no in RREQ.

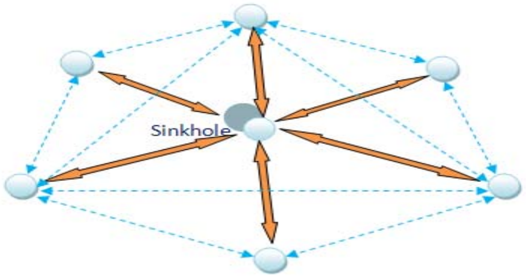

Fig.2 Example of Sinkhole attack

A. Effect of Sinkhole Attack on routing protocols

Routing protocols are required whenever a data packet needs to be transmitted from source node to the destination node by communicating with number of intermediate nodes. Various routing protocols have been proposed for such kind of ad hoc networks. These protocols help to find a specific route for packet delivery and deliver the packet to the correct destination. The studies on various aspects of routing protocols have been an active area of research for many years. This paper analyzes the “Sinkhole Attack” that can be easily employed against various routing protocols. Routing protocols used in wireless Ad hoc networks can be classified in two major types.

- Table-driven routing protocols (Pro-Active)
- On-demand routing protocols (Reactive)

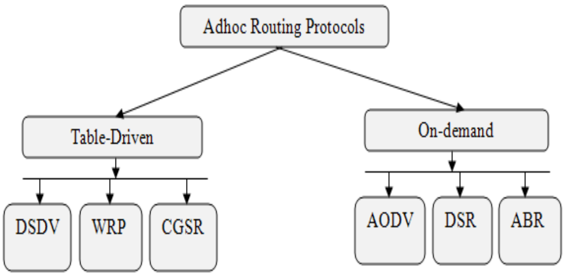

Fig.3 Ad hoc Routing Protocols

Table-driven routing protocols are enhancements of the wired network routing protocols. They maintain a table structure in order to store the routing information of each router. Table is consistently updated to maintain the correct information of network status [5, 7]. On the other hand, on-demand routing protocols executes the path-finding process when a path is required by a node.

1). DYNAMIC SOURCE ROUTING (DSR)

The Dynamic Source Routing (DSR) protocol is an on-demand routing protocol that is based on the concept of source routing. DSR is mainly designed to restrict the bandwidth consumed by control packets in wireless ad hoc network [5]. The protocol consists of two major phases:

- Route discovery phase
- Route maintenance phase

In DSR when a node has a packet and it does not know the route for the destination, it sends out a ‘route request’ packet i.e. it initiates route discovery by broad-casting a route request packet. All the traversed nodes are recorded in the packet header [6]. The source node maintains the discovered route in its ‘route cache’ and delivers the packets to the destination node through the discovered route by using source routing. The address of each node to visit until reaching the destination is written in the packet header by the source node. If the routing is done through a previously discovered route fails, than a ‘route error’ message generated by the node that discovers the route failure [6, 11]. The route failure is sent back to the source node, the failed route is removed from the ‘route caches’ and a new route discovery procedure are initiated for the destination. On the other hand, if node has route then, it verifies its route cache to determine whether it has already a route to the destination. If it has an unexpired route to the destination node, than it will make use of this route to send the data packet over it.

A. Route Discovery Phase

In route discovery phase, any node can discover a route to other node in local ad hoc network. In order to get the route from source node to the destination node, a source node broadcasts a route request packet (RREQ) which contains a source id, destination id, sequence number[5, 8 ,13]. On receiving RREQ node rebroadcasts the packet to its neighbors if it does not have a route to the destination in its cache. If it has, then it sends route reply packet (RREP) that contains the route information to the source node through reverse path of the RREQ shown in figure 5.

