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
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 4, April 2017, pg.241 – 248

DETECTION AND PREVENTION OF WORMHOLE ATTACK IN ADHOC NETWORK USING AODV PROTOCOL

Rahul Jain[1], Rishabh Gupta[2], Rashmi[3], Sandhya Katiyar[4]

[#1, 2, 3,4]Information Technology Department, Galgotias College of Engineering & Technology, Greater Noida (U.P.), India

ABSTRACT: Ad hoc networks are vulnerable due to their structure less property. A Mobile Ad-Hoc Network (MANET) is an infrastructure less collection of mobile nodes that can arbitrarily change their geographic locations such that these networks have dynamic topologies and random mobility with constrained resources. They also have capability of network partition. The wormhole attack is the most attention seeking attack in ad hoc networks; it consists of two malicious nodes and a tunnel between malicious nodes. In wormhole attack, attacker records the packets at one location and tunnels them in another location in same network or in different network.

In this paper, a mechanism is proposed which is helpful in prevention of wormhole attack in ad hoc network is verification of sequence number of sending nodes by receiving node because each legitimate node in the network contains the IP address of every other legitimate nodes of same network. In proposed solution, if sender wants to send the data to destination, firstly it creates a secure path between sender and receiver with the help of sequence number and number of hops. If there is presence of any malicious node in between the path then it is identified because malicious node does not have its own sequence number and also the number of hops is large.

KEYWORDS: MANET; RREP; RREQ; RERR; Wormhole

1. INTRODUCTION

There are two types of Wireless Network: Infrastructure Wireless Network and Infrastructureless Wireless Network.

In Infrastructure Wireless Network, the wireless nodes can not communicate directly and the communication between these nodes take place through Access Points. These access points act as bridge between nodes.

In Infrastructureless Wireless Network, the wireless nodes can communicate directly without access points; these are known as Adhoc Networks. They do not fix infrastructure for communication. These networks do not have any routers and wireless nodes work as routers.

The collection of mobile devices that use wireless transmission for communication are called Mobile Adhoc Networks. They do not have fixed infrastructure. The setup of mobile adhoc networks is very easy as the routers can move randomly.

There are three types of routing protocols: Proactive Routing Protocol, Reactive Routing Protocol and Hybrid Routing Protocol.

In Proactive Routing Protocol, each node has a table which contains the information of all other nodes of the network. Example- DSDV, WRP.

In Reactive Routing Protocol, each node has a route cache instead of routing table. Route cache is only generated when the node wants to communicate. Example- AODV, DSR, TORA.

Hybrid Routing protocol is a combination of proactive routing protocol and reactive routing protocol. Example- Zone Routing Protocol (ZRP).

2. WORMHOLE ATTACK

Wormhole Attack is a very dangerous attack in the Mobile Adhoc Network. In these networks, few nodes make a tunnel together by a high quality wireless link or a logical link. In wormhole attack, the traffic is enter from one end, moves through the tunnel and exit from another end. When the attacker attacks on the message, it copies the packet to other attacker through tunnel and then the attacker replays the message in the network.

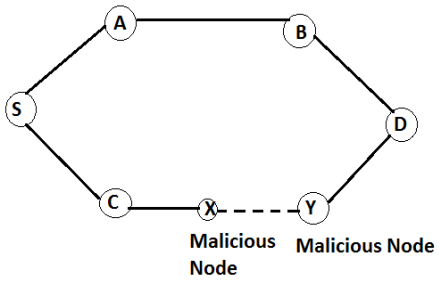


Fig.1: Adhoc Network

3. AODV PROTOCOL

Adhoc On Demand Distance Vector is a reactive protocol for mobile adhoc network. It is an on demand protocol as this protocol generates a routing table only when a node transmits a message. It supports unicast and multicast routing. It is able to accommodate large number of nodes in the network. The transport layer has used UDP protocol which offers best delivery of packets in the network. The communication between the nodes takes place through IP addresses. Each node has its own IP address and the information of IP address of every other node of the network. The routing table contains many fields such as IP address, sequence number, number of

hops, IP address of neighbour from whom got route request(RREQ), IP address to which it forward the RREQ, sending time, receiving time, count, name of nodes.

