Mohammed Ashfaq Hussain, Dr. A. Francis Saviour Devaraj / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 2, March -April 2013, pp.1737-1741

Upshot of Sinkhole Attack in DSR Routing Protocol Based MANET

Mohammed Ashfaq Hussain
Scholar, Department of Information Science & Engineering, The Oxford College of Engineering Bangalore, India

Dr. A. Francis Saviour Devaraj
Professor, Department of Information Science & Engineering, The Oxford College of Engineering Bangalore, India

Abstract

Mobile Ad-hoc Network (MANET) is a kind of wireless network which has no infrastructure and is a self configuring wireless network of mobile nodes, each node on the MANET will act like a router which forwards the packets. Due to these properties MANET is vulnerable to attacks. Most common of them is routing attack. Sinkhole attack is a kind of routing attack launched by a malicious node on MANET. A sinkhole node tries to attract all the network packets to it-self from all neighboring nodes. Sinkhole node does this by luring itself as a better route to reach the destination. Further it may launch other severe routing attacks like black hole or selective forwarding attack. This paper studies the characteristics of sinkhole attack and how it will affect the performance of the Distance Vector Routing (DSR) Routing protocol. The implementation is done using NS2 as the simulator.

Index Terms— MANET, Sinkhole attack, DSR, NS2 simulator.

I. INTRODUCTION

MANET operates in absence of a centralized administration. Nodes on the Adhoc network communicate with each other and are highly mobile resulting in a dynamic topology. The challenges of MANET [1] are security, battery backup of mobile nodes, bandwidth utilization and slower data transfer rates. The routing protocols for MANET are classified as proactive and reactive protocols. DSR [2] is classified as on-demand reactive routing protocol because it initiates route discovery only when it is needed. It is based on source routing, it maintains a route cache at each node and the route is maintained on a node until it is required or the destination is unreachable.

The possible type of attacks [3] on MANET, are active and passive attacks. Monitoring and listing to the communication channel by unauthorized nodes is categorized as a passive attack. Whereas, active attacks are those in which a malicious node monitors, listens, modifies the packets or add new packets on the network. Sinkhole attack is an active routing attack, as it is performed on the network layer.

A sinkhole node tries to lure nearly all the network traffic towards it. Sinkhole attack [4] will be launched by making the compromised node look attractive and better intermediate node to reach the destination from source node on the network with respect to routing metric. This will be done either by introducing new bogus routing packets on the network or by changing the content of the genuine packets. After performing the attack, it may drop the packets [5] or launch some other severe attacks.

The scope of this paper is to delve into the sinkhole attack behavior and its impact on the performance of Dynamic Source Routing (DSR) routing protocol using ns2 [6] network simulator. Rest of the paper is organized as follows, Section 2 reviews the related work done to study sinkhole attack on MANET, Section 3 describes how Sinkhole attack is launched on MANET, Section 4 deals with simulation study of sinkhole attack in DSR, its result analysis and section 5 explains the conclusion and future work.

II. RELATED WORK

In [1], the different characteristics of the DSR protocol like reactive on-demand routing, route discovery mechanism are discussed. This helps to properly understand the working of DSR and how a sinkhole attack can be launched over it. Simulation of DSR is done using NS2 and the results are studied to show the working of the DSR protocol on MANET.

MANET is very much vulnerable to attacks. Sinkhole is a severe attack launched on MANET. Security Aware Routing (SAR) [4] helps to reduce the impact of these kind of attacks and this is called as Secure-DSR (S-DSR). In secure-DSR routing packets are signed digitally to provide integrity and authentication for the routing messages. The performance of both are compared, simulation is done [13] using NS2 based on parameters like packet drop, delay and delivery ratio. Analysing the results show that, S-DSR performs well compared to normal DSR. These parameters are useful to study the impact of sinkhole of DSR.

DSR allows the network to be completely self configuring [6], DSR protocol can be implemented in NS2 simulator using DSR MANET

draft in simulator environment. NS2 is event driven and runs in non real fashion. MANET topology with DSR protocol can be easily created. This paper helps to see how DSR can be simulated in the NS2 and analyzing the generated trace file.

