E-ISSN: 2321–9637
Volume 1, Issue 4, November 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

PERFORMANCE ANALYSIS OF DSR PROTOCOL UNDER SINKHOLE ATTACK IN MANETs

Anuprita Gawande[1]
Datta Meghe College Of Engg.& Technology,Airoli.
anushri_01@rediffmail.com

Dr.D.J.Pethe
Datta Meghe College Of Engg.& Technology,Airoli.

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 paper, we investigated the effects of Sinkhole attacks on the dynamic source routing protocol by considering different performance metric. The simulation results show the effectiveness of sinkhole attack on DSR protocol.

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

1. INTRODUCTION

A mobile ad hoc network is a self-configuring wireless network of mobile nodes. The mobility of the nodes is independent of each other. MANETs do not have any controlling point to regulate the traffic. Each node in the MANET has to take care of the routing aspects as well. There are many routing protocols available for routing in ad-hoc networks. The routing protocols for MANETs are broadly classified into two types as proactive and reactive. The protocols like DSDV, OLSR, OSPF, are proactive protocols which will use periodic messages in order to know the network topology. The reactive protocols include AODV, DSR. [8]. Because of the infrastructure-less nature and having dynamically changing topologies, MANETs are vulnerable to many kinds of failures and attacks. Most of the attacks in MANETs target the routing protocols. The mobility of nodes makes it more vulnerable to routing protocol attacks. By attacking the routing protocols, the attackers can absorb network traffic or inject themselves into the path between the source and destination. Some latest attacks on the routing protocol in MANETs are, wormhole attack, black hole attack, grey-hole attack, byzantine attack, rushing attack [7] [9] [12]. A sinkhole attack often sets the stage for other attacks by modifying routing to improve an attacker's ability to modify packets - the routing changes often place the attacker in a position where he can receive pertinent data [3]. It is important to detect the sinkhole nodes and prune them from the MANET.

2. 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.

E-ISSN: 2321–9637
Volume 1, Issue 4, November 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

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.

3. SINKHOLE ATTACK

Sinkhole attack, a sinkhole node tries to attract the data to itself from all neighboring nodes. It generates fake routing information that let the nodes in local network know itself on the way to specific nodes. Through this procedure, sinkhole node attempts to draw all network traffic to itself. Thereafter it alters the data packet or

E-ISSN: 2321–9637
Volume 1, Issue 4, November 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

drops the packet silently. Sinkhole attack increases network overhead, decreases network's life time by boosting energy consumption, finally destroy the network[4]. In DSR protocol, sinkhole attack is set up by modifying sequence number in RREQ. Sequence number used to prevent loop formations indicates the recency of the route. The higher sequence number, the more recent route the packet contains. Sinkhole node selects the source, destination node. It observes the source node's sequence number carefully, and generates bogus RREQ with selected source, destination and higher sequence number than observed source sequence number. It adds itself on the source route and broadcasts the bogus RREQ. Nodes that take this bogus RREQ recognize that the reversed route could be a better route to the source than incumbent route. Figure 1 shows the generation of the bogus RREQ packet. Sinkhole node 2 makes the bogus RREQ which looks as if it is originated by node 0. Sequence number of bogus packet is 999, much higher than original source's, 6. Intermediate nodes on route learn that node 2 is on one hop distance to node 0 and to send packet to node 0, the data packet may go through the node 2. Sinkhole node 2 can easily repeat this procedure; draw all local network traffic to itself. Thereafter node 2 can do malicious acts including dropping, modifying the traffic.

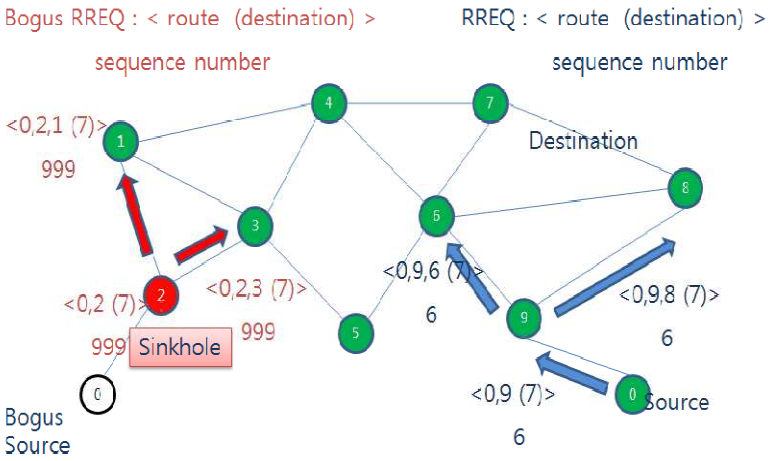

Figure 1. The generation of Bogus RREQ [1]

