IJEE Volume 5 • Number 1 • January-June 2013 pp. 73-75 © Serials Publications, ISSN : 0973-7383

Mechanism for Detection and Reaction Wormhole Attack in AODV

Anand Singh[1], Saurab Shrivastava[2], Jitendra Kumar Gupta[3], and Anil Singh[4]

[1]*M.Tech Scholar, Deptt. of Comp. Science & Engg, SR Group of Institution, Jhansi, India*
E-mail: bisenanand82@gmail.com

[2]*Associate Professor, Deptt of Comp. Science, Bundel Khand University, Jhansi, India*
E-mail: hanu.saurabh@gmail.com

[3]*Asstt. Professor, Deptt. of Comp. Science & Engg., SR Group of Institution, Jhansi, India*
E-mail: jitendra1503@gmail.com

[4]*Associate Professor, Department of Computer Science, VITM, Gwalior, India*
E-mail: itanilmits@yahoo.co.in

Abstract: The lack of centralized infrastructure in ad hoc network makes it vulnerable to various attacks. MANET routing disrupts if participating node do not perform its intended function and start performing malicious activity. A specific attack called Wormhole attack enables an attacker to record packets at one location in the network, tunnels them to another location, and retransmits them into the network. In this paper, we provide a mechanism for detecting and reaction wormhole attacks without use of any special hardware such as directional antenna. This mechanism able to provide in establishing a method to reduce the rate of refresh time and the response time to become more faster.

Keywords: Ad hoc network, Sensor network, Wormhole attack.

1. INTRODUCTION

An ad-hoc network is inherently a self-organized network system without any infrastructure. Typically, the nodes act as both host and router at the same time i.e. each node participates in routing by forwarding data for other nodes and deciding which nodes forward data next based on the network connectivity. The proliferation of wireless devices also stimulates the emergent applications in wireless ad hoc network. However, the realization and wide deployment of such network face many challenges. Security is one of the most challenging problems as the operation environment of such network is usually unpredictable and the existing mechanisms such as routing protocols assume a trusted environment. Hence any malicious behavior could disrupting the normal operation of the networks. Wormhole can be formed using in-band channel where malicious node m1 tunnels the received route request packet to another malicious node *m*2 using encapsulation even though there is one or more nodes between two malicious nodes, the nodes following *m*2 nodes believe that there is no node between m1 and *m*2. Second, out-of-band channel where two malicious nodes *m*1 and *m*2 employ an physical channel between them by either dedicated wired link or long range wireless link

The purpose of this work is overcome a special attack called wormhole attack launched by at least two colluding nodes within the network. In this paper we enhance AODV to detect and reaction wormhole attack in real-world mobile ad hoc networks.

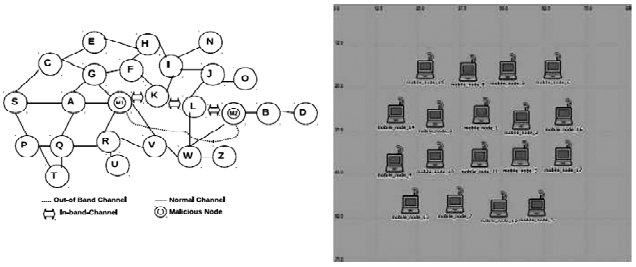


Figure 1: Wormhole Attack

2. RELATED WORK

Two types of wormhole attacks have been discussed in the literature: hidden wormhole attack and exposed wormhole attack. The former is the conventional wormhole attack in which the adversary records and retransmit packets verbatim. This attack can be easily mounted using only hardware introduced by the attacker and without compromising any hosts in the network. Thus, it is more challenging to be detected. In multi hop wireless systems, such as ad hoc and sensor networks, mobile ad hoc network applications are deployed, security emerges as a central requirement. A particularly devastating attack is known as the wormhole attack, where two or more malicious colluding nodes create

a higher level virtual tunnel in the network, which is employed to transport packets between the tunnel end points. These tunnels emulate shorter links in the network. In which adversary records transmitted packets at one location in the network, tunnels them to another location, and retransmits them into the network. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality.

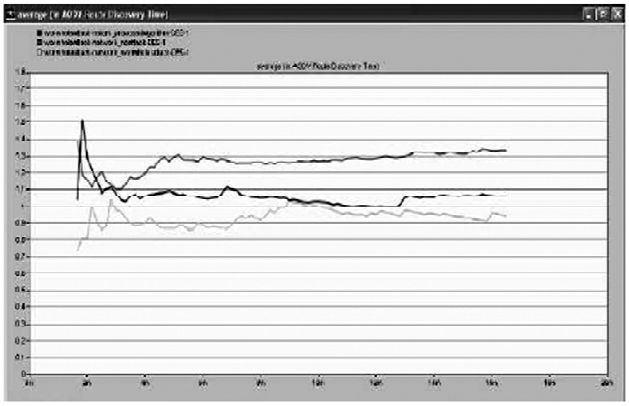


Figure:

3. OPERATION OF AODV-DR

Our proposed solution i.e. AODV-DR not only detects but also reaction the wormhole attack without the use of any special hardware. The proposed solution handles wormhole attack that is launched by two colluding node. Colluding nodes have the capability to communicate with all other nodes. All nodes are considered in promiscuous reception mode and are bidirectional. The colluding nodes use wireless capability that is of larger range than other normal nodes in the network. The operation of the proposed solution for wormhole attack can be categorized in two steps:

Detection of colluding node

Reaction of colluding node

Detection and Reaction of Colluding Node

Normally in AODV (Perkins, Belding Royer & Das, 2003) all intermediate nodes that have no route to destination node rebroadcast RREQ forwarded by the originator of the RREQ. The source node/intermediate node keeps record of all the next neighbors from which it listen RREQ during rebroadcast. The following information is maintained by each node while broadcasting RREQ from originator node to destination node:

Originator ID

Originator Seq#

RREQ ID

Neighbor Node ID

Timer

Maintaining this information at all nodes insure detection of any node conducting wormhole attack. As the colluding node, its rebroadcast of RREQ is not listened by the neighboring intermediate nodes, instead it forwards the RREQ to its colluding partner, and the forwarding neighbours of malicious node therefore do not listen to rebroadcast from the malicious node M1. As shown in Figure 1 in introduction section, the wormhole attackers establish a shortcut link between source node and destination node having least number of hops, therefore path having wormhole link will be selected, as RREQ packet reached by destination node in short period of time as compared to RREQs reached by other normal paths.

The working of our proposed scheme is summarized as:

(*i*) RREQ is created by source node and broadcast it to all neighboring nodes which are in its communication range.

(*ii*) RREQ is rebroadcasted by all receiving nodes of RREQ until received by destination.

(*iii*) The sending nodes of RREQ listen to the rebroadcast from all its neighbors, before discarding such RREQs they keep record of their IDs as next neighbor nodes. All normal nodes in MANETs get list of information as mentioned in the network.

(*iv*) If receiving node of RREQ is malicious, its rebroadcast is not listened by normal neighboring nodes, because it unicasts RREQ to its colluding partner, thus all its neighbors will not hear from it and they will be unable to record their ID.

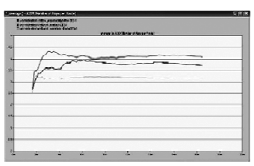
(*v*) As shown in Figure 1, normally RREQ is