Volume 2, Issue 4, April 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Detection of Sinkhole Attack against DSR Protocol MANET

Ms. Sonal R. Jathe *,Prof. D.M. Dakhane
Sipna's College of Engg & Tech Amravati (MS) INDIA
Sonal_jathe@rediffmail.com

Abstract— **A wireless ad hoc network is a temporary network set up by wireless nodes usually moving randomly and communicating without a network infrastructure. Due to security vulnerabilities of the routing protocols, however, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. In this study we investigated the effects of Sinkhole attacks on the network performance. And detection of nodes that behaves as like Sinkhole against the DSR Protocol MANET. And comparison between the performance with DSR protocol with no malicious nodes and with sinkhole nodes in DSR MANET. The network performance in the presence of a Sinkhole is reduced up to 32%.**

***Keywords*— MANET, DSR, routing, Security, Sinkhole attack**

I. INTRODUCTION

An autonomous system of mobile hosts connected by wireless links, often called *Mobile Ad hoc Networks* (MANETs)

A. Characteristics of MANET

1. No fixed infrastructure
2. Dynamic changing topology
   -Mobile devices join/leave the network unexpectedly; they can also move freely
3. Energy-constrained
4. Limited bandwidth
5. Each node also serves as router
   -Help to relay packets received from neighbours
6. Interoperation with the Internet

Security is an essential requirement in mobile ad hoc network (MANETs). Compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. Attacks on ad hoc networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not.

Security requirements

1. *Availability*
2. Authorization and Key Management
3. Data *Confidentiality*
4. Data *Integrity*
5. Non-repudiation

Security Solution Constraints

- Lightweight
- Decentralized
- Reactive
- Fault-tolerant

Challenges:

1. No infrastructure
2. Peer-to-peer architecture with multi-hop routing
3. Mobile device physical vulnerability
4. Stringent resource constraints
5. Wireless medium
6. Node mobility

This paper analyses One type of Sinkhole Attack the Sinkhole Attack that can easily be employed against MANET Routing Protocol. This paper focuses on detecting the sinkhole attacker on dynamic source routing (DSR) Protocol effectively. The sinkhole attack, a malicious node in MANET advertises wrong routing information, such as advertising itself as being on the way to specific nodes, so receives the whole traffics in local network. Then it modifies the data packets or drops them to make the network complicated.

In the rest of Paper is organized as follows. In Section 2, DSR Protocol in MANET we see the performance measures of DSR Protocol with no malicious nodes and in Section 3, Sinkhole attack are described and we also see the performance of DSR Protocol with Sinkhole nodes. In Section 4, we see the performance comparison between the DSR Protocol and DSR with Sinkhole nodes. We make the Conclusion in Section 5.

II DYNAMIC SOURCE ROUTING

'Dynamic Source Routing' (DSR) is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. However, it uses source routing instead of relying on the routing table at each intermediate device.

Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse. This may result in high overhead for long paths or large addresses, like IPv6. To avoid using source routing, DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis.

This protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node (route record which is initially contained in Route Request would be inserted into the Route Reply).To return the Route Reply, the destination node must have a route to the source node. If the route is in the Destination Node's route cache, the route would be used. Otherwise, the node will reverse the route based on the route record in the Route Reply message header (this requires that all links are symmetric). In the event of fatal transmission, the Route Maintenance Phase is initiated whereby the Route Error packets are generated at a node. The erroneous hop will be removed from the node's route cache; all routes containing the hop are truncated at that point. Again, the Route Discovery Phase is initiated to determine the most viable route.For information on other similar protocols, see the ad hoc routing protocol list.

Dynamic source routing protocol (DSR) is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The major difference between this and the other on-demand routing protocols is that it is beacon-less and hence does not require periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbors of its presence. The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding RouteRequest packets in the network. The destination node, on receiving a RouteRequest packet, responds by sending a RouteReply packet back to the source, which carries the route traversed by the RouteRequest packet received.