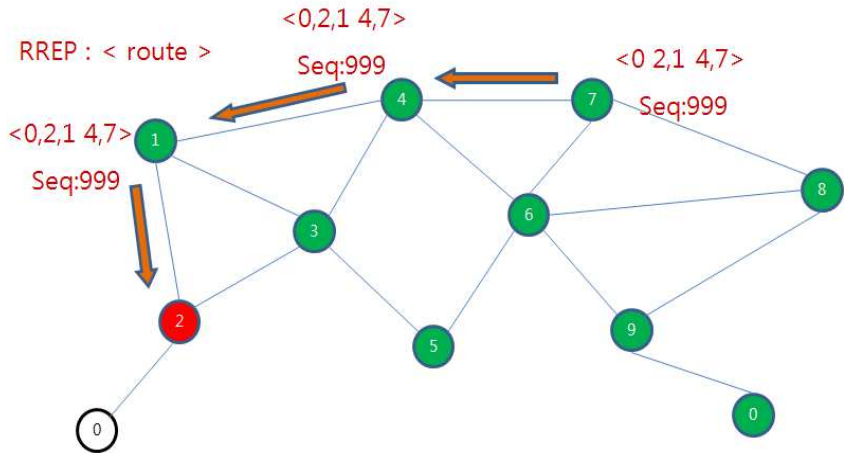

Figure 2. Bogus RREP propagation [1]

E-ISSN: 2321–9637
Volume 1, Issue 4, November 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

4. SIMULATION OF DSR UNDER SINKHOLE ATTACK

For simulation, we set the parameter as shown in Table 1. Random Waypoint Model (RWP) [1] is used as the mobility model of each node. In this model, each node chooses a random destination within the simulation area and a node moves to this destination with a random velocity. The simulation is done using Network Simulator 2 to analyze the performance of the network by varying the nodes mobility. The metrics used to evaluate the performance are given below.

Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.

Average End-to-End Delay: This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc. It is measured in milliseconds.

Table: 1 Simulation Parameters

Simulator	Ns-2(version 2.32)
Simulation Time	100 (s)
Number of Mobile Nodes	20
Topology	750 * 750 (m)
Routing Protocol	DSR
Traffic	Constant Bit Rate (CBR)
Pause Time	10 (m/s)
Max Speed	0,1,2,3,4

Fig. 3 shows the effect of Packet Delivery Ratio for DSR protocol. The result shows the cases, with sinkhole and without sinkhole attack on DSR. It has been measured that Packet Delivery Ratio decreases with sinkhole nodes in the wireless network on DSR routing protocol as compared to without sinkhole nodes. Also Fig 4 and 5 shows the effect of sinkhole attack on packet delivery ratio and end to end delay when we varied mobility speed of nodes.

E-ISSN: 2321–9637
Volume 1, Issue 4, November 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

Figure 3. Packet Delivery Ratio of Normal DSR Vs Sinkhole attack DSR

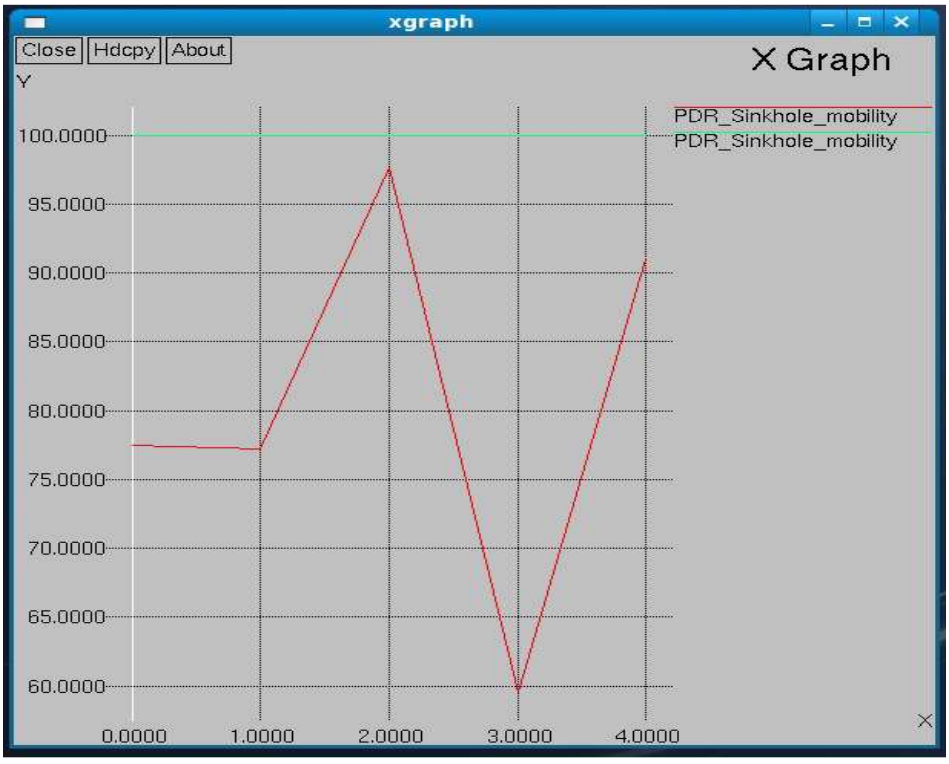

Figure 4. Packet Delivery Ratio of Normal DSR Vs Sinkhole attack DSR with varying speed