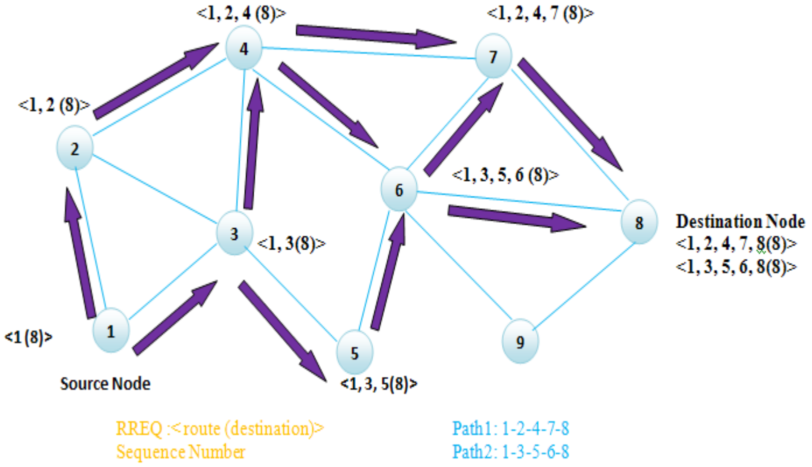

Fig.4 Route Establishment in DSR

Given diagram shows the RREQ propagation procedure. Source node 1 initiates RREQ packet to its neighbors in order to find the path for destination node 8. Each intermediate node rebroadcasts the RREQ until the packet meets the destination node 8. Route < 1 2 4 7 8 > is selected and RREP is generated by node 8. RREP traverses through reverse route < 8 7 4 2 1 >. The procedure of RREP is well described in figure 5.

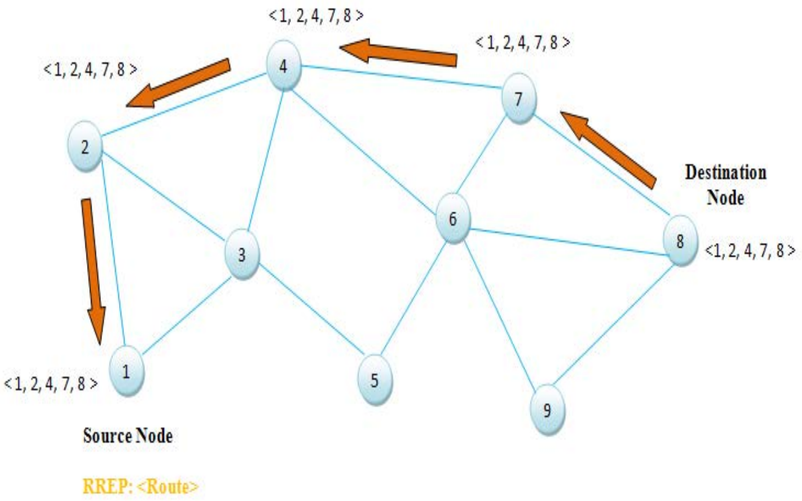

Fig.5 Route Reply Propagation in DSR

B. Route maintenance phase

Route maintenance is the mechanism by which the source node detects whether the network topology has been changed. It determines how long it is available for use as a route to destination because a link along the route no longer works [8]. Each forwarding node is responsible for confirming the receipt of each packet by the next hop node by a link-layer acknowledgment [6, 8]. If a packet is retransmitted the maximum number of times and no receipt confirmation is received, the node returns a Route Error message to original source, identifying the link over which the packet could not be forwarded. Source node then removes the broken link from its cache. If source node has another route to destination in its route cache, Source can send packets using the new route immediately. Otherwise, Source node may perform a new route discovery.

C. Sinkhole Attack in DSR

In DSR protocol, whenever sinkhole attack is encounter it starts modifying sequence number in RREQ. Sequence number used to prevent loop formations and to avoid multiple transmissions of the same Route Request by an intermediate node that receives it through multiple paths [5]. The higher sequence number, the more recent route the packet contains. Sinkhole node selects the source, destination node. It monitors the source node's sequence number, and generates bogus or fake RREQ. It places itself on the source route and broadcasts the bogus RREQ. When neighbors receives bogus RREQ can observes this route could be a better route to reach destination.