When a message is transmitted in the mobile adhoc network, the message contains RREQ, RREP, RERR and message.

3.1 RREQ(Route Request)

When a node wants to send a message to the destination then it broadcast RREQ to the neighbour node with its current sequence number. The neighbouring node uses the RREQ to make an entry in its routing table.

3.2 RREP (Route Reply)

When the message from the source is delivered to the neighbouring node then it broadcast the RREP message to the source. It indicates that the message is received by the node and forwarded further towards the destination.

3.3 RERR (Route Error)

When a message is not received by a node or the connection is broken up then RERR message is broadcasted to the source node and the message is transmitted again in the same manner.

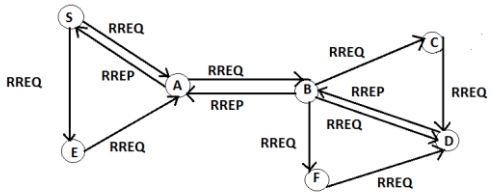


Fig.2: Wormhole Attack

4. LITERATURE REVIEW

Wormhole Attack can be quickly and easily launched by the different attackers even if the attackers does not have much knowledge about the nodes and networks. Many researchers try to work on this and have provided their ideas, solutions regarding this. Some of them are:-

L. Sudha Rani et al [1] This paper is concerned about the multicasting approach done geographically.Reason for selecting this protocol is Robust and Scalable Multicast Geographic Multicast Protocol [RSGM] protocol is able to track source efficiently. Has minimum overhead. Handles empty zone problems. It is robust and scalable. This type of attack are Difficult to handle but there detection and prevention is required. To defend or stop wormhole attack in RSGM protocol the only solution is Multicast Authentication Node Scheme.

Harbir Kaur et al [2] This paper gives information about the wormhole attack solutions. If packets in wormhole attack are discarded then this can lead to another type of attack i.e. DOS [Denial Of Service] that leads to slowdown of overall performance. Decision packets play a very key role in Minimization of wormhole though decision packets.

Pushpendra Niranjan et al [3] This paper deals with the tunnelling concept in which when packets are transmitted from source to destination in between attacker used to capture information. It is able to detect great number attackers in the minimum given time. Routes where chances of attack is maximum are blocked and if possible are modified also after some time if require.

Buch et al [4] This paper deals with RREP[Route Request, Route Reply] in which when one node wants to send information to another node if it is not there on route then need to broadcast it and when received route reply is done. In this way we identify two nodes, check authenticity and hop count.

Nishant Sharma et al [5] This paper deals how wormhole attack can harm the network badly. This deals with long term prevention and detection. Here they have discussed about the concept of Euclidean distance Formula through which prevention and detection of such wormhole attack can be stopped of long term as well as short term basis. Results that are obtained using this are satisfactory enough.

Guowei Wu1 et al [6] This paper is totally concerned with detection of wormhole attack. In this information about neighbourhood nodes is collected on basis of transmission range. All this things are done without using the clock synchronization, any other hardware etc

El Kaissi et al [7] This paper introduces a new protocol named as DAWWSEN that deals with defense mechanism against the wormhole attack, which is a powerful attack that can cause serious problems and consequences network and routing protocols. An advantage of DAWWSEN is that it doesn't require any geographical information about the nodes, and doesn't take the time stamp of the packet constrained nature of the sensor nodes. They examined the performance of DAWWSEN through different- different types of ns-2 simulations, and the results shows that they are absolutely correct in their means and can efficiently defend wormhole attack and also obtain low delay for better means.