In [7], comparative study between the DSR and AODV protocols of MANET is done based on parameters like throughput, average end-to-end delay, packet loss [9], packet delivery percentage, normalized routing load, average jitter. This can be efficiently used to understand the effect of sinkhole.

Mobile Ad hoc networks suffer from more kind of attacks. In [10], studies the detail behavior of the sinkhole attack. An architecture has been defined to effectively analyze this attack on MANET. Various performance metrics and attributes like packet delivery, delay calculation has been considered to understand the effect of this attack. The simulation and evaluation of the results have been done using NS2.

In [14] the behavior of AODV protocol in the presence of a Blackhole attack is discussed. The sinkhole node can further act as a Blackhole and its effect are studied carefully with the help of parameters like throughput, packet delivery and delay are studied which can be considered for sinkhole study as well.

III. LAUNCHING SINKHOLE ATTACK ON MANET

Dynamic source routing (DSR) [1] is an on-demand/ reactive routing protocol where the nodes on the network utilizes the source routing mechanism. The source node adds the routes that have to be taken by each packet after the route discovery. This route information is stored on a cache memory of the nodes. To discover a route, the source node that needs to send the packet to the destination node floods a Route Request (RREQ) [2] message. The RREQ has sender's address, destination address and a unique sequence ID determined by the sender. Whenever the RREQ reaches a neighbouring node they will check their cache memory for a route to destination. If there is a route to the destination or if this node is the target (destination) node they will append their ID and send Route Reply (RREP) message back to the source node in the reverse path followed by the RREQ. If the node is not the destination node [7] then it will append its ID in the RREQ and forwards this to its neighbouring nodes. After this route discovery process, the source will append the whole path in the other packets and send it to the destination.

Sinkhole attack is one of the most severe attacks on mobile Ad-hoc networks [5].In sinkhole attack, the compromised node or the malicious node will advertise the wrong routing information to the other nodes so as to make it as specific node and attracts [10] the whole network traffic towards it. Figure 1 Shows a MANET with a sinkhole.

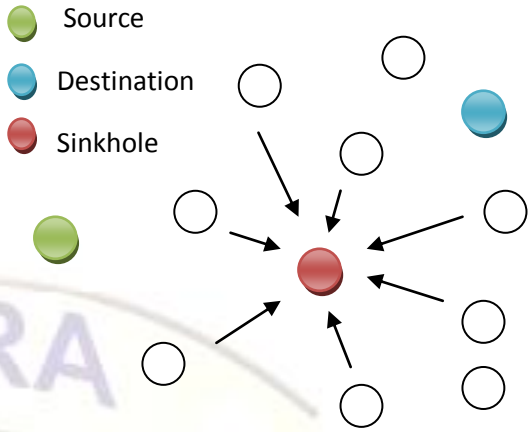

Figure 1. Manet topology with sinkhole

In DSR protocol, Sinkhole attack affects the performance of the DSR routing by using the flaws like sequence number. The sinkhole node modifies the sequence number [4] in the RREQ packet and modifies the value with a higher value so that it will be treated as a fresh route (updated route) to the destination node. The malicious node keenly observes the source node's RREQ packet and its sequence number and it then generates a bogus RREQ with higher sequence value and broadcasts it to the neighbouring nodes. The neighbouring nodes upon receiving this bogus RREQ, assume that it is a better route and updates this route in their cache and broadcasts it to the destination node. The destination node will generate a RREP for this bogus RREQ and sends it to the source node. Thus a route is established and the packets are lured towards the sinkhole node.

Instead of creating the bogus RREQ [8] the sinkhole can also modify the RREQ received from the source node adding itself in the route and sending back a RREP to source projecting that it has better route to the destination. The sinkhole may either modify or extract the data from the attracted packets or may simply drop the packets; also it may launch some other attacks. This affects the performance of the MANET.

IV. STUDYING THE SIMULATION RESULTS

A. scope of study

In order to do the simulation study for this paper, a MANET is created, the protocol used is DSR and then a sinkhole node is configured on MANET. To create the sinkhole node on the network, Bogus Route Requests (BRREQ) is used. This Bogus Route Request (BRREQ) is broadcasted by the malicious nodes. The sequence number is increased and also the hop count is minimized in the packet so that it's route will be accepted by the other nodes and the route remains for a longer time. Figure 2 Shows the exchange the bogus RREQ

(BRREQ) packets between the nodes to create the sinkhole.