Consider a source node that does not have a route to the destination. When it has data packets to be sent to that destination, it initiates a RouteRequest packet. This RouteRequest is flooded throughout the network. Each node, upon receiving a RouteRequest packet, rebroadcasts the packet to its neighbors if it has not forwarded it already, provided that the node is not the destination node and that the packet's time to live (TTL) counter has not been exceeded. Each RouteRequest carries a sequence number generated by the source node and the path it has traversed. A node, upon receiving a RouteRequest packet, checks the sequence number on the packet before forwarding it. The packet is forwarded only if it is not a duplicate RouteRequest. The sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions of the same RouteRequest by an intermediate node that receives it through multiple paths. Thus, all nodes except the destination forward a RouteRequest packet during the route construction phase. A destination node, after receiving the first RouteRequest packet, replies to the source node through the reverse path the RouteRequest packet had traversed. Nodes can also learn about the neighboring routes traversed by data packets if operated in the promiscuous mode (the mode of operation in which a node can receive the packets that are neither broadcast nor addressed to itself). This route cache is also used during the route construction phase. If an intermediate node receiving a RouteRequest has a route to the destination node in its route cache, then it replies to the source node by sending a RouteReply with the entire route information from the source node to the destination node.

Advantages and Disadvantages :

This protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. In a reactive (on-demand) approach such as this, a route is established only when it is required and hence the need to find routes to all other nodes in the network as required by the table-driven approach is eliminated. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead. The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length

III **DYNAMIC SOURCE ROUTING AND SINKHOLE ATTACK**

DSR is one of the most widely used reactive protocols in ad-hoc networks. DSR uses two kinds of messages known as RREQ – Route Request and RREP – Route Reply for route discovery process. The following figure (Fig.1) depicts the sequence of operations in route discovery. DSR uses the

RREQ message if and only if there are no routes available in the route cache to reach the destination. DSR starts the route discovery by sending Route Request (RREQ) packet. The Fig.2 shows the propagation of RREQ packets. The RREQ will be uniquely identified by the sequence number, source id and destination id. Node A initiates the route discovery by broadcasting the RREQ message. Each node will then add their id to the route and broadcasts it again. The nodes B, C, D are intermediate nodes and they do not have any source route to reach the node 8, which is the intended destination. The intermediate node which has the route to the destination will send a Route Reply (RREP) and if no intermediate node has the information, the RREQ will be propagated to the destination. The Fig.3 depicts the RREP propagation from the destination node E to the source node A. Bogus RREQ will be used to carry out the sinkhole attack. If the bogus RREQ has higher sequence number than the sequence number of the original RREQ from the target node, the intermediate nodes will treat the bogus one as the latest request and discard the original one. Fig.4 depicts the propagation of bogus RREQ message from node A with the sequence number 888 and the target as D. By doing this, the sinkhole nodes can draw the network traffic towards them. This can cause node failure because of the higher power consumption and the network may fail because of the heavy congestion in a particular route. So, it is imperative to detect the sinkhole nodes as early as possible and detach them from the MANET.

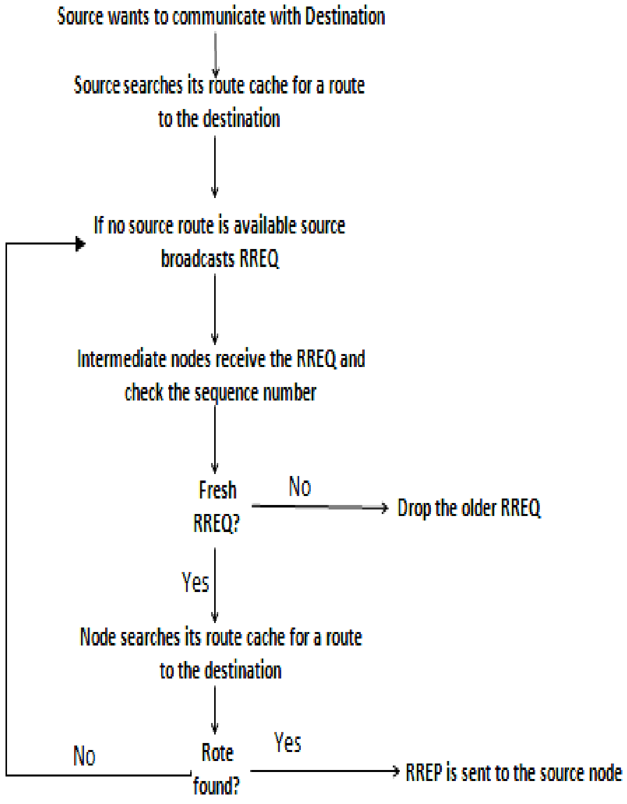
Source wants to communicate with Destination
Source searches its route cache for a route to the destination
If no source route is available source broadcasts RREQ
Intermediate nodes receive the RREQ and check the sequence number
Fresh RREQ?
No
Drop the older RREQ
Yes
Node searches its route cache for a route to the destination
No
Rote found?
Yes
RREP is sent to the source node