Hubaux et al [8] In this paper a solution is found for the detection of wormhole attack in a different way by using antennas. In this communication is based on antennas. So when this happens everyone has the information about the neighbourhood locations when message is received. So antennas can play a vital role in detection of wormhole.

Subrat kar et al [9] This paper deals with a routing protocol named WHOP which is responsible in detecting wormhole attacks even if we have long tunnels without use of any type hardware and clock synchronisation. In WHOP AODV protocol is performed without making any changes in it. It uses an additional feature named Hound packet for wormhole detection, so if there are an adhoc network formed between trusted parties or private use then, security related issues will not be required or needed hence Hound packet will not be sent but if we find that network is not private i.e. it is public and nodes are experiencing a high packet dropping features then Hound packet will be send but after the path discovery phase is over.

Jyoti Thalor et al [10] This paper deals with Wormhole attacks in MANET.Give information about how wormhole attack can degrade the performance and is threat to network. Here they have examined the present approaches as well as future approaches which are helpful in avoiding such type of attacks. But these approaches are not always provide the correct output sometime their results are not satisfactory. So there is a need for standard solution which can be applied in maximum problems.

Kaur et al [11] This paper is based on different routing protocol to prevent wormhole attack in Adhoc . The performance of different routing protocol is evaluated using there throughput, end-to end delay and energy consumption. Another problem is unprotected environment of nodes. ANODR protocol performs well in threshold mode. The advantage of DSR protocol is that it consumes less amount of energy in receiving and transmitting data

Saurabh et al [12] This paper consist of implementation information about the wormhole attack detection . Few approaches and techniques have been discussed here to prevent such attacks .This paper will help every reader in understanding the wormhole attacks on different types of network.

Pirzada et al [13] This paper consist of an algorithm in which there is no requirement of any special hardware. This approach is basically based on round trip time concept . Basically, the round trip time is the total time require to deliver the message to the destination in addition with the time to receive the acknowledgement.
In general the round trip time is two times of the propagation time. So we can conclude that by this theory, that

it is easy to identify difference between real node and fake nodes.In this approach, every node calculates the round trip time and detects the fake nodes.

5. PROPOSED SOLUTION

1. When a source node S wants to send a message to destination D, S searches its route table for a route to D.

2. If no route found, S sends a RREQ request with the following components:

(a) IP addresses of S and D.

(b) Current sequence number of S and the last sequence number of D.

(c) Broadcast ID from S. This is incremented each time when S sends a RREQ request.

3. If a route is found to P, then P first checks whether it receives this RREQ before

(a) All nodes store <broadcast ID, IP address> for all RREQs they have received.

(b) If P has already this RREQ before from P then it discards this otherwise P process this RREQ:

(i) P sets a reverse entry for source S.

(ii) This contains the IP address, sequence number of S, number of hops to the node S and address of neighbour from whom P got RREQ.

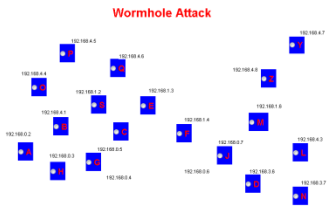
(c) If P is not the destination then it forwards the packet to its neighbour.

(i) P sets a reverse entry for S.

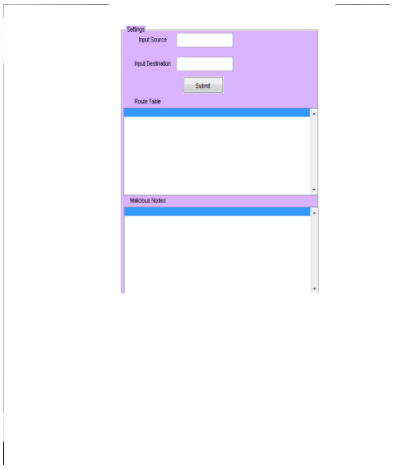
(ii) It contains node ID, sequence number, number of hops, sending time, receiving time, count.

