ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Wormhole Prevention Protocols for Securing Ad Hoc Networks Using NS2

Steffi Saldanha [1], Smita Pawar [2], Mouris Silviya[3], Leena Mariaselvam[4]

B.E. Student, Department of Electronics and Telecommunication Engineering, Xavier Institute of Engineering College, Mahim, Maharashtra, India[1]

Professor, Department of Electronics and Telecommunication Engineering, Xavier Institute of Engineering College, Mahim, Maharashtra, India [2]

B.E. Student, Department of Electronics and Telecommunication Engineering, Xavier Institute of Engineering College, Mahim, Maharashtra, India[3]

B.E. Student, Department of Electronics and Telecommunication Engineering, Xavier Institute of Engineering College, Mahim, Maharashtra, India[4]

ABSTRACT- Creation of secure mobile ad-hoc networks is a major issue faced today. There are many attacks on the security of ad-hoc networks like the blackhole attack, sinkhole attack etc. In this paper we are focusing on the issue of "wormhole attack". This a severe attack on mobile ad-hoc networks. Wormhole attack is fairly difficult to defeat because in this attack new packets are mainly not created , the packets are simply replayed in the network. This attack affects the working of the routing protocol used in the network. There are quiet a few techniques available for avoidance of the wormhole attack like packet leaches, liteworp, cluster based etc. Our proposed solution involves the detection of malicious nodes and avoiding the routes containing the colluding nodes.

KEYWORDS - Ad-hoc, Manet, Network security,Ns-2,Wormhole.

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile hosts without fixed network infrastructure and also no centralized administration.[1]. The Ad Hoc Networks considers original, high quality and unpublished contributions addressing all aspects of ad hoc and sensor networks. MANET is done via multi-hop paths. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably.Ns-2 is an open source discrete event simulator used by the research community for research in networking [2]. It has supporting platform for several network protocols such as TCP, UDP, multicast routing, etc.It gives hands to both wired and wireless network. In practical wireless network coding systems face new challenges and attacks, whose impact and counter measures are still not well understood because their underlying characteristics are different from well-studied traditional wireless networks. The wormhole attack is one of these attacks.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

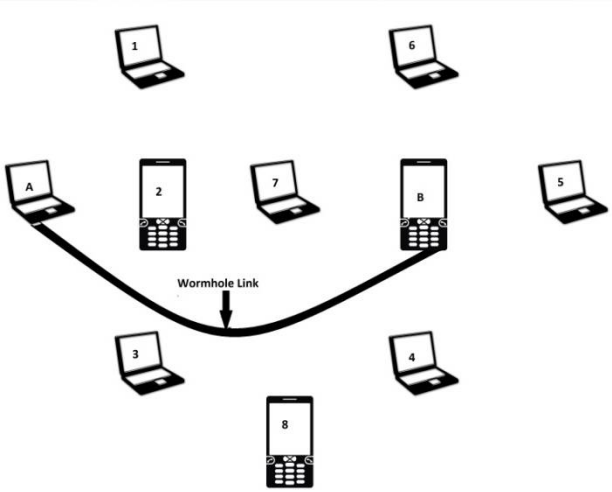

Fig. 1 Wormhole tunnel

In fig1 node A and node B are the malicious nodes .The wormhole link is created between these two nodes. There are two classes of wormhole attack: Hidden Mode (HM) and Participation Mode (PM) [3]. HM wormhole nodes does not contain routing packets, the purpose of this nodes are just to accept and forward packets which does not include in the routing table.PM nodes are totally opposite to that of HM nodes.PM nodes are visible during the routing process since they process routing packets as any normal node. Aside from relaying routing packets to its neighbors ,a PM wormhole node tunnels routing packets to the other PM node, giving it the opportunity to control network performance malicious nodes can carry out both Passive and Active attacks against the network. In passive attacks a malicious node only eavesdrop upon packet contents, while in active attacks it may imitate, drop or modify legitimate packets [4]. Among the two colluding nodes, one lies at the sender end while the other lies at the receiver end. Mahajan et al. [9] considered several terms for measuring the capacity of nodes involved in wormhole attack, terms considered were strength, length, attraction and robustness. There are various techniques that have been proposed for preventing the wormhole attack on a wireless network. For detection of wormhole attack, various techniques have been suggested. One of the technique expiry time of the packet is determined. Another technique is geographical leash, in which the position of the sender and its sending time is used to determine the distance between them. The most commonly cited wormhole prevention mechanism is 'packet leashes' by Hu et al [9].Packet leashes can be classified broadly as geographical leash and temporal leashes. Geographical leashes should work fine when GPS coordinates are practical and available [10]. As opposed to geographical leashes, temporal leashes require much tighter clock synchronization (in the order of nanoseconds), but do not rely on GPS information [10]. A leash using a timestamp requires accurate time synchronization, so that the receiver can detect if the packet traveled past the distance restricted by the leash; this approach is similar to TIK [11].

