ISSN: 2321-7782 (Online)
Volume 3, Issue 1, January 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Survey on Sinkhole Attack Techniques in Mobile Ad hoc Networks

Vivek Tank[1]
PG Scholar – Computer Engineering
School of Engineering, RK University
Gujarat, India

Prof. Amit Lathigara[2]
Head of Department – Computer Engineering
School of Engineering, RK University
Gujarat, India

Abstract: ***MANET is most emerging and highly demanding wireless network technology. MANET is an infrastructure less data network, where all nodes behave like source or router. Mobile ad hoc network are considered to be vitally important for wireless communication. Security is the fundamental requirement in mobile ad hoc network, so routing protocol is most recent challenges. Most of the attacks on MANETs are routing protocol attacks. Sinkhole attack is one of the most sever attack in MANETs. It tries to attract all neighbour nodes to itself and broadcast fake or bogus routing path. In this paper, sinkhole attack describes in routing protocol also.***

Keywords: Sinkhole attack, Security, Mobile ad hoc networks (MANETs), Routing protocol, Techniques, Comparison.

I. INTRODUCTION

Mobile ad hoc network is an infrastructure-less data network, also a collection of wireless mobile nodes (or routers) dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably.

Dynamic nature of wireless ad hoc network perform a vital role. It is one of the significant factors in the performance of a wireless ad hoc network. It allows mobile nodes to join or leave freely in the network. Wireless ad hoc dynamic topology provides flexibility to the network in comparison to other wireless alternatives [8]. This is not limited to the capability of the mobile nodes communication, as mobile nodes in the network can move freely within the range of other members in the network. Mobile units may move out of the transmission range after the connection has already been established and this may cause data loss during transmission [8].

Security Issue: Security has become a primary concern to provide protected communication between mobile nodes in an antagonistic environment. The wireless channel is accessible to both legitimate network users and malicious attackers. Ad hoc network attacks can be classified into active and passive attack. A passive attack does not inject any message, but listen to the channel. In case of active attack, message are inserted into the area of network; such as replication, modification and deletion of exchanging data etc. all this actions involves in attacks. There are certain specific attacks to which the ad hoc context is vulnerable. Performing communication in free space exposed ad hoc networks to eavesdrop or inject messages. Sinkhole is one of the most risky attacks in mobile ad hoc network.

The rest of the paper is organized as follows: In section 2 Introduction to Sinkhole attack in MANET with routing protocols. In section 3 Survey of diff.-diff. technique for sinkhole attack. In section 4 conclude our work.

II. SINKHOLE ATTACKS IN MANET

Sinkhole attack is one of the severe attacks in wireless ad hoc network. In sinkhole attack, a malicious node broadcast wrong routing information to produce itself as a specific node and receives whole network traffic itself. 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 or information from all neighboring nodes. Sinkhole attacks affects the performance of ad hoc networks protocols such as AODV, DSR etc. by using flaws as maximizing the sequence number or minimizing the hop count. In this way the path presented through the malicious node appears to be the better route for the nodes to communicate [2] [3].

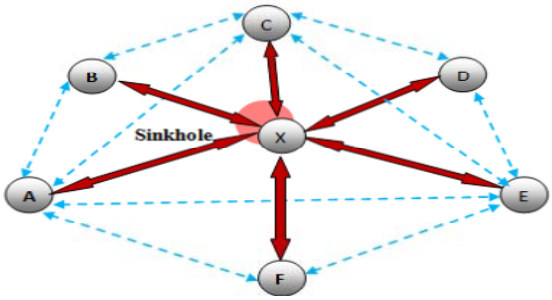

Fig.-1 sinkhole attack [3]

A. *Effect on Routing Protocols*

When data packets need to be transmitted from source to destination node at that time routing protocols are required by communicating with number of intermediate nodes. In ad hoc network there is various kind of routing protocol is there. These all protocols help to find a correct route for packet delivery to its destination [9]. In mobile ad hoc network, various routing protocol are used in area of research since many years.