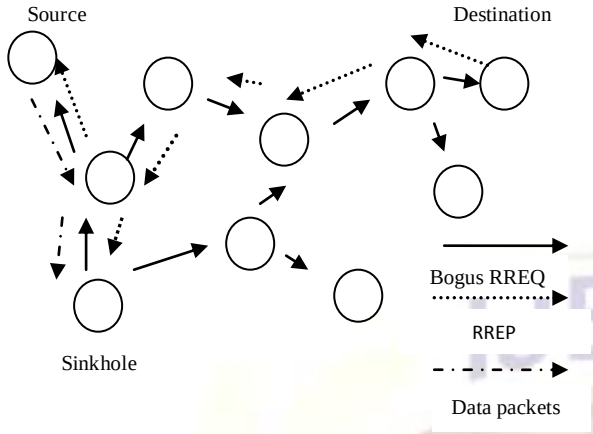

Figure 2. Sending bogus packet and attacking packets

The implementation properties of the sinkhole are provided by modifying the code present in protocol implementation files dsr.cc and dsr.h files. Sinkhole node and dropper agents are created and these are attached to the nodes which have to act as a malicious node. It is done using the front end TCL language used in NS2. The method for creating the bogus RREQ request_fake_send() is written in dsr.cc and called as agent by the malicious node.

B. Simulation parameters

The table 1 shown below is the set of parameters used in the simulation environment. These parameters are configured in the NS2 simulator, with the area of 1200 meters both along x and the y axis with 50 mobile nodes in it, simulating it for 25 seconds, there are 5 connections on the network and 3 sinkhole nodes that operates to attack the network. Random waypoint mobility model [12, 15] is used, as it is efficient method to provide mobility to nodes in simulating MANET in NS2.

Table 1. Parameters used for simulation

PARAMETER	VALUE
Area	1200 m * 1200m
Simulation Time	25 seconds
Number of nodes	50
Traffic Model	CBR
Mobility model	Random Way Point
Number of sinkhole nodes	3
Number of connections	5
Mac protocol	802.11
Data rate	2 Mbps
Data Packets	512bytes/packet

C. Simulation results analysis

To study the effect of sinkhole attack on DSR protocol, the following network parameters like throughput, packet drop and packet delivery ratio are analyzed without the sinkhole on the network and with the sinkhole nodes present on MANET.

Network throughput

Throughput is the total number of packets received by the destination node over a period of time and the metric used to calculate the throughput is kbps. In Figure 3 simulation results are compared; it is clear from the graph that as the time for simulation increases the throughput decreases. The reason is sinkhole has access to more packets on the network and sinkhole will not allow the packets to reach the destination and hence the throughput decreases.

In Table 2, the throughput is compared between the normal DSR and DSR in the presence of the attack. The values show that there is a decrease in the throughput, which are shown in decrease in percentage in the table. The number of connections has been increased from 1 to 5 and hence the throughput is increasing for sinkhole affected DSR.But when compared to normal DSR the throughput has gone down by 31% as shown in the table.

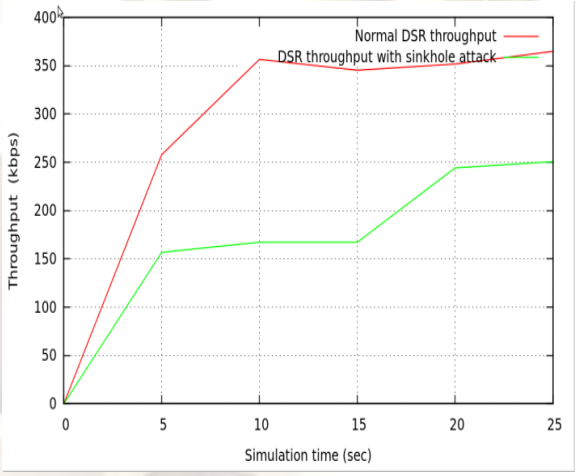

Figure 3. Graph showing throughput decreases in presence of sinkhole

Table2. Throughput in kbps

Simulation Time	Throughput in normal DSR	Throughput in sinkhole affected DSR	Percentage decrease in Throughput
5	257.85600	156.780800	39%
10	356.576000	167.078400	53%
15	345.344000	167.078400	52%
20	351.748800	244.185600	31%
25	364.921600	250.649600	31%

Packet drop

Packet drop is calculated as the difference between the number of packets sent by the source node to that of the number of packets received by the destination node. As sinkhole is a malicious node it may drop the packets that are being received by it. Hence the packet drop will increase in the presence of sinkhole attack. Figure 4 shows how the packet drop happens in the presence of sinkhole.