II. WORMHOLE ATTACK

In wormhole attack the wormhole acts as a shortcut path between two far off nodes. The wormhole nodes make the two distant nodes feel as instant neighbours and route their packets through them. The wormhole nodes are connected via a high speed wireless link or a long-range wireless transmission in a different band .The end-point of this link (wormhole nodes) is equipped with radio transceivers compatible with the ad hoc or sensor network to be attacked [5] .The wormhole attackers do not create separate packets - they simply replay packets already existing on the network, which pass all cryptographic checks. Since the packets are resent in the exactly same way, encryption or authentication alone cannot prevent the attacks. Other nodes cannot tell whether the packets are from the real originator or from the resender. A group of collusive attackers can form a wormhole that has as many ends as the number of malicious nodes.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Wormhole attacks put severe threats to ad hoc routing protocols. In the protocols that use distance vector technique, such as Ad hoc On demand Distance Vector protocol (AODV) [6] and Destination-Sequenced Distance Vector protocol (DSDV) [6], the hop count of a path affects the choice of routes. A pair of attackers can form a long tunnel and fabricate the false scenario that a short path exists between the source and the destination. The fake path will attract the data traffic. As soon as the packets are absorbed to the wormhole, the attackers can either drop them or compromise them. The path created between the two malicious nodes can be either an in-band or an out-of-band channel.

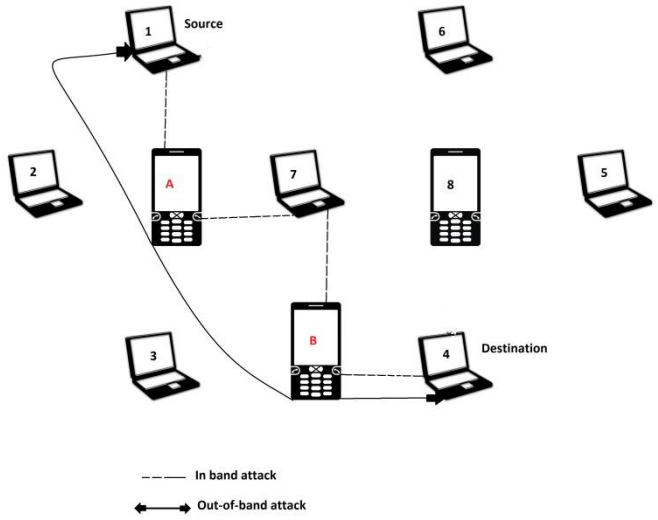

Fig 2 In band and out-of band attacks

The former is an open wormhole attack [7] while the latter is a closed or hidden wormhole attack. In the latter method the are transmitted between the malicious nodes via a dedicated wired or wireless link. Wormhole attack is one of the Denial-of-Service attacks. Denial-of-Service attacks attempts to make resources unavailable to legitimate users.

III. SOLUTION

The proposed technique is based on the comparison of the control packets with the data packets in the network. The AODV protocol is used for implementing the technique. Aodv is a distance vector routing protocol , in this protocol the routes are established on demand that is, only when there is a necessity for communication between two nodes. The fig 3 shows aodv forward and reverse route set up.

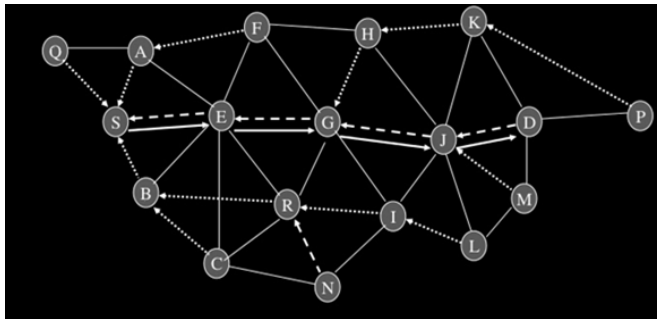

Fig 3- Path setup (a) ← – – : reverse path formation, (b) ⟶ : forward path formation

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

In AODV protocol the RREQ and RREP packets are considered as the control packets. These packets are sent for route discovery from source to destination. The RREQ packet is broadcasted in the network till it reaches the destination. The destination does not further broadcast the RREQ packet. Now, as a malicious node generates its own fake reply packet which states that it has the shortest route to the destination. Everytime a RREQ is recieved by the malicious node it will send the fake packet to the sender of the RREQ, this will in turn increase the control packets in the network as compared to the data packets. In such a condition the node sending the RREP is considered as a potential wormhole node. Hence this node is eliminated from the network.