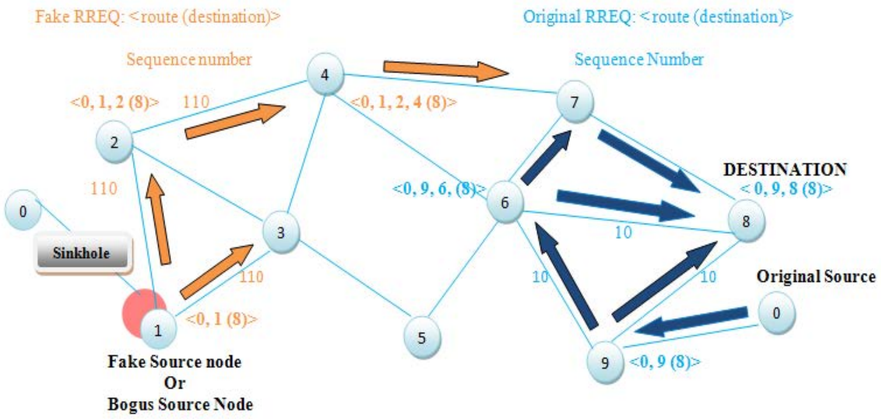

Fig.6 Sinkhole attack introducing bogus node

The given diagram shows how bogus node affects the routing process by advertizing itself as an active participant in transmission of packets. Sinkhole node 1 initiates the bogus RREQ which looks as if it is initiated by the node 0. The sequence number of the bogus node is 110 i.e. much higher than the original source node sequence number 10. Which results in higher sequence number is observed as source sequence number. Then it adds itself on the source route and broadcasts the bogus RREQ.

Neighbor nodes when receives the bogus RREQ and recognize this route could be better than original route. The bogus route <0 1 2 4 7 8 > is established and RREP is generated by the Destination node 8 in the form of <8 7 4 2 1 0> path.

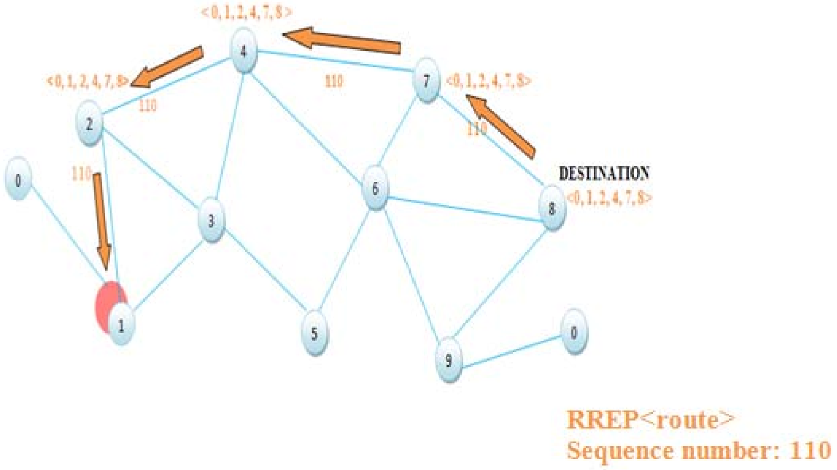

Fig.7 Bogus RREP

In summary, a malicious node can disrupt the routing mechanism employed in DSR protocols.
(1) Attack the route discovery process by:

- Changing the contents of a discovered route;
- Modifying a route reply message, causing the packet to be dropped as an invalid packet;
- Invalidating the route cache in other nodes by advertizing incorrect paths;
- Refusing to participate in the route discovery process.

(2) Attack the routing mechanism by:

- Modifying the contents of a data packet or the route via which that data packet is supposed to travel;
- Behaving normally during the route discovery process but dropping data packets, causing a loss in throughput.

(3) Generate false route error messages whenever a packet is sent from a source to a Destination.

2). AD HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

AODV is an on-demand ad hoc routing scheme that adapts the distance vector algorithm to run on a network with a mobile backbone [11].AODV keeps all these routes as long as they are desirable to the sources. Unlike DSR, which uses source routing, AODV uses hop -by-hop routing. AODV requests a route only when it is needed, but it does not require mobile nodes to maintain routes to the destination that are not actively used. AODV retains the desirable feature of DSR that routes are maintained only between nodes that need to communicate. When a source node have data packets to send at the destination but have no required routing information in its route table then the source node initiates the route discovery process.

A. Control Messages in AODV

- Route Request Message
- Route Reply Message
- Route error Message (RERR) and HELLO Messages are used for discovery and breakage of route.

