Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.239 – 244

SURVEY ARTICLE

A Survey of Sinkhole Attack on DSR in MANET

G. Vennila[1], D. Arivazhagan[2], N. Manickasankari[3]

[1, 2,3]Department of Information Technology, AMET University, India

[1] g.vennila265@gmail.com; [2] it_manager@ametindia.com; [3] manickasankari@gmail.com

Abstract:

MANET is a collection of wireless mobile node that communicating with each other without the use of network infrastructure. Each mobile node in mobile ad hoc network act as a host as well as router and willing to forward data to other nodes. A routing protocol is essential whose primary goal is to establish correct & well-organized route between pair of nodes, due to this reason, the routing protocols have been proposed for MANET. Routing security is one of the important challenges in MANET. Sinkhole attack is a type of routing attack in network layer which alter or drops the whole network traffic. This paper describes the sinkhole attack on DSR protocol. We have analysis the sinkhole attack, various detection and prevention techniques in MANET.

Keywords: MANET; DSR; sinkhole attack; RREQ; RREP

I. INTRODUCTION

A Mobile Ad-hoc network is a wireless network which is used to exchange information. Each node is willing to forward data to other nodes and act as a host as well as router. Routing can be classified as three types in MANET [1]. They are Flat, Hierarchical, and Geographic. The Flat routing protocols are further classified into three types. They are reactive, proactive and hybrid. The major difference between DSR and other on-demand routing protocol is that it is fully based on beacon-less transmission and consequently it does not require periodic hello packet (beacon) transmissions [3], which are used by a node to inform the presence of its neighbors. A major issue in Mobile ad-hoc network is "SECURITY". There are two approaches to protect the mobile ad-hoc networks. First, Reactive approach is seek to detect security threats and react accordingly. Second, Proactive approach is attempt to prevent an attacker from launching attacks through various cryptographic techniques.

This paper analyses one type of sinkhole attack and it focuses to see the existing detection and prevention techniques in sinkhole attack. A sinkhole attack is one type of attack in network layer. A sinkhole node tries to attract the data to it from all neighboring nodes. It generates fake routing information that let the nodes in local network know itself on the way to specific nodes. So, sinkhole node attempts to draw all network traffic to itself [4]. Thereafter it alters the data packet or drops the packet mutely. The routing protocol can be analyses by three factors [2] throughput, packet drop and packet delivery ratio.

In the rest of the paper is organized as follows as, Section 2 describes the DSR Protocol in MANET. Section 3 describes sinkhole attack in DSR protocol. Section 4 illustrates various existing detection techniques of sinkhole attack and Section 5 describes various existing prevention techniques of sinkhole attack.

II. DSR PROTOCOL IN MANET

DSR is a reactive routing protocol designed for MANETs. This protocol is based on source routing whereby all the routing information is maintained at mobile nodes. The basic operation of Dynamic Source Routing protocol [5] is shown in Fig.1. In this DSR process, it checks the corresponding packet type with respect to carry out the particular operations such as route discovery, route reply and data transmission. This on-demand protocol consists of two main phases: Route Discovery and Route Maintenance.

Route discovery

When a source node S wants to send a packet to destination node D, but it does not known a path to reach destination D. So, node S broadcast the Route Request (RREQ) to the desired destination. First it transmits the RREQ. The next node receives this RREQ and appends its own address then a node only forwards the RREQ, if the RREQ has not been seen by the node and also if the node address does not already appear in the route record when it does not have a path to the targeted destination. If it has a path to the targeted destination then it will send RREP message with the route information to source node [6].

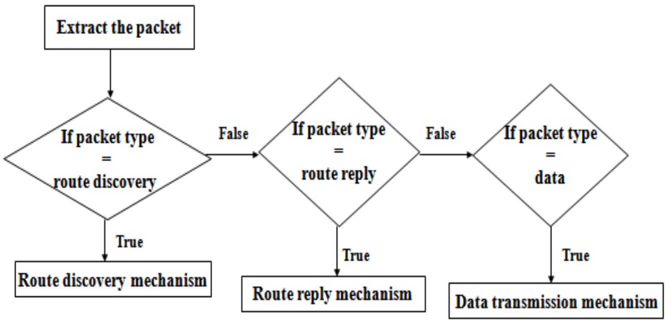

Extract the packet
If packet type = route discovery
False
If packet type = route reply
False
If packet type = data
True
True
True
Route discovery mechanism
Route reply mechanism
Data transmission mechanism

Fig.1.Flow chart for Basic operation of DSR

Route maintenance

Route Maintenance is done by two mechanisms namely route error packet (RERR) and Acknowledgements [7]. The destination node sends an acknowledgement ACK to the sender that the message received successfully [8]. If there is any problem in the communication link, it sends a route error message to the sender. Due to the problem in data link layer, it generates the Route error packets. When it receive the route error packet, then it removes the hop from the node's route cache [5] .if any node has another path in its route cache to reach the destination, then it can send the packet through the new route.