Table.1 Simulation parameters

Parameter	Value
Simulator	NS-2
Protocols studied	AODV
Simulation time	150 sec
Simulation area	500 x 500
Transmission range	250 m
Node movement	Random
Traffic type	UDP
Data payload	512 Bytes / packet

The table.1 contains information about the simulation environment in NS2. The simulation parameters that were selected for the testing are mentioned in the table.1.

Algorithm

1. Since AODV is an on demand routing protocol the route discovery begins only when there is a need to send data from source to destination. For the purpose of route discovery the source node broadcasts the RREQ packets.
2. The intermediate node that receives the RREQ packet checks the destination address. If the destination address does not match then the packet is forwarded.
3. On receiving the RREQ packet each node update their routing table
4. When the destination node receives RREQ message from its neighboring nodes, it then unicast the RREP back to the source node.
5. Attacker is now interested in converting a node.If it is in the path then a node at random is selected by the router to be the malicious node.
6. Malicious node creates its own false reply packet which contains (destination address and source address, data rate, default $random $node_id).
7. Malicious node unicasts the RREP and tells source that it has the shortest path to destination.
8. A malicious node keeps sending replies stating that it has the shortest route , due to this the number of control packets increase in number as compared to its data packets .
9. if { $control> $data } {
set Thresh_ $CPThresh_ | $CSThresh_| $RXThresh_
set $Thresh > $ini_Thresh || $Thresh < $ini_Thresh
$transmit $ack($n($i))
10. Hence the malicious node is detected and not used for future communications.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

IV. EXPERIMENTAL RESULTS

Network with wormhole attack**:** In this simulation wormhole attack is detected after completing the following steps: The following figures are of the screenshot of simulation of node deployment, wormhole detection. Here the black nodes are indicating wormhole node. In the graphs the red line shows the throughput and packet loss respectively during a wormhole attack.

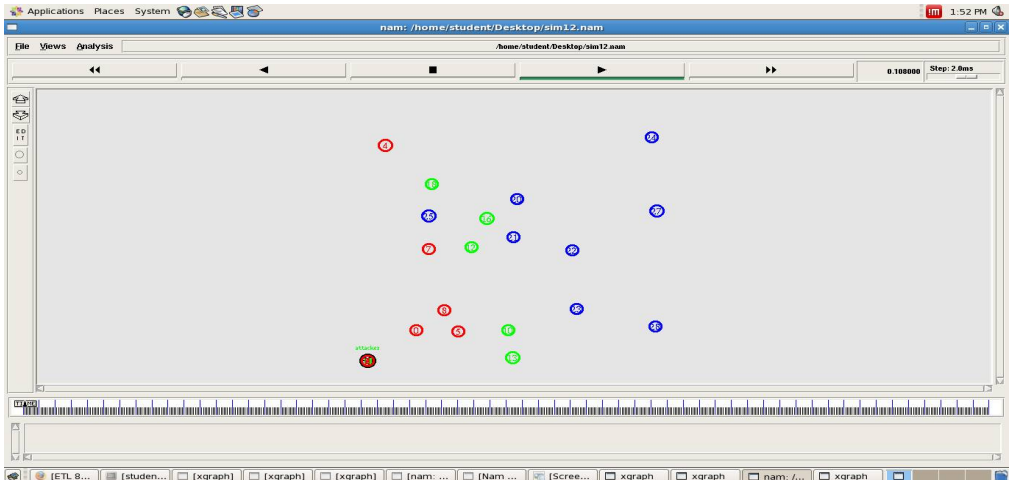

Fig 4 Node deployment in NS2

The Fig 4 shows the stage1 of the simulation. In the stage1 the deployment of the wireless network using the AODV protocol is accomplished.