E-ISSN: 2321–9637
Volume 1, Issue 4, November 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

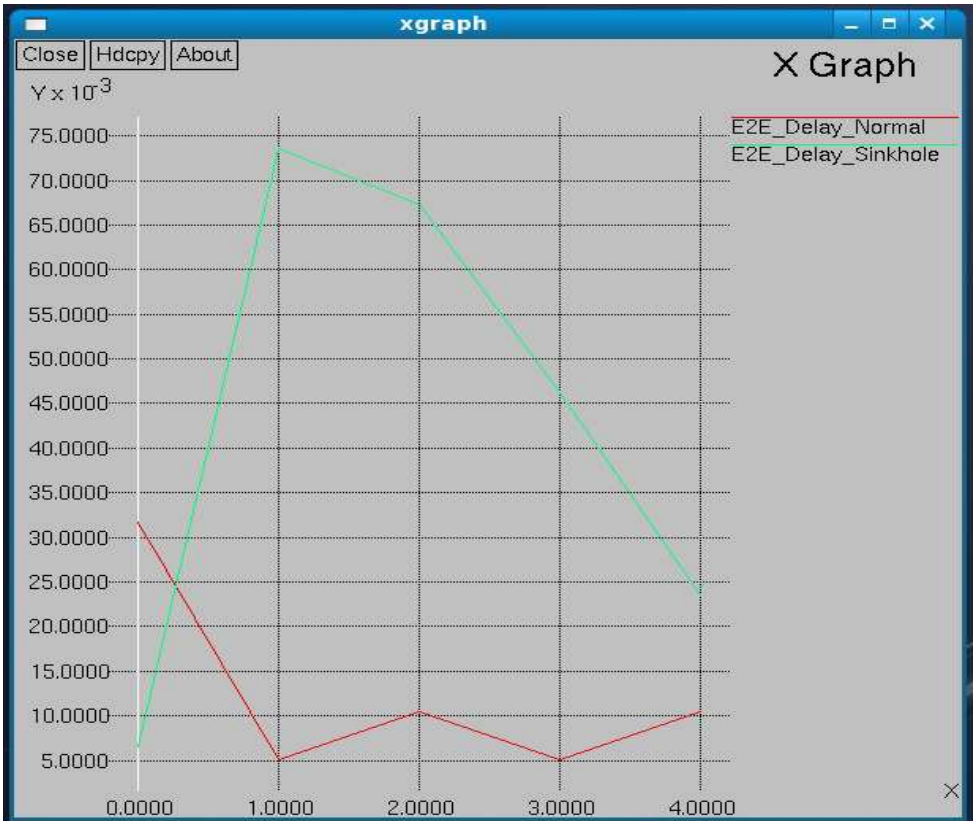

Figure 5. End to End delay of Normal DSR Vs Sinkhole attack DSR with varying speed

CONCLUSION

Sinkhole attack is one of the most important security problems in MANET. It is an attack that a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In this paper, we have analyzed the effect of sinkhole attack on DSR protocol. The result shows significant degradation in performance of dynamic source routing protocol (DSR) under sinkhole attack.

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. Cu lpepper, ―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 algorith m‖, 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] M. M. Ghonge, "A Survey of Mobile Ad Hoc Network Attacks," International Journal of Engineering Science and Technology (IJEST) Vol. 2(9), 2010, 4063-4071.ISSN: 0975–5462 (online version) September 2010.(Impact factor: 1.85, Cited by 15)
[8] 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.
[9] C.Siva Ram Murthy and B.S.Manoj. Ad Hoc Wireless Networks Architectures and Protocols. PRENTICE HALL, 2004.

E-ISSN: 2321–9637
Volume 1, Issue 4, November 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

[10] Hong mei Deng, Wei Li, and Dharma P. Agra wal, ― Routing Security in Wireless Ad Hoc Netwo rks,‖ IEEE Communicat ions Magazine, October 2002, pages 70-75.
[11] Douglas S. J. De Couto, Daniel Aguayo, John Bicket and Robert Morris, ―A High-Throughput Path Metric for Mult i- Hop Wireless Routing,‖ in *Proceedings of the Ninth Annual International Conference on Mobile Computing and Networking (MobiCom '03)*, San Diego, California, September 2003.
[12] M. M. Ghonge, "Countermeasures of Network Layer Attacks in MANETs," International Journal of Computer Application (IJCA), Special Volume on Cryptography & Network Security 2011, ISSN: 2229-5208 December 2011.
[13] 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.