Figure 1. Route Discovery Process

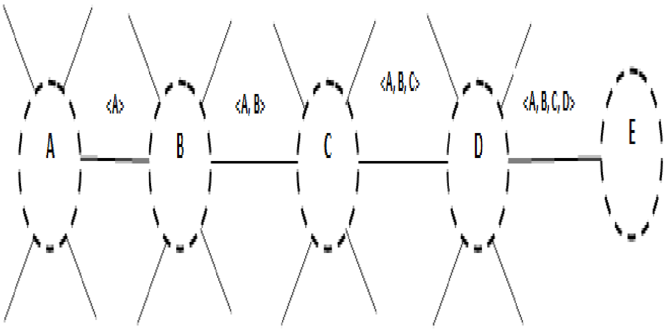

Figure 2. Propagation of RREQ

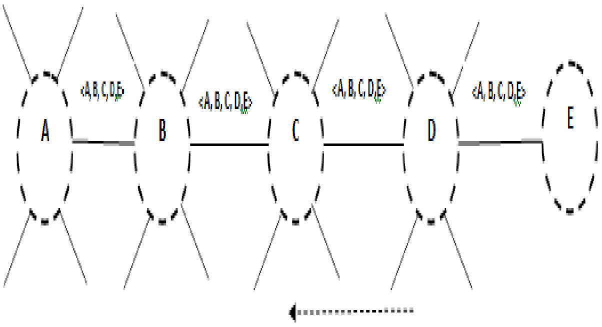

Figure 3. Propagation of RREP

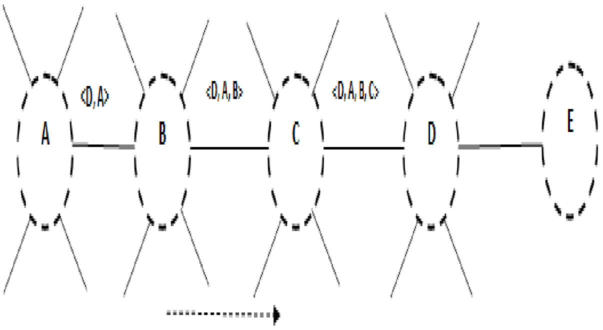

Figure 4. Bogus RREQ from node A

Our approach uses the mutual understanding among the nodes in order to detect the malicious nodes. This approach is based on the DSR protocol. The RREQ will consist of source id, destination id, sequence number and source route. A sequence number indicates the freshness of the RREQ. The sequence number of the nodes will be strictly increasing monotonically. In other words, each different packet will have different sequence numbers. The sinkhole node appends its id on the source route and broadcasts the bogus RREQs. The sinkhole attack increases network overhead, decreases the network's lifetime. Our proposed approach uses the advantages of the cooperative technique as well as the discontinuity in the sequence number. We are using four different types of messages during the detection process. A value known as 'peak' value will be selected based on the scalability of the network. The peak value will be the threshold of the discontinuity in sequence numbers. Whenever a node receives any RREQ message, it will calculate the peak value by comparing the sequence number of the current RREQ with the previously received message from the same source. The nodes will send a Message if the discontinuity in sequence number is greater than peak value. The Message will contain the source route and the sequence number of the bogus RREQ message. On the other hand, if the attacker is so intelligent, the attack cannot be detected using the peak value. In this case, the second part of the algorithm begins. The target node will send the Attack Information Message to the network. The next step will be the generation of the Path Information Message (PIM). These messages contain the path of the sinkhole node. This path will be a reduced set when compared to the path in the Attack Information Message. The path in the PIM massage will be different from different sources. The final step will be the broadcasting of the message will confirm the sinkhole node.