III. SINKHOLE ATTACK IN DSR PROTOCOL

A sinkhole node tries to attract the packet from all adjacent nodes. It generates forged routing information that allows the nodes in network know itself on the way to specific nodes. So, sinkhole node tries to draw all network traffic itself. Subsequently it alters or drops the packet silently [9]. In this DSR, it modifies the sequence number in RREQ. The Sequence number used to stop loop formations. It watches the source node's sequence number suspiciously and produce fake RREQ with higher sequence number than observed source sequence number. Then it broadcasts the fake or bogus RREQ [3].

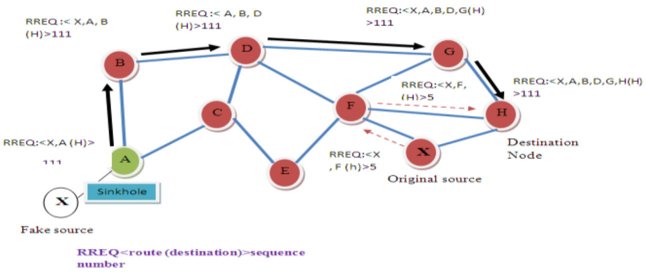


Fig.3.Creation of Fake RREQ

The Fig .3 shows the creation of the Fake RREQ packet. Sinkhole node A makes the fake RREQ which looks as if it is originated by node X. Sequence number of fake packet is 111, much higher than original source's, 5. Then it broadcasts the fakes RREQ.

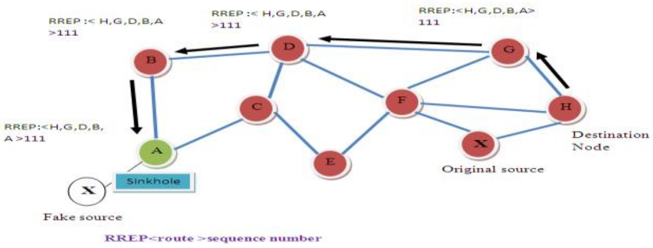


Fig.4. Broadcast of Fake RREP

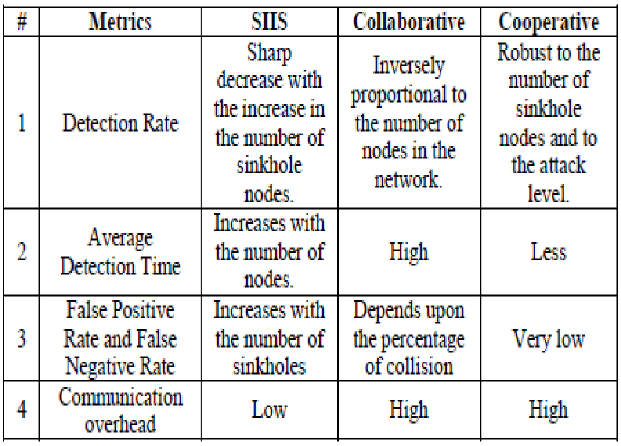
Neighbor nodes when receives the fake RREQ and identify this route may possibly better than original route. The fake route <X, A, B, D, G, H> is established and RREP is generated by the Destination node H in the form of <H, G, D, B, A, X> path as shown in Fig.4.

IV. SURVEY OF SINKHOLE ATTACK DETECTION TECHNIQUES ON DSR

Kisung Kim et al [11], developed a sinkhole detection algorithm using 3 indicators as sequence number discontinuity, route add ratio and Sequence number duplication. This sinkhole detection algorithm is based on incremental learning proposed to reflect the network's topology changes. It works very well for sequence number below the threshold value. Subsequently, a node broadcasts alarm messages to other nodes to exclude the sinkhole node in their route. There is an additional sinkhole indicator, sequence number duplicate. If sequence number duplicate is take place in a detecting node, the node can know the sinkhole existence by Ra_r. since it directly shows the sinkhole existence and is occurred while sinkhole node try to produce unusually high sequence number avoiding SeqN_D.

Gisung Kim et al [9] proposed a co-operative sinkhole detection algorithm is composed of three packets named as SAP, SDP, and SNP. He proposes a sinkhole indicator which is a sinkhole indicator is detected through the assessment of the RREQ. If a node accepts an RREQ whose source id is equal to the id of the receiving node, it checks the sequence number. If the sequence number of the RREQ is greater than the current sequence number of the node, then the node knows the existence of sinkhole and it recognizes this RREQ is from the fake node. Hence, we can find that there is a sinkhole node in the path of the RREQ .When a sinkhole indicator is detected, the sinkhole detection algorithm is begin by distributing a 'sinkhole alarm packet' (SAP). Then, the sinkhole detection algorithm tries to detect a sinkhole node by distributing a 'sinkhole detection packet' (SDP) and 'sinkhole node packet' (SNP). This algorithm works better than SIIS in terms of detection rate and detection time.