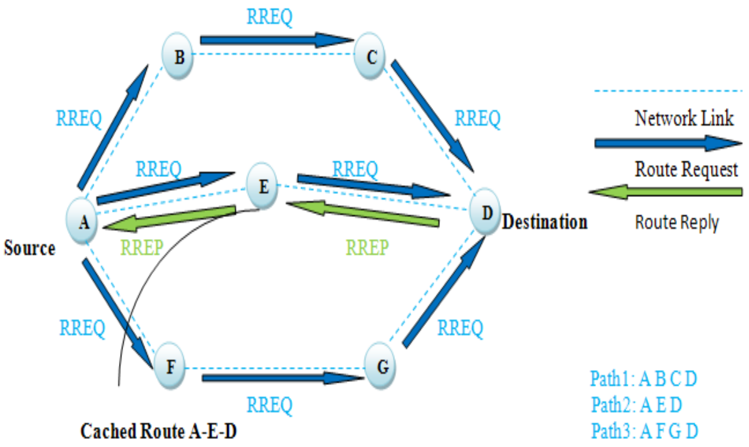

Fig.8 a possible path for a route replies if A wishes to find a route to D

Consider A wants to send a data packet to node D; it checks its route table to determine whether it has a route to D. If A has a route to D, then A forwards the packet to the next-hop node toward D. If A does not have a route to D, it initiates route discovery. Node A floods a Route Request (RREQ) message, which contains source address, destination address, source sequence number, destination sequence number and broadcast ID and hop count.

Table 1 RREQ Fields

source address	broadcast ID	Source sequence no.	destination address	destination sequence no.	Hop count

After sending the RREQ message, A sets a timer to wait for a reply. If a node receives a route request that has the same source address and request id field's as those in one of the previous route request packets, it discards the packet. Otherwise it checks if there is an entry in its routing table for the destination address.

If a node has a route for a destination in its routing table, and if it cannot reach the destination through that route, it increments the destination sequence number and sends a route request. Therefore, the destination sequence number indicates the freshness of a route. If a router has an entry for the destination in its table, and the sequence number for the request is smaller than the sequence number for the destination in its table, this means the route known by the router is fresher than the one known by the router that sends the request. In this case the receiver sends a route reply (RREP). The RREP is forwarded back to the source node through the route where the request is received [6].

B. Sinkhole Attack in AODV

When a node forwards the RREQ control packet to the destination, a node automatically sets up the reverse path from all nodes back to the source. It records the address of every neighbor which takes part in route and which received the first copy of RREQ [4, 6]. A malicious node may send RREP messages for every RREQ and make the other nodes forward their packets towards it. It may then sink the incoming packets, forward them to another route or gain unauthorized access to their contents. The basic AODV does not provide any security mechanisms which results in severe problems [1].

- ***Subverted:*** A node may become subverted when a malicious node forced it to violate the routing protocol in operation.
- ***Unauthorized:*** A node may become unauthorized when a malicious node tries to take part in communication and makes the network complicated.
- ***Subverted links:*** A links become subverted links when a malicious node gains access to the links between nodes and starts manipulating them.

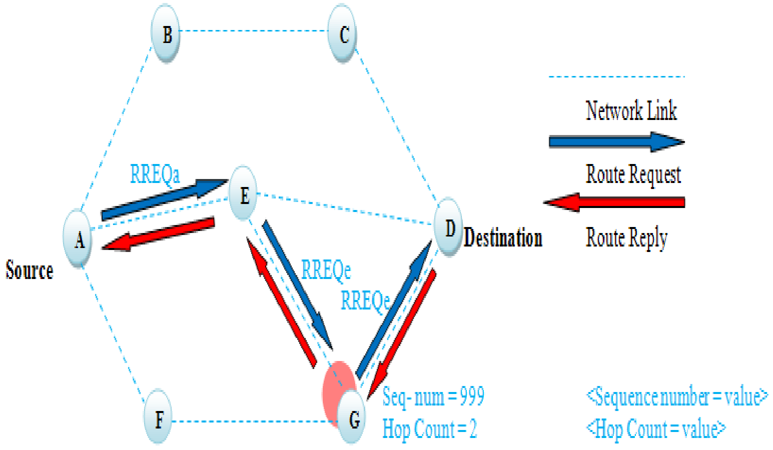

Fig.9 Sinkhole attack in AODV

In the given diagram it shows the compromised node G which looks like other node, become malicious node and advertize itself. The node G sends greater sequence number to node E to misguide that it is fresh route. It also sends lesser hop count value to tell this is shortest path. Node E assumes that the route through G is the shortest route and starts sending data packets to the destination through it. In an AODV protocol, there are two types of messages transfer or receive among the nodes from source to destination.