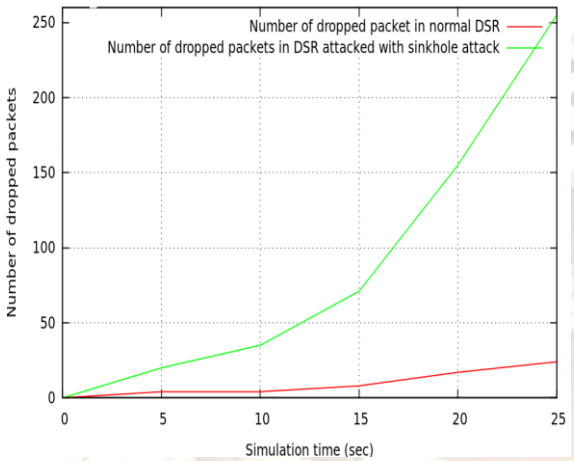

Figure 4. Graph showing packet drop in presence of sinkhole

From the values show in Table 3, it is clear that the packet drop on the network increases in the presence of sinkhole node compared to normal DSR operations, which adheres to the property of sinkhole.

Table 3. Packet drop in (%)

Simulation Time	Packet drop rate in normal DSR	Packet drop in sinkhole affected DSR	Percentage increase in packet drop
5	4	20	80%
10	4	35	87%
15	8	71	88.8%
20	17	155	89%
25	24	255	90%

Packet delivery ratio

PDR is the ratio of number of packets received at destination node to that of number of packets sent by source node. It is expressed in percentage. As sinkhole will drop and hold the packets of the network the packet dilivery ratio (PDR) of the network will decrease this is shown in the Fig. 5. below. The packets which are not dilivered are either dropped or may be forwarded to some other node in the network.

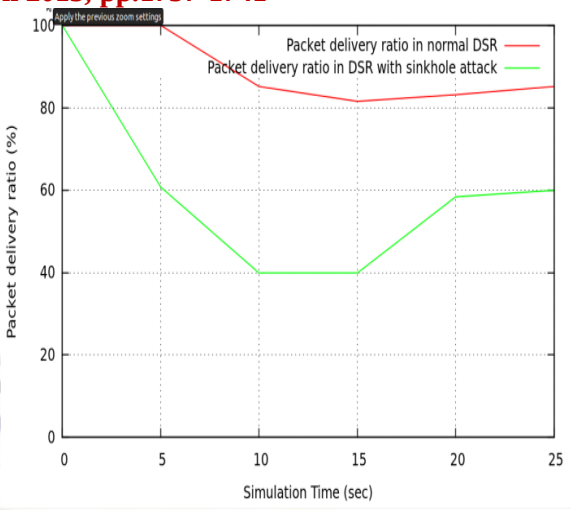

Figure 5. Graph shows decrease in delivery ratio when sinkhole present

In the Table 4, the Packet delivery ratio observed in normal DSR and sinkhole infected DSR is represented. Also the percentage of decrease in PDR due to the presence of sinkhole node is also depicted**.** There is fluctuation in the delivery ratio because, the sinkhole may selective forward some packets or may drop them.

Table 4. Packet delivery ratio (PDR) in (%)

Simulation time	Packet delivery ratio in DSR	PDR in sinkhole affected DSR	Percentage decrease in PDR
5	100.0000	60.784314	39%
10	85.2000	40.000000	53%
15	81.6000	40.000000	51%
20	83.2000	58.400000	30%
25	85.2000	60.000000	29%

V. CONCLUSION AND FUTURE WORK

In this paper, it is shown that the presence of a sinkhole node on the network will affect the performance of the DSR routing protocol, with the help of parameters like network throughput, packet drop and packet delivery ratio. It is very much clear from the above discussion that a sinkhole node will degrade the network performance to a large extent and hence must be detected and avoided.