Immanuel John Raja Jebadurai et al [13], the detection mechanisms used here are classified into two parts; the first part is using the sinkhole detection indicators (SIIS) and the next one is the collaborative and final one is cooperative methods. The following table (TABLE 1) provides a brief comparison of these methods under different parameters.



#	Metrics	SIIS	Collaborative	Cooperative
1	Detection Rate	Sharp decrease with the increase in the number of sinkhole nodes.	Inversely proportional to the number of nodes in the network.	Robust to the number of sinkhole nodes and to the attack level.
2	Average Detection Time	Increases with the number of nodes.	High	Less
3	False Positive Rate and False Negative Rate	Increases with the number of sinkholes	Depends upon the percentage of collision	Very low
4	Communication overhead	Low	High	High

TABLE 1: Comparison of Various Detection Methods under Different Parameters

Ms. Sonal R. Jathe et al [3] proposed one approach uses the advantages of the cooperative technique as well as the discontinuity in the sequence number. It uses four different types of messages during the detection process. The first one as peak value will be selected based on the network. The peak value is nothing but threshold of the discontinuity in sequence numbers. Whenever a node receives any RREQ message, it will calculate the peak value by comparing the current RREQ with the previously received message of sequence number from the same source. The nodes will send a Message if the discontinuity in sequence number is greater than peak value. This Message contains the source route and the sequence number of the fake RREQ message. Suppose, if the attacker is so brilliant, the attack cannot be detected using the peak value. In this case, the second one begins. The target node will send the Attack Information Message to the network. The next one will be 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 message will be different from different sources. The final one will be the broadcasting of the message will confirm the sinkhole node.

Mohammed Ashfaq Hussain et al [2] deals with simulation study of sinkhole attack in DSR by NS2, its result analysis as below, Network throughput:Throughput is receiving the total number of packets by the destination node over a period of time and the kbps is metric used to calculate throughput. The sinkhole has access to more packets on the network and it does not allow the packets to reach the destination and hence the throughput decreases.

Packet drop:

Packet drop is the difference between the numbers of packets sent by the source node and the number of packets received by the destination node. As sinkhole is a fake node it may drop the packets that are being received by it. Therefore, the packet drop increases in the presence of sinkhole attack.

Packet delivery ratio:

PDR is the ratio of number of packets received at destination node to number of packets sent by source node. It is expressed in percentage. The packets which are not delivered are either dropped or may be forwarded to some other node in the network. These network parameters are analyzed with the sinkhole nodes present on MANET. After analyzing the above three parameters that gives the result as sinkhole node decrease the network performance. Hence, it must be detected and avoided.

V. SURVEY OF SINKHOLE ATTACK PREVENTION TECHNIQUES ON DSR

SECURITY-AWARE ROUTING (SAR) [6]: The SAR protocol facilitates to overcome the problems occur due to Sinkhole attacks in DSR protocol. In the security-aware routing protocol (SAR), the security measures are inserted into RREQ packet. When the node receives RREQ, if it is accomplished to provide desired security features, then the packet is forwarded to the next node, otherwise, the packet is dropped. The SAR offers Solution to handle the problems related to sinkhole attack in DSR as follows, Routing message protection: The routing messages consist of both digital signature and sequence numbers. When source node sends a message, the sequence number is initialized to zero in the starting and is incremented at every time. Digital signature provides the ability by which sender sign each message that assist to maintain the integrity and authentication of message. The message is dropped if it is corrupted. Routing update protection: As a source node updates the routing information to particular destination node than updates the routing information is sent to each node in that particular path.

Winnie Main et al [14], proposed a prevention techniques are Digital Encryption, Sequence Number Discontinuity Check and Sequence Number Duplication check as follows,

Step1: Security encryption check

A secret key is shared with each legitimate node and the packet is encrypted and decrypted with this secret key.

Step2: Sequence number check

A threshold_diff and prob_mal_node parameters are set based on network size. The way of calculating threshold_diff is the difference between the current sequence number and previously received sequence number for the same packet has been done. If the difference is below the threshold_diff, then the packet is forwarded. Else if the difference is above the threshold_diff, then the value of the prob_mal_node is incremented and the packet is dropped. Else if the value of prob_mal_node is below its threshold, then the packet is forwarded.

Step 3: Duplicate sequence number test

A dup_threshold and dup_prob_mal_node parameters are set based on network size. Next, the value of dup_prob_mal_node is incremented by 1. Now if the value of dup_prob_mal_node goes beyond its dup_threshold value, then the nodes is treated as fake node and drop the packet. Else if the value of prob_mal_node is less than its threshold value, simply it forwards the packet.