Routing protocols can be classified in two major types:

- Table-driven routing protocol (Pro-active)
- On-demand routing protocol (Reactive)

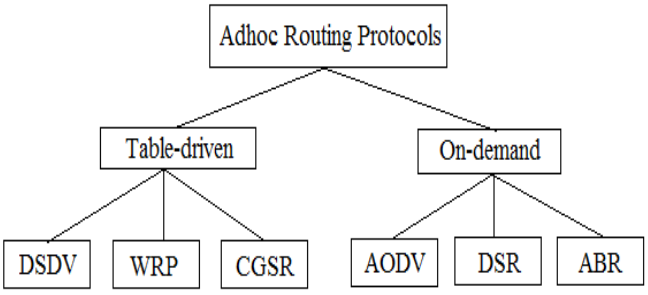

Fig.-2 Ad hoc Routitng Protocols

Table-driven routing protocols maintain a route by each node to all other network nodes. It also store the routing information of each router in form of table approach. Tables are consistently updated to maintain the correct information of the whole network status [3]. On the other hand, on-demand routing protocols, to reduce the overhead, the route between two nodes is exposed only when it is needed.

A.I DSR Routing Protocol

DSR protocol is source-based, loop-free, on-demand routing protocol, where each node maintains a route cache that maintain the source route learned by the nod. Sinkhole attacks use RREQ route-discovery process, which is based on sequence number increment. Sequence number are used for avoid multiple transmission and prevention of loop formations on source route request. The higher sequence number, the more recent route the packet contains. Sinkhole node selects the source node and destination node. It monitors the sequence number of source nodes, and broadcast fake or bogus RREQ. When all neighbor node receives fake or bogus RREQ can think and observe that this route is a better route to reach the destination [3].

The given diagram shows that how bogus or fake node affects the routing process by advertising itself as an active participant in transmission of packets. Sinkhole node 1 initiates the bogus/fake RREQ which looks as if it is initiated by the node 0. The sequence number of the bogus/fake 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.

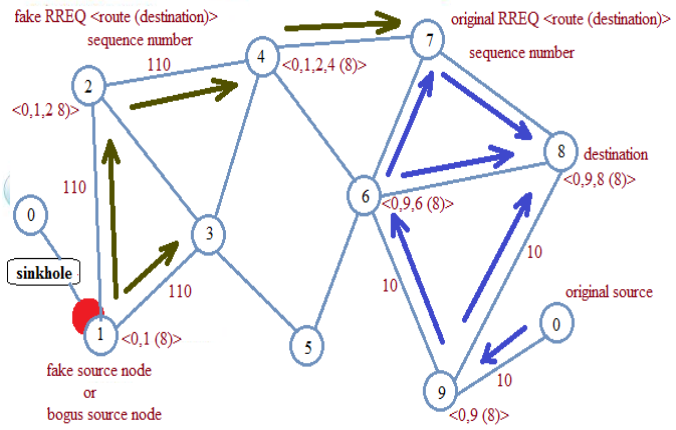

Fig.-3 sinkhole attack introducing bogus node

A.II AODV Routing Protocol

AODV routing protocols are known as reactive routing protocols. AODV is source initiated routing protocol. AODV protocols are different from traditional proactive protocols since in proactive the routing mechanism is based on periodic updates which leads to high routing overhead [12]. On demand protocols create routes only when it looked-for source nodes. AODV is an improvement of DSDV algorithm. It is typically to minimize the number of required transmissions by creating routes on insist basis [4].

Control message in AODV

- Route request message
- Route reply message
- Route error message (RERR) and HELLO messages are used for discovery and breakage of route.

In AODV, when a source node wants to send a data packet to a destination node a route discovery process is started by in order to find an original route to the destination node. The immediate neighbor nodes who receive this RREQ, it rebroadcast the same RREQ to its neighbors. The process is carry out continually until the destination node for proper RREQ is found. When the RREQ message reaches the destination node, a route reply RREP is generated by the destination. The RREP is sent to the source node as a node as a unicast along the reverse route which was established during the RREQ broadcast [4] [7].

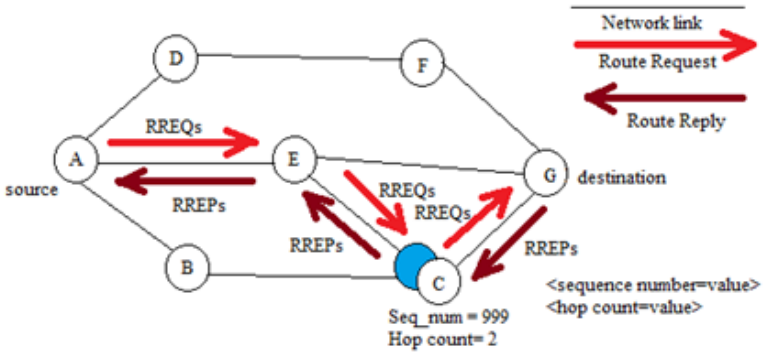

Fig.-4 sinkhole attack in AODV

Above diagram shows the compromised node C which looks like other node, become malicious node and advertise itself. The node C 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 C 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 [9].