In future, an efficient sinkhole detection and prevention method based on sequence number on MANET can be proposed. The efficacy of the approach shall be merited based on the network parameters like throughput, packet drop and packet delivery ratio.

REFERENCES

[1] Sangeeta Biswal, Suneeta Mohanty, Dambarudharh seth, "Study of DSR Routing Protocol in Mobile Adhoc Network", International Conference on Information and Network Technology, Singapore, vol. 4, 2011.

[2] Drs. Baruch Awerbuch and Amitabh Mishran, Dynamic Source Routing (DSR) Protocol, Advanced Topics in wireless Networks, CS: 647.

[3] Dr. G. padmavathi, D. shanmugapriya, "A Survey of attacks, security mechanisms and challenges in wireless sensor networks", International journal on computer science and engineering, vol. 4, June 2009.

[4] Gagandeep, Aashima, "Study of sinkhole attacks in wireless Ad hoc networks", International journal on computer science and engineering, vol. 4, June 2011.

[5] Sonal R. Jathe, Dhananjay M. Dakhane, "Indicators for detecting Sinkhole Attack in MANET", Proc.International Journal of Emerging Technology and Advance Engineering, volume 2, Issue 1, Jan. 2012.

[6] Venkatapathy Ragunath , "Implementations of DSR Protocol in NS2 simulator".

[7] Satveer Kaur, "performance Comparison of DSR and AODV Routing Protocols with Efficient Mobility Model in Mobile Ad-Hoc Networks", IJSCT Vol. 2, June 2011.

[8] kisung kim and se hun kim, "A Sinkhole Detection method Based on Incrimental Learning in wireless Ad Hoc Networks", Department of industrial Engineering, korea advance institute of science and technolog.

[9] Syamak Shah, Amit Khander, Mahesh Shirole and Girish Bhole, "Performance Evaluation of Ad Hoc Routing Protocols Using NS2 Simulation", Mobile and Pervasive Computing (CoMPC), 2008.

[10] Usha G and Dr.Bose S, "Impact Of Sinking Behavior in Mobile Ad Hoc Network", International Journal of Ad Hoc, Sensor & Ubiquitous Computing (IJASUC) vol. 3. No. 3, June 2012.

[11] The Network Simulator ns-2, http://www.isi.edu/nsnam/n.

[12] Raid Alghamdi, John DeDourek, Przemyslaw Pochec, "New Random Motion Geneartor for Wireless Mobile Network Simulator NS2", 2012.

[13] P. Samundiswary and P.Dananjayan, "Secured Dynamic Source Routing Protocol for Mobile Sensor Networks ", Proc of the 12th International Conference on Networking, VLSI and Signal Processing, 2010.

[14] Arti Sharma and Satendra Jain, " A Behavioral Study of AODV with and without a Blackhole attack in MANET", International Journal of Modern Engineering Research, vol. 1, issue. 4, pp. 391-395.

[15] Raid Alghamdi, John DeDourek, Przemyslaw Pochec, "Evaluation and Improvement to Motion Generation in ns2 for Wireless Mobile Network Simulator", Internation Journal of Digital Information and Wireless Communications, 2225-658x, vol. 2, issue. 4, 2012.

Authors Biography :

Mohammed Ashfaq Hussain is currently perusing his M.Tech in computer networks under VTU University. He has received his Bachelor of engineering from VTU in the year 2010.His area of interest includes security in networks.

Dr A Francis Saviour Devaraj has done his B.Sc and M.Sc in Computer Science from St.Xavier's College, M.E (Computer Science & Engineering) from Anna University. He has obtained his PhD in Computer Science from Manonmaniam Sundaranar University, Tirunelveli. He has also obtained certification in CCNA. He is a life member in technical societies like CSI, ISTE,CRSI, and ISOC. He has around eleven years of teaching experience in leading educational institutions in India and abroad. He has authored/co-authored research papers at the national and international levels. He has attended/conducted national and international level workshops/ seminars/conferences.