To Detect and Overcome Sinkhole Attack in Mobile Ad hoc Network

Vivek Tank
PG Scholar
Computer Engineering
RK University, Gujarat, India

Amit Lathigara
Head of Department
Computer Engineering,
RK University, Gujarat, India

ABSTRACT

Mobile ad-hoc network abbreviated as MANET is most emerging and highly demanding wireless network technology. Due to the property of self-deliberate, where all point of network behaves like source or router and also all nodes are keeps on moving freely in network area. Mobile ad hoc network perform important role in connectionless environment. Security is the most fundamental requirement in mobile ad hoc network to secure the sensitive information from hackers. In MANETs typically many attacks are routing protocol attacks. Sinkhole attack is one of the most severe attacks in MANETs. It tries to attract all neighbor nodes to itself and broadcast fake or bogus routing path. Here sinkhole attack describes in AODV routing protocol to applying security by using digital signature and hash chain to prevent the attack.

Keywords

Sinkhole Attack, Mobile ad hoc network, Routing protocol, Security, Digital signature

1. INTRODUCTION

Mobile ad hoc network is a self-deliberated data network and also a group of connectionless mobile nodes (or routers). There is no any infrastructure and centralized administration in mobile ad hoc network. The routers are keeps on moving freely and arbitrarily organize themselves. Thus, the topology may change very fast and unpredictably in wireless network.

Mobile ad hoc network perform a vital role in its dynamic nature. It is one of the most considerable factors for the functioning. It allows mobile nodes to linkup or go away from the network freely. As compared to other wireless alternatives, wireless ad hoc network provide flexible dynamic topology [8]. The capability of the mobile nodes communication is not limited. In the network mobile nodes can easily mobile within the network area. If connection has already been established in ad hoc network and mobile node may out of area of the radio range at that time data may be loss during transmission [8].

Security Issue: Security has become a basic concern for mobile network, to secure the communication between mobile hops in an antagonistic network. Both validate network requires and intruder attackers access the wireless channel. Here attacks are categorized broadly in active and passive attack. A passive attack does not modify any data, but listen to the network. But in active attack, data are inserted into the area of the network, such as duplication, alteration and removal of exchanging data etc. all this action involves in attacks. The ad hoc context is vulnerable to certain specific attacks. Functioning communication in gratis area exposed ad hoc networks to listen in or insert messages. So, Sinkhole is one of the most risky attacks in mobile ad hoc network.

In this paper: section 2 Introduction to Sinkhole attack in MANET with AODV routing protocol. In section 3 Problem Statement, in section 4 Related work of sinkhole, in section 5 Proposed system, in section 6 Simulation parameters, in section 7 Result Analysis, in section 8 Conclusion and 9 Future Work.

2. SINKHOLE ATTACK IN MANETs

One of the most dangerous and risky attack in mobile ad-hoc network is sinkhole attack. In sinkhole attack, an intruder hops broadcast immoral routing message to generate itself as a specific hop and entertain whole network volume of data transfer itself. After entertaining whole network volume of data, it moderated the confidential data, such as data packet may changes or drops the packets to make the network very complex.

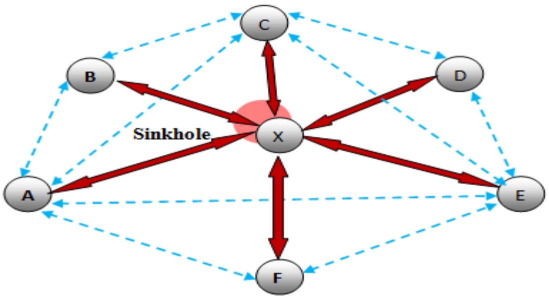

Fig.: 1 Sinkhole Attack

An evil node attempts to focus the protected data or information from all the nearest hops. Sinkhole attacks distress the functioning of ad hoc networks environment such as AODV, DSR and ZRP etc. by using traffic as enlarging the sequence number or reducing the number of hop between routes. The route introduce by the intruder node seems to be the healthier path for the every hops to convey [2] [3].