6. SIMULATION RESULTS

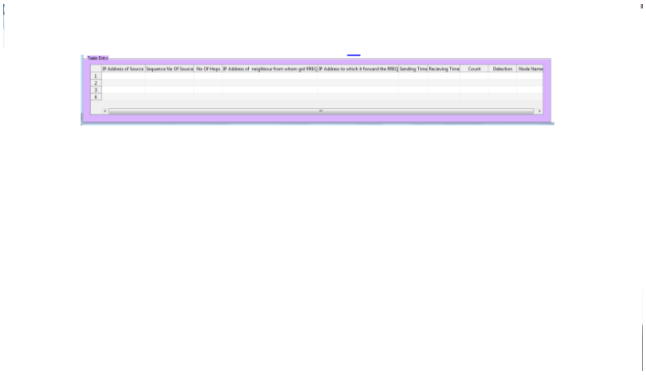
In this figure, 18 nodes are shown with unique name, unique IP address. In these 18 nodes, we have one source node and one destination node at a time through root can be set.



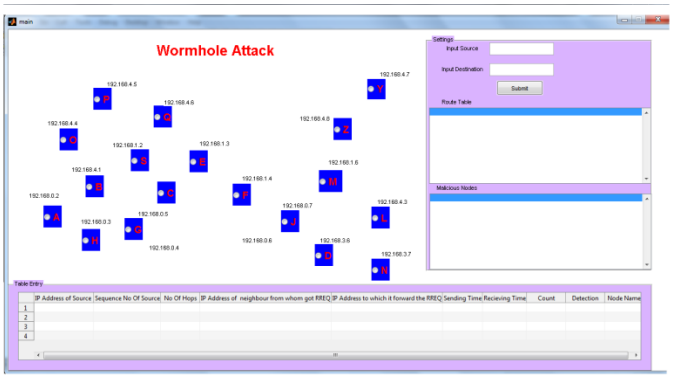
In this figure, an interface has created for providing input source and destination for showing route by submitting the input using submit button. Rout table shows name of nodes between source and destination travelled names and their IP address.



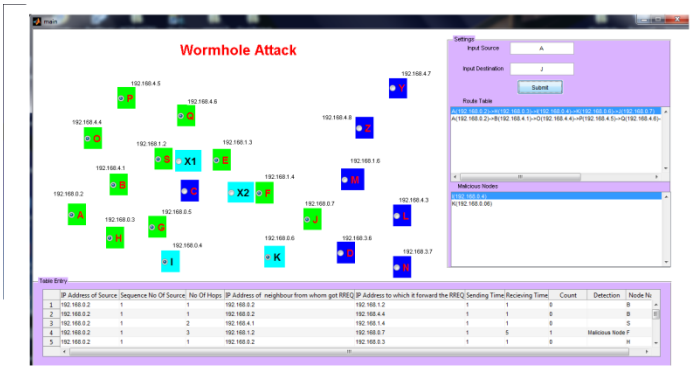
In this figure, a table is created for nodes traversed between source and destination, their sequence number, hops for around, RREQ information, send and receive time, count and detection of malicious nodes and name of nodes.



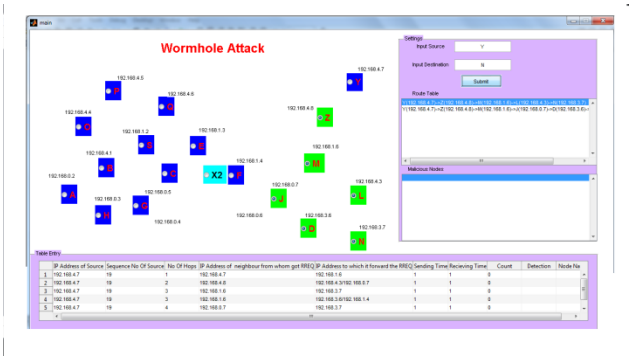
In this figure, a network of wireless nodes has been created and a source and destination text box is there to enter the source and destination and the path shows the route table and all the malicious nodes will be entered the column of malicious node.