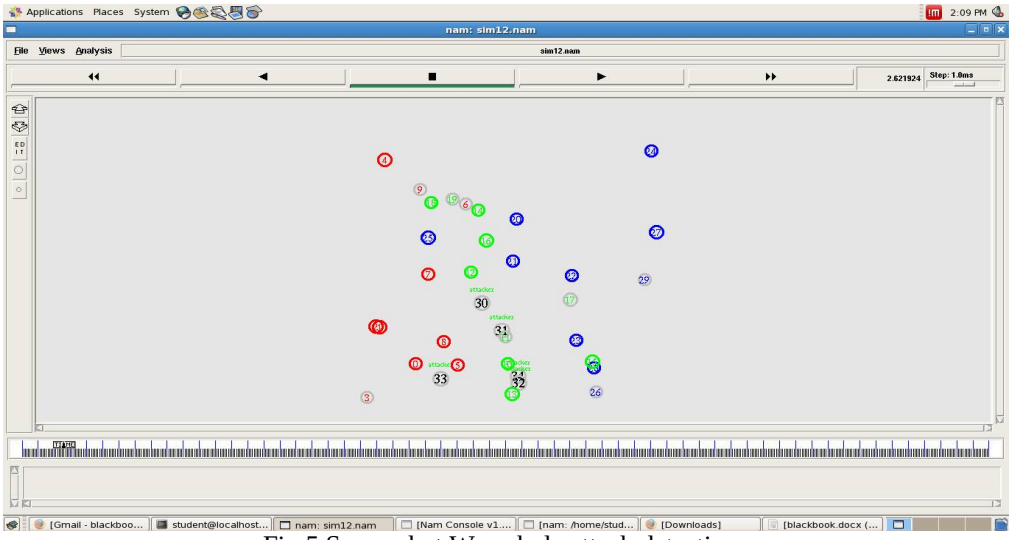

Fig 5 Screenshot Wormhole attack detection.

The Fig 5 shows the stage2 of the simulation. In the stage2 the nodes 30,31,32 and 33 are detected as potential wormhole nodes. The detection is based on the algorithm mentioned earlier in the paper. Following are the graphs based on the network parameters such as throughput and packet loss.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

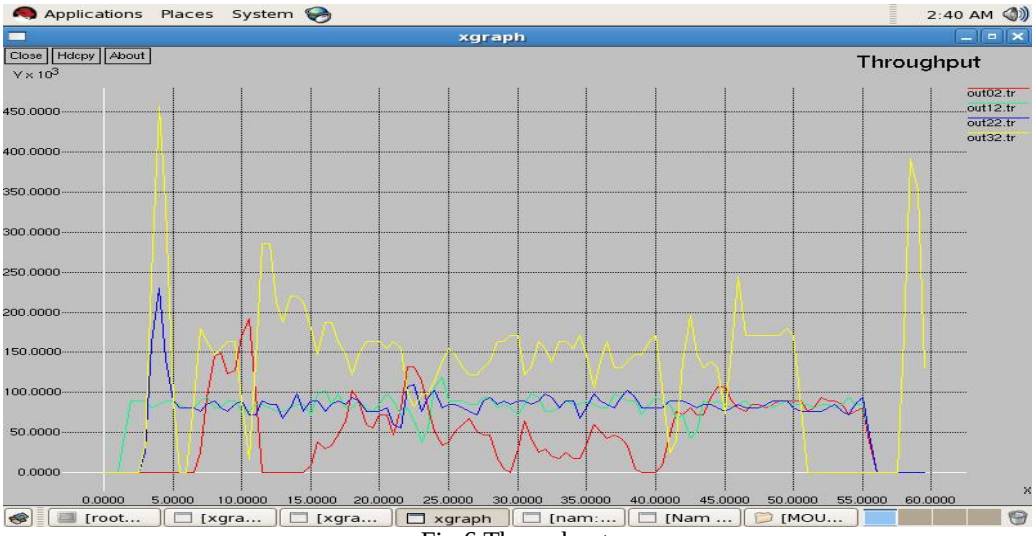

Fig 6 Throughput

The network throughput is the average of successful message delivery over a communication channel. This data may be delivered over a physical or logical link. In our simulation the data is passed through a wireless channel.The Fig 6 shows the throughput of the network. As it can be seen in the Fig 6,the throughput decreases in the presence of a wormhole link. The red graph indicates the throughput in the presence of a wormhole link.