III. SECURITY-AWARE ROUTING (SAR)

The SAR protocol helps to overcome from the problems occur due to Sinkhole attacks in AODV and DSR protocols. In the security-aware routing protocol, the security measures are embedded in RREQ packet. When the node receives RREQ it verifies whether it is capable to provide desired security features [1]. If it is, the packet is forwarded to the next hop, otherwise packet is dropped. Upon finding the secure path, any node in path can create a RREP and sends back to source node. SAR provides two security metrics.

- *Trust hierarchy* SAR supports hierarchy of trust levels among various available routes.
- *Security Capabilities* it deals with ability to handle various security features such as encryption, decryption, digital signatures etc.

In routing protocols, mainly two types of messages are exchanged between various nodes. They are:

(1) Routing messages that are forwarded to the neighboring nodes.
(2) Routing updates messages forwarded to the remote nodes, including all neighbors.

The SAR provides Solutions in order to handle the problems related to sinkhole attack in DSR and AODV are:

- *Routing message protection:* the routing message includes both digital signature and sequence numbers. As sequence number is included in each routing message. It is initialized to zero at starting and is incremented every time when source send message. Digital signature provides the facility by which sender sign each message that helps to maintain the integrity and authentication of message [1]. The message is dropped if it is corrupted.
- *Routing update protection:* when a source node updates the routing information for a specific destination than the updates is sent to each node in that particular path.

IV. CONCLUSION

The Structure wireless ad hoc network is a decentralized type having no fixed administrative approach. Due to this approach wireless ad hoc are vulnerable to many active and passive attacks. In this paper we discuss about how sinkhole attack causes problem in on-going communication between different nodes. The security of wireless ad hoc network can be enhanced by using different approach such as Security-aware routing (SAR) which applicable in both DSR and AODV routing protocols

V. ACKNOWLEDGEMENT

We are grateful to Shaheed Bhagat Singh College of Engineering & Technology, Ferozepur (India) for providing continuous support throughout the work.

References

[1] Amitabh Mishra, “SECURITY AND QUALITY OF SERVICE IN AD HOC WIRELESS NETWORKS”, ISBN- 13 978-0-521-87824-1 Handbook.

[2] Amit N. Thakare, Mrs. M. Y. Joshi, “Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks”, IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, 2010

[3] Ad hoc network specific attacks held by Adam Burg.

[4] D. Sheela, Nirmala. S, Sangita Nath and Dr. G Mahadevan, “A Recent Technique to Detect Sinkhole Attacks in WSN”.

[5] Kisung Kim and Sehun Kim, “A Sinkhole Detection Method based on Incremental Learning in Wireless Ad Hoc Networks”.

[6] The Handbook of Ad Hoc Wireless Networks, Mohammad Ilyas.

[7] Satyendra Singh, Vinod Kumar Yadav, Ganesh Chandra, & Rahul Kumar Gangwar, “ An Efficient and Improving the Security of AODV Routing Protocol” IJCST Vol. 3, Issue 1, Jan. - March 2012.

[8] C. Siva Ram Murthy and B. S. Manoj, “Ad Hoc Wireless Networks: Architectures and Protocols”.

[9] PRADIP M. JAWANDHIYA & MANGESH M. GHONGE, “A Survey of Mobile Ad Hoc Network Attacks”, International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071.

[10] K.P.Manikandan, Dr.R.Satyaprasad & Dr.Rajasekhararao, “Analysis and Diminution of Security Attacks on Mobile Ad hoc Network”, IJCA Special Issue on “Mobile Ad-hoc Networks “MANETs, 2010.

[11] Erdal Çayırcı & Chunming Rong, “Security in Wireless Ad Hoc and Sensor Networks”.

[12] Wenjia Li and Anupam Joshi, “Security Issues in Mobile Ad Hoc Networks- A Survey”.

[13] David B. Johnson &David A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks”.