III. Survey on Sinkhole Attack with Different Techniques

A. Trust management technique

K. Tunwal, P. Sharma [7], here sinkhole prevention method is based on individual trust management. All the node have trusted weight, each node forward the packets to next node until it reached at destination. When sinkhole node assume that the node is malicious at that time it decrements the local trust of that node. At last when route is created the node with the lowest trust values are avoided. So, the efficiency and reduce false alarming the time is dynamically modified as per the packet received per seconds. The simulation, conforms that method is well suited for robust to network environment.

B. Incremental learning technique

K. Kim and S. Kim [3], method can adapt to the changes within a MANET and can find the sinkhole attack precisely. The method is well used for special version of sinkhole attack (stealthier attack) and robust to network environment. This algorithm works very well for high sequence number in attack.

C. SIIS (sinkhole intrusion indicators system)

J. Culpepper, H. Tseng [13], the DSR protocol for routing in MANETs was presented and an important class of routing intrusion described. Two intrusion indicator rules were developed: (1) sequence no. duplication:- in a normal DSR simulation, the difference between last and current sequence number in packets received by a specified source would usually be one, and that in a DSR simulation with a sinkhole attacker, this diff. would be much higher. (2) route add ratio:- ratio of number of routes added through a given node to total routes added by a node, 1. A cooperative node would observe a route add count for the attacker node would observe a much longer route add ratio for an attacker node than it would for other cooperative node.

D. Collaborative technique

Marchang N., Datta R. [14], the mobile node used as a monitor node. This approach include extra burden on the mobile node which is acting as a monitor node. Mobile nodes work with small amount of battery power. Some time we select a mobile node which has high capabilities as monitor node, than the problem in the form of mobility.

E. Adaptive technique

Thanachai T., Tapanan Y. and Punthep S. [8], mechanism for adaptively detecting & defending against sinkhole attack in dynamic ad hoc system by applying trust-based algorithm on ad hoc nodes. Weights & threshold are used for separating suspicious behaviors from normal ones. Every ad hoc node assigns a trust weight to its neighbors. During the time of transmission if a neighbor node fails to reply its message to a designated receivers node, than the ad hoc node reduce the trust weight it has given to the neighbor node. For the decision purpose, it does not require any centralized unit. But allows the node to make the decision for itself.

F. Cooperative technique

G. Kim, Y. Han, S. Kim [6], cooperative method sinkhole detection algorithm is based on three packet broadcasting processes: SAP, SDP & SNP. When sinkhole indicator is detected, the sinkhole detection algorithm is initiated by broadcasting a 'sinkhole alarm packet' (SAP). After, sinkhole detection algorithm will tries to detect a sinkhole node by broadcasting a 'sinkhole detection packet' (SDP) and 'sinkhole node packet' (SNP). Any node that received the same fake or bogus RREQ has the same route information from the source to the sinkhole node, than intersection of those routes can reduce the set of sinkhole candidates.

G. Cluster analysis technique

W. Shim, G. Kim, S. Kim [11], cluster analysis works like categorical data, such that objects in a given category are similar to each other and dissimilar from other groups. Here use cluster analysis to separate false RREQs from normal RREQs and to verify indicators for detection. Here does not require predetermined numbers of groups in hierarchical approach, because there could be more than two groups such as normal RREQs or false RREQs. Suggest fully decentralized and robust feature under various types of a sinkhole attack by analyzing sinkhole attacks thoroughly.

H. Detection & Prevention technique

Nisarg G., Rahila P. [10], discusses the sinkhole problem, its consequences & presents a mechanism of detection and prevention of it on the context of AODV protocol. The detection and prevention technique is based on sequence numbers. Applying AODV protocol, prove that performance of AODV is improved after applying detection & prevention mechanism, which is deteriorated due to attack. The paper does not consider the problem of duplicate sequence number.