In this figure, source as "A" & destination "J" are entered and then pressed submit. It shows that the path between A and J and I & K as malicious nodes.



In this figure, source as "Y" & destination "N" are considered and then pressed submit. It shows us the path between Y and N and no malicious nodes are there.



7. CONCLUSION & FUTURE SCOPE

In this paper best possible algorithm is given for wormhole prevention and detection using AODV protocol. It also provides a solution which is basically based on sequence number and IP address of sending nodes and receiving nodes.

For the future work, a better solution can be found

If we increase number of nodes and apply on ZRP.

REFERENCES

[1] L. Sudha Rani , R.Raja Sekhar [Ph.D] , "DETECTION AND PREVENTION OF WORMHOLE ATTACK IN STATELESS MULTICASTING", International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518

[2] Harbir Kaur, Sanjay Batish & Arvind Kakaria, "An Approach To Detect The Wormhole Attack In Vehicular Adhoc Networks" International Journal of Smart Sensors and Ad Hoc Networks [IJSSAN] ISSN No. 2248-9738 Volume-1, Issue-4, 2012

[3] Pushpendra Niranjan, Prashant Srivastava, Raj kumar Soni, Ram Pratap "Detection of Wormhole Attack UsingHop-Count And Time Delay Analysis" Information Technology, LNCT [RGPV] Bhopal, India International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012 1 ISSN 2250-3153

[4] Buch, Dhara Hitarth, and Devesh Jinwala. "Prevention of wormhole attack in wireless sensor network." arXiv preprint arXiv:1110.1928 [2011].

[5] Nishant Sharma, Upinderpal Singh, "A Location Based Approach to Prevent Wormhole Attack in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue. 1, 2014.

[6] Guowei Wu1, Xiaojie Chen1, Lin Yao1, Youngjun Lee2, and Kangbin Yim, "An Efficient Wormhole Attack Detection Method inWireless Sensor Networks", Computer Science and Information Systems 11[3]:1127–1141, Retrived 2014

[7] El Kaissi, Rouba Zakaria, Ayman Kayssi, Ali Chehab, and Zaher Dawy. "DAWWSEN: A defense mechanism against wormhole attacks in Nwireless sensor networks." PhD diss., American University of Beirut, Department of Electrical and Computer Engineering, 2005

[8] P. Hubaux, and L. Buttyan, "Mobility helps security in ad hoc networks", Proceedings of MobiHoc, 2011

[9] Subrat Kar, S Dharmaraja, " WHOP: Wormhole Attack Detection Protocol using Hound Packet" Dept CSE Indian Institute of Technology Delhi Hauz Khas, New Delhi , 2011 International Conference on Innovations in Information Technology.

[10] Jyoti Thalor, Ms. Monika, "Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks" Department of Computer Science &Applications Kurukshetra University, Kurukshetra Haryana, India, International Journal of Advanced Research in Computer Science and Software Engineering 3[2], February - 2013, pp. 137-142

[11] Kaur, Gurpreet, and Er Sandeep Kaur Dhanda. "'Analysing the effect of Wormhole Attack on Routing Protocol in Wireless Sensor Network'." International Journal of Advanced Research in Computer and Communication Engineering 2, no. 8 [2013]: 3217-3223.

[12] Saurabh Ughade, R.K. Kapoor, Ankur Pandey, " An Overview on Wormhole Attack in Wireless Sensor Network: Challenges, Impacts, and Detection Approach", International Journal of Recent Development in Engineering and Technology, [ISSN 2347 - 6435 [Online] Volume 2, Issue 4, April 2014]

[13] A. Pirzada and C. McDonald, "Detecting and evading wormholes in mobile ad-hoc wireless networks", International Journal of Network Security, 3[2]:191C202,