2.1 Routing Protocols

When information need to be transfer from origin point to destination point at that time routing protocols are required by communicating to its intermediate nodes. In ad hoc network many type of routing mechanism is there. This all mechanism used for find correct route for packet delivery to its destination [9]. In mobile ad hoc network, various routing mechanism 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)

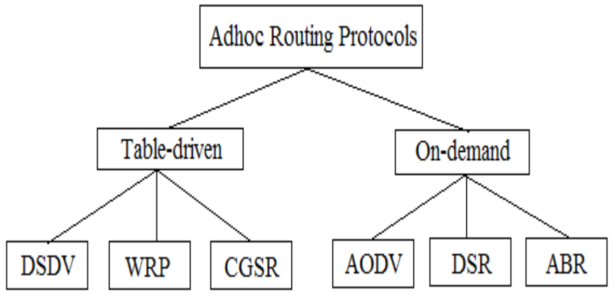

Fig.-2 Ad hoc Rouitng Protocols

Proactive routing mechanism maintains a route to each hop in mobile environment. It also stores the routing information of each router in the form of table approach. To uphold the proper information of the whole network status, tables are updated reliably [3]. On the other hand, on-demand routing mechanism, to decrease the load, the path between 2 hops is established only when it is required.

2.2 AODV Routing Protocol

A Reactive routing protocols of simple known as AODV. It is origin point instructed routing protocol. AODV mechanism are different from usual proactive mechanism, since in proactive the networking device is based on cyclic updates which leads to excessive routing load [12]. On demand mechanism creates routes only when it looked-for source nodes. AODV is an advanced version of DSDV algorithm. It is typically to minimize the number of needed transferring by creating routes on insist basis [4].

Control message in AODV

- Request message (RREQ)
- Reply message (RREP)
- Error message (RERR) and HELLO messages are used for find and breakage of route.

Source Id	Req Id	Source sequence number	Destination Id	Destination Sequence number	Hop Count

Fig.-3 RREQ Format

Source Id	Destination Id	Destination Sequence Number	Hop Count	Life Time

Fig.-4 RREP Format

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

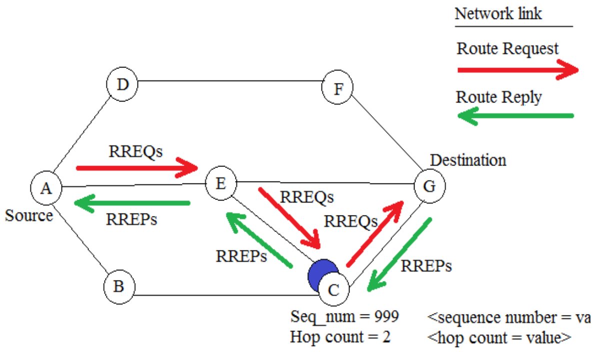

Fig.-5 Sinkhole Attack in AODV

Above figure shows that the cooperated node C is different node from other nodes, it turns out to be intruder node and promote itself. Now, hop C sends higher sequence number to next hop E to erroneous for novel path. It also sends smaller number of intermediate hop value for shortest path at that time node E granted that node C has smallest path, so starts posting the data packets to the destination. AODV has two types of messages handover or pick up in the middle of nodes from source to destination [9].

3. PROBLEM STATEMENT

In mobile ad hoc network, sinkhole attack is very serious problem in the area of operation and its services. Sometimes the system may be failure due to network availability, at that time ad hoc node can’t transmit and receive messages from the any other nodes, so the performance of the network is degraded. To detect any attack in ad hoc network required more powerful presence of mind and attention also. Now a days, researcher use encryption techniques to prevent the attacks. This type of system required more overhead and also increase the network complexity.

When any of the system developed for prevent the attacks at that time there is some factors to be considered. Most popular factor is flexibility of the network. Flexibility does not need any fixed infrastructure, so in mobile ad hoc network it works very well. It has also valid and authentic characteristics of ad hoc network. In wireless network, every trusted ad hoc node should have enough capacity and capability to detect any attacks. Due to dynamic nature of the ad hoc network, every node can freely link up and leave the network area very easily. So it is very hard to stop the attackers to link up and leave the network.