IV PERFORMANCE COMPARISON BETWEEN DSR AND DSR WITH SINKHOLE:

Packet delivery ratio

Nodes	10	20	30
DSR	99.035	98.969	98.695
Sinkhole	32.827	69.238	58.993

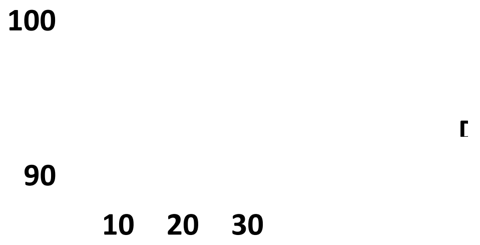

Figure 5. No of Nodes

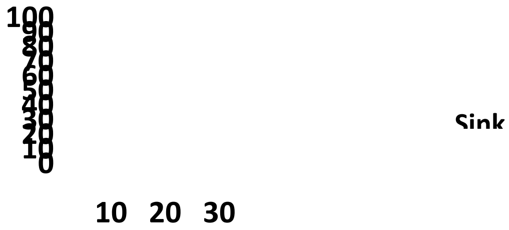

Figure 6..No of Nodes

V CONCLUSION

In this paper we see the introduction about MANET means various challenges in MANET, Security requirements , Security solution Constraints as security is main issue in MANET. Many routing protocols are vulnerable to attack because of its infrastrucureless characteristics and wireless medium, one such attack is Sinkhole attack in which a malicious node in MANET advertises a wrong routing information, such as advertising itself as being on the way to specific nodes, We also discuss the DSR protocol in deep and Sinkhole attack is analyzed against the DSR Protocol MANET. We also see the Performance Comparison between DSR protocol with no malicious nodes and the DSR Protocol With the sinkhole nodes

REFERENCES

[1] Kisung Kim and Sehun Kim" A Sinkhole Detection Method based on Incremental Learning in Wireless Ad Hoc Networks".

[2] H. C. Tseng, B. J. Culpepper, "Sinkhole intrusion in mobile ad hoc networks: The problem and some detection indicators",

[3] David B. Johnson and David A. Maltz. Dynamic source routing in ad hoc wireless networks. Technical report, Carnegie Mellon University, 1996.

[4] Lee kang hyen, "Detecting Inner Attackers and Colluded nodes in Wireless Sensor Networks Using Hop-depth algorithm", IEEK journal vol 44-1, pp.113-121, 2007.

[5] Satoshi Kurosawa, et al "A Self-adaptive Intrusion Detection Method for AODV-based Mobile Ad Hoc Networks" Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on

[6] H. Ebbinghaus, Memory : A contribution to experimental psychology, Teachers College Press,1913.

[7] Y. an Huang, and W. Lee, "Attack Analysis and Detection for Ad Hoc Routing Protocols," the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125–145,French Riviera, Sept. 2004.

[8] C.Siva Ram Murthy and B.S.Manoj. Ad Hoc Wireless Networks Architectures and Protocols. PRENTICE HALL, 2004.

[9]Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Communications Magazine, October 2002, pages 70-75.

[10] Douglas S. J. De Couto, Daniel Aguayo, John Bicket and Robert Morris, "A High-Throughput Path Metric for Multi-Hop Wireless Routing," in *Proceedings of the Ninth Annual International Conference on Mobile Computing and Networking (MobiCom '03)*, San Diego, California, September 2003.

[11] Benjamin J. Culpepper and H. Chris Tseng, "Sinkhole Attack Detection in DSR MANETs: A Fuzzy Logic Approach," *Technical Report No. 200303*, Computational Intelligence Lab., SJSU, 2003.

[12] Yongguang Zhang and Wenke Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," In *6th International*

Conference on Mobile Computing and Networking (MOBICOM'00), pp275-283, June 2000.

[13] Elizabeth M. Royer and Chai Keong Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," In *IEEE Personal Communications*, Volume 6, pp46-55, April 1999.