The above proposed prevention techniques will effectively curtail the sinkhole problem.

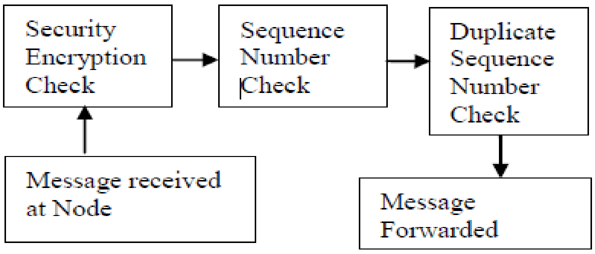


Fig.2.Prevention Techniques

The message Flow of all the above three prevention techniques are shown in Fig.2.After getting the first RREQ packet, start a first_time timer. If the packet is encrypted then continue for Security Encryption Check Using the same shared secret key, decrypt the packet. If the packet cannot be decrypted, it drops the packet. If the packet can be decrypted, continue to extract packet contents. When the packet is received with a new sequence number, it performs Sequence Number Check. Else if the sequence number has been received previously for the same packet and if the timer (first_time) has not expired so far, it drops the packet. If the timer has expired as first time, it performs the Duplicate Sequence Number Test. Else simply it drops the packet.

VI. CONCLUSION

Mobile Ad-Hoc networks are popular networks used broadly due to their dynamic nature. These types of networks are suffered from the sinkhole attack as there is no centralized security management. The “Sinkhole attack” is one of the cruel attacks in network layer and it constructs the legitimate nodes as fake nodes that give the result in loss of secure information. This paper focuses on sinkhole attacks on routing protocol on DSR. We discussed about how sinkhole attack origin problem between different nodes which is applicable in DSR routing protocol and also provided a survey on various detection and prevention techniques to elude the sinkhole attack in Mobile Ad-Hoc network.

REFERENCES

1. Usha G and Dr.Bose S,” IMPACT OF SINKING BEHAVIOR IN MOBILE ADHOC NETWORK”, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.3, June 2012
2. Mohammed Ashfaq Hussain, Dr. A. Francis Saviour Devaraj, Upshot of Sinkhole Attack in DSR Routing Protocol Based MANET, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com, Vol. 3, Issue 2, March -April 2013, pp.1737-1741
3. Ms. Sonal R. Jathe ,Prof. D.M. Dakhane , “Detection of Sinkhole Attack against DSR Protocol MANET”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012
4. Rajeshwar L. Balla, Venugopal Kotoju,”Sinkhole Attack detection and prevention in MANET & Improving the performance of AODV Protocol”,COMPUSOFT, An international journal of advanced computer technology, 2 (7), July-2013 (Volume-II, Issue-VII)
5. D. B. Jagannadha Rao ,Karnam Sreenu, Parsi Kalpana,”A Study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks”, International Journal of Advanced Research in Computer and Communication Engineering,Vol. 1, Issue 8, October 2012
6. Gagandeep, Aashima,”Study on Sinkhole Attacks in Wireless Ad hoc Networks”, International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 06 June 2012
7. Deepa.S , Dr. D.M Kadhar Nawaz , ”A Study on the Behavior of MANET Routing Protocols with Varying Densities and Dynamic Mobility Patterns” IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, 2010
8. Sajjad Ali & Asad Ali ,”Performance Analysis of AODV, DSR and OLSR in MANET”, Department of Electrical Engineering with emphasis on Telecommunication Blekinge Institute of Technology, Sweden 2009
9. Gisung Kim, YounggooHan, SehunKim , “A cooperative-sinkhole detection method for mobile adhoc networks”, International Journal of Electronics and Communications.(AEU) 64 (2010) 390–397.
10. 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.

11. Kisung Kim and Sehun Kim , "A Sinkhole Detection Method based on Incremental Learning in Wireless Ad Hoc Networks", Department of Industiral Engineering, Korea Advanced Institute of Science and Technology,373-1, Guseong-Dong, Yuseong-Gu, Daejeon, 305-701, Korea.2007
12. Sonal R. Jathe, Dhananjay M. Dakhane ," Indicators for Detecting Sinkhole Attack in MANET", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 1, January 2012)
13. Immanuel John Raja Jebadurai, Elijah Blessing Rajsingh , "A Survey on Sinkhole attack Detection methods in Mobile Ad-hoc Networks", 2011 3rd International Conference on Machine Learning and Computing (ICMLC 2011)
14. Winnie Main, Narendra M. Shekokar, "Study of DSR and AODV under Sinkhole Attack and Its Proposed Prevention Technique", Int. Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 4, Issue 3(Version 3), March 2014, pp.01-04