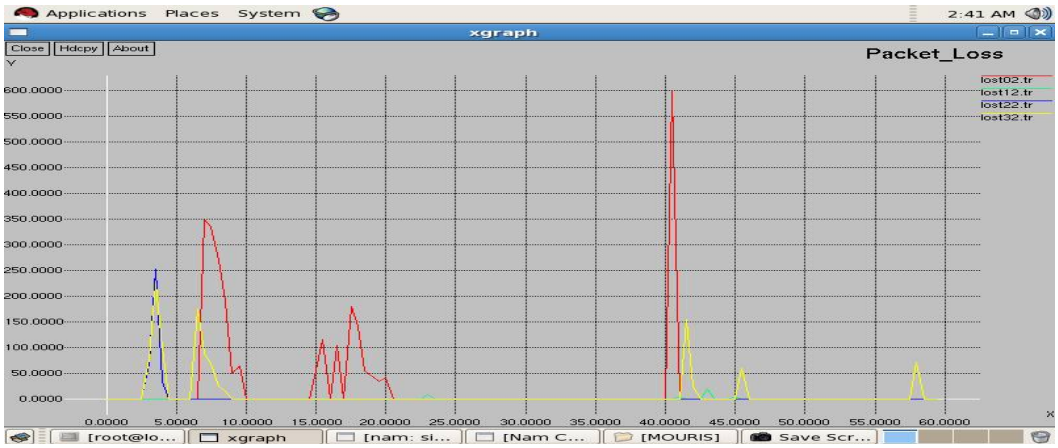

Fig 7 Packet_loss

Packet loss in a wireless communication is the difference between the generated and received packet.The Fig 7 shows the packet loss of the network. As it can be seen in the Fig 7, the packet loss increases in the presence of a wormhole link. The red graph indicates the loss of packet in the presence of a wormhole link.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

V. CONCLUSION

In conclusion of this paper, we would like to believe that we meticulously explained the notion of a wormhole attack in an ad-hoc network and also stated a technique for the detection and prevention of the wormhole attack in ad-hoc networks. The approach detects the wormhole attack in mobile ad hoc networks using AODV routing protocol by comparing the control and data packets for a node. The algorithm is simple. This method does not require any specialized hardware or synchronized clocks, but detects the presence of a wormhole. The algorithm is implemented on a small network using NS2. The simulation results confirm the proposed solution which successfully detects wormhole nodes.

REFERENCES

[1] Chandraprabha Rawat Master's in Software system, Department of computer application, Samrat Ashok Technological Institute, Vidisha, India. "A Review: Wormhole attack In Mobile Ad Hoc Network.", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 3, March 2013.
[2] ns-2 Home page :http://www.isi.edu/nsnam/ns/
[3]Khabbazian M., Mercier H., Bhargava V.K. NIS02-1: "Wormhole Attack in Wireless *Ad Hoc* Networks: Analysis and Countermeasure." Proceedings of the Global Telecommunications Conference (GLOBECOM '06); San Francisco, CA, USA.; pp. 1–6, 27 November–1 December 2006.
[4] A. A. Pirzada and C. McDonald, "Kerberos assisted authentication in mobile ad-hoc networks", in Proceedings of the 27th Australasian Computer Science Conference (ACSC), 2004.
[5] Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak.UIET, MD University,Rohtak, India dr.yudhvirs@gmail.com. "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks" Third International Conference on Advanced Computing & Communication Technologies. 978-0-7695-4941-5/12 $26.00 © 2012 IEEE DOI 10.1109/ACCT.2013.68; 2012
[6] W. Wang, B. Bhargava, Y. Lu, X. Wu, "Defending Against Wormhole Attack In MANETs", under review at Wiley Journal Wireless Communication and Mobile Computing (WCMC), vol.6, pp-483-503, 2006.
[7] M.A. Azer S.M. El-Kassas A. Wahab F Magdy S and El-Soundani. "Intrusion detection for wormhole attacks in ad hoc networks a survey and a proposed decentralized scheme". In the proceedings of the IEEE international conference on availability, reliability and security, pages 630–646, 2008
[09] Y.-C. Hu, A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing", Security and Privecy Magazine, IEEE,vol. 2, issue 3,pp. 28-39, May 2004.
[9] Y.-C. Hu, A. Perrig, D. B. Johnson; "Packet leashes: a defense against wormhole attacks in wireless networks"; INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, Vol. 3, pp. 1976-1986, 2003.
[10] D. Barman Roy, R. Chaki, N. Chaki, "A new cluster-Based Wormhole Intrusion Prevention Algorithm for Mobile Ad-Hoc Networks", International journal of network security and its application, vol.1, pp-44-52, 2009.
[11] Y. Chun- Hu , A. Perrig, B. Johnson David, "Wormhole Detectionin Wireless Ad Hoc Networks", In Ninth International Conferenceon Network protocol (ICNP), vol.1, 2002.