TABLE I
COMPARISON OF NUMEROUS TECHNIQUES

Technique Name	Advantages	Disadvantages
SIIS (sinkhole intrusion indicators system)	Average detection time is increase with the number of nodes	Communication overhead is low
Trust Management	Robust to network environment	Every time node assume the node is malicious and decrease the local trust value of node
Collaborative	Average detection time is high	False positive and negative rate is depends on the percentage of collision
Cooperative	Robust to the number of sinkhole nodes and to the attack level	Average detection time is very less

Adaptive	Not require ant centralized unit to make the decision	Can't tell whether the suspicious node is the malicious node or the node that moves too frequently and unintentionally causes link failures
Cluster analysis	Fully centralized and robust features	Mobility of the nodes and some controlling point
Detection & Prevention	Communication overhead is high	Performance degraded when increase number of node

IV. 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. This paper provided a survey on various countermeasures for sinkhole attack in mobile ad hoc network and different-different techniques for sinkhole attack. In this paper we discuss how sinkhole attack causes problem in on-going communication between different nodes and also effect of routing protocol. Now, in AODV protocol to solve the duplicate sequence number problem is a challenging research area.

ACKNOWLEDGEMENT

We would like to thank everyone who helped us in our research work.

References

1. Immanuel john raja jebadurai, Elijah Blessing Rajasingh, "A survey on sinkhole attack detection methods in mobile ad hoc networks", 2011 3rd International Conference on Machine Learning and Computing (ICMLC 2011)-IEEE, 978-1-4244-925 3-4.
2. Gangdeep, Aashima, Pawan kumar, "Analysis of different security attacks in MANETs on protocol stack-A review", International Journal of Engineering Advanced Technology (IJEAT), ISSN: 2249-8958, Volume-1, Issue-5, june-2012.
3. K. Kim, S.Kim, "A sinkhole detection method based on incremental learning in wireless ad hoc networks".
4. R.Madhumathi, J.Jenno Richi Benat, "Attacks in mobile adhoc networks: Detection and counter measure", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-1, 2012.
5. Jeba veer singh jebadurai, Alfred raja melvin A, Immanuel john raja jebadurai, "Sinkhole detection in mobile ad hoc network using mutual understanding among nodes". India. IEEE-2011.
6. Gisung Kim, Younggoo Han, SehunKim, "A cooperative-sinkhole detection method for mobile ad hoc networks", International Journal of Electronics and Communication. 64 (2010) 390397.
7. Khusboo Tunwal, Priyanka singh dabi, pankaj sharma, "An individual trust management technique for mitigating sinkhole attack in manet", International journal of computer application(0975-8887), volume 95-No.24, june-2014.
8. Thanachai T., Tapanan Y. and Punthep S., "Adaptive Sinkhole Detection on Wireless Ad Hoc Networks", Assumption University, Thailand. IEEE 2006.
9. Gagandeep, Aashima, Pawan Kumar, "Study on Sinkhole Attacks in Wireless Ad hoc Networks", International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397, Volume-4, Issue-5, June 2012
10. Nisarg Gandewar , Rahila Patel , "Detection and Prevention of sinkhole attack on AODV Protocol in Mobile Adhoc Network", fourth international conference on CICN, IEEE-2012.
11. Woochul Shim, Gisung Kim, Sehun Kim, "A distributed sinkhole detection method using cluster analysis", 0957-4174, 2010-Elsevier.
12. Usha G and Dr.Bose S, "Impact of Sinking behaviour in Mobile adhoc network", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.3, June 2012
13. Benjamin J. Culpepper, H.Chris Tseng," Sinkhole Intrusion Indicators in DSR MANET", First International Conferenc on broadband networks IEEE 2004.
14. Marchang N, Datta R., "Collaborative techniques for intrusion detection in mobile ad-hoc networks", Ad hoc networks 6(2008) 508-523, Elsevier-2008.

AUTHOR(S) PROFILE

Vivek Tank, Received the B.E. degree in Information Technology from Gujarat Technology University, Gujarat, India, in June 2012 and Pursuing Master of Technology degree in Computer Engineering from RK University, Gujarat, India. His main area of interest includes ad hoc network, network security and wireless sensor network.

Amit Lathigara, received the B.E. Computer Engineering from the Saurashtra University, in May 2004 and the M.E. Computer Science and Engineering from the Anna University, in May 2011. He is currently pursuing a Ph.D. in School of Engineering, RK University, India. During the course of his M.E and Ph.D. he has authored a more than 10 different journal and conference papers. He has also been a technical referee for various different conference and journals, and is currently working as head of department in computer engineering and information technology at school of engineering, RK University and a faculty member of ISTE. His research interests are mobile ad hoc network unicast routing, energy efficiency and QoS.