Now a days in any attacks, there is main problem is sequence number duplication. Sometimes attackers use same sequence number to theft the data, so we must provide authentic security to every node of the network to and the duplicate sequence number. We can use any of the encryption techniques to find out the duplicate sequence number, it is very important for the current ongoing network activities. For attacks from superior malicious nodes, an issue of receiving packets with duplicate sequence number can also be encountered. This scenario will pan out when a malicious node sets its sequence number slightly higher than the current sequence number being used. Legitimate will continue sending packets with increasing sequence numbers and a situation will arise of receiving duplicate sequence numbers as well.

4. RELATED WORK

K. Tunwal, P. Sharma [7], here sinkhole prevention method is based on individual trust management. The entire 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.

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.

J. Culpepper, H. Tseng [13], the DSR protocol describe an important class in evil node detection system in mobile ad hoc network. 2 evil node indicator protocol were developed: (1) sequence no. duplication:- in a simple DSR environment, the ratio between current and previous order number in chuck of data received by a genuine node would usually be one with a sinkhole attacker, this diff. would be much higher. (2) route add ratio:- the route added ratio by given node from the total number of data paths added by node one. For find the attacker node, a adjacent node would check a path sum the value in network and also check a much longer data path add ratio for an intruder node.

Marchang N., Datta R. [14], the mobile node used as a monitor node. This approach include additional load on the mobile node which is temporary as a monitor node. With the use of small amount of battery power all the mobile node works well. Some time we choose a mobile hop which has grater abilities like observer node, than the generate difficulty in the form of mobility.

Thanachai T., Tapanan Y. and Punthep S. [8], author adaptively detect & prevent for sinkhole attack in continuously changes ad hoc system, by applying reliance value algorithm in ad hoc network. For separating doubtful behaviors from normal ones, weights & threshold are used. Each hop network environment allocate a faith trust-value to its neighbors. During the time of transfer data if a neighbor node feck reply message to a specified receivers node, than the ad hoc node reduce the trust-value to the given neighbor node. For the decision purpose, it does not require any centralized unit. But allows the node to make the decision for itself.

G. Kim, Y. Han, S. Kim [6], cooperative method is based on data chuck propagating over network processes: SAP, SDP & SNP. If this algorithm is instructed by means of communication a sinkhole alarm packet at that time sinkhole indicator is detected. After, this algorithm will attempt to identify a sinkhole hops by means of communication a sinkhole identify data chunk and sinkhole hops data chunk. When node received the similar fault request has the similar path information from the origin node to the intruder hop, than connection of those path can decreases the set of sinkhole applicants.

W. Shim, G. Kim, S. Kim [11], cluster analysis means categorical information, such that point in a given form is similar to each other and dissimilar to another cluster. Discrete and fake request from simple RREQ and validate observer for identification by exploiting cluster analysis. In hierarchical approach not require setting numbers of cluster, Due to there could be more than two clusters such as normal RREQs or false requests. Propose fully distributed and healthy feature under numerous kinds of a sinkhole attack by analysis it completely.

Nisarg G., Rahila P. [10], discusses the sinkhole difficulty; its importance & exiting a mechanism of identify and overcome of it in AODV protocol. The detection and prevention technique is based on sequence numbers. After applying detection & prevention mechanism, it show that performance of AODV is make better which is get worse due to attack. The paper does not consider the problem of duplicate sequence number.

T. Mishra, B. Singh, A. Kumar [18], used digital signature concept to secure the data. Here key is used for all nodes, this key generated by digital signature and verify it when decrypt the data. This algorithm provides security to its private nodes. To find the ease of use and corroboration of route on basis of hop count and time interval, a route validation scheme is also used. To changes conservative digital signature in secure routing data chunk, at the same instance, upholding the same level authentication, its advantages of first of all signature, which is more effectively in signing and validation. Every node in the network verified the digital signature for security purpose, if the signature is not verified or any of the packets has no valid signature than drop that packet. [19] [20] [21].

5. PROPOSED SYSTEM

After studying the problem of sinkhole attack in MANETs, the security is main problem with regarding to sequence number. Each of the RREQ packet can be uniquely identified by 3-things: Source, Destination and Sequence number.

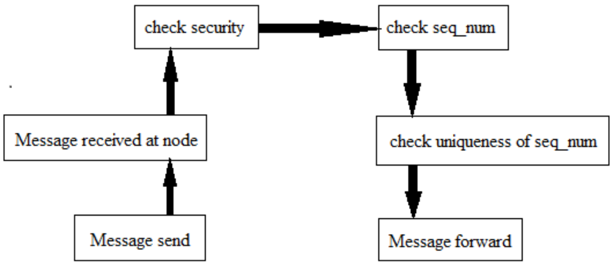

Fig.-6 Proposed System- Flowchart

Step 1: In the network, messages are keeps on moving free space and nearest node catch that message.

Step 2: Message received at next node and Reply message to sender node.

Step 3: Receiver node check the security with Digital Signature and Hash chain. The digital signature used for maintain the identity of each packet. Hash chain used to authenticate the hop count of RREQ/RREP messages. This technique is used to authenticate each and every hop.

Step 4: After checking security by digital signature, now the main thing is sequence number. Check the sequence number difference between current and previous sequence number.

Step 5: check the duplicate sequence number compared to security technique. If packet has digital signature and hash chain then forward the packet else drop the packet.

Step 6: If packet has unique sequence number then forward the message else drop it.

6. SIMULATION PARAMETER

We have used NS-2.35 simulator to implement our applied work for defending sinkhole attack. The simulation parameter is protest in Table-1. In this work, we take 10 to 50 mobile hops which communicate each other in AODV protocol. Nodes were placed randomly in a 700*700 area using simulation time is 500sec.

Table-1 Simulation Parameters

Parameter	Value
Simulator	NS-2.35
Channel type	wireless channel
MAC type	Mac/802.11
Traffic type	CBR
Maximum packet	150
Area	700*700
Simulation time	500 sec
Number of nodes	10-50
Routing protocol	AODV

7. RESULT ANALYSIS

7.1 Packet Delivery Fraction

It is the ratio between total numbers of received packet to the total number of packet sends by source node or sender node over a network.

PDF = ∑ No of packet receive / ∑ No of packet send

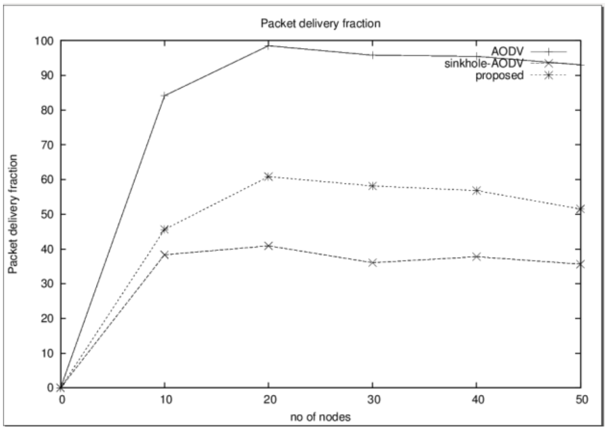

Fig.7 PDR vs No of Node

As per the graph, the value of the PDF in normal AODV is too much high when use number of nodes from 10 to 50. But when apply attack at that time PDF is low for number of nodes from 10 to 50 at same simulation time. But after applying our proposed security mechanism in AODV the ratio of the PDF is high as compared to sinkhole attack where number of nodes from 10 to 50. So here we successfully increase the value of PDF.

7.2 Packet Loss

It is the amount of number of packet abandoned by nodes due to numerous causes.

Packet loss = No of packet send – No of packet received

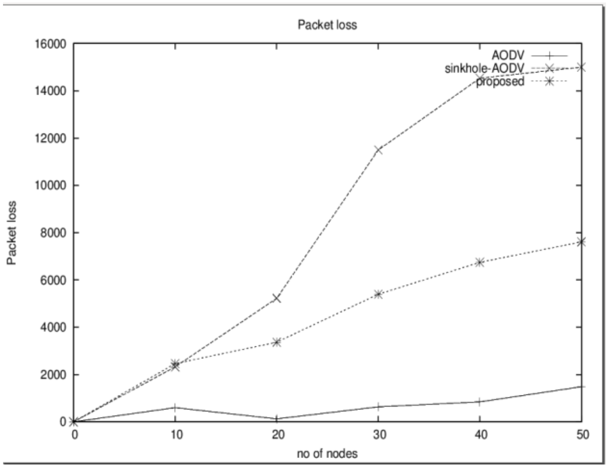

Fig.8 Packet Loss vs No of node

From the above graph, the result of packet loss in normal AODV is very low means continuously decreasing the value where number of nodes from 10 to 50. In sinkhole attack, the ratio of packet loss is highly increase as compared to normal AODV at same simulation time. But when apply our proposed mechanism, easily decrease the packet loss ratio as compared to sinkhole attack AODV for same simulation time. Thus our proposed system is very effective to improve the ratio the packet loss.

7.3 Throughput

In the specified time amount of data transfer for one point of network another point. And the rate for using transmitted data is known as throughput.

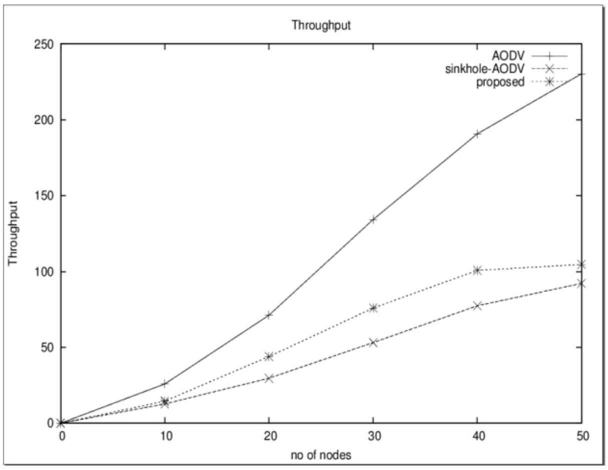

Fig.9 Throughput vs No of node

As per the graph, the value of Throughput in normal AODV is too much high when use number of nodes from 10 to 50. But when apply attack at that time Throughput is very low for number of nodes from 10 to 50 at same simulation time. But after applying our proposed security mechanism in AODV the ratio of the Throughput is high as compared to sinkhole attack where number of nodes from 10 to 50. So improve the performance of the value of Throughput.

8. CONCLUSION

MANETs 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. Here in this paper, we apply digital signature and hash chain for security and increase the performance of networks in diff-diff parameters. Every node has valid signature to verify it to next node and if it is not match than drop the packets. By using AODV protocol solve the duplicate sequence number problem using security technique and increase the network functioning.

9. FUTURE WORK

In future focus on to analyse and report sinkhole attack violation in other protocols and assess difference in its functioning after applying our proposed system in mobile ad hoc network. This proposed system is also useful in other types of attack to prevent it.

10. ACKNOWLEDGEMENT

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

11. 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.

[15] Ad hoc On-demand distance vector (AODV) routing ietf-draft-manet-aodv-13.txt.

[16] Mouhamad Ibrahim, “Introduction to network simulator”.

[17] NS-2. The ns manual (formally known as NS documentation) available at http://www.isi.edu/nsnam/ns/do

[18] T. Mishra, B. Singh, A. Kumar, “A Security Scheme for Mobile Ad-hoc Network with Reduced Routing Overhead”, IJARCSSE journal, Volume 3, Issue 8, August 2013

[19] L. Reyzin and N. Reyzin, “Better Than BIBA: Short One- Time Signatures With Fast Signing and Verifying”, 7th Australasian Conference on Information Security and Privacy, LNCS 2384, April- 2002.

[20] M. Zapata, “Key Management and Delayed Verification for ad hoc Networks”, Hi1gh Speed Networks, volume-15, no-1, January 2006

[21] Shidi Xu, Yi Mu and W. Susilo, “Authenticated AODV Routing Protocol Using One-Time Signature and Transitive Signature Schemes”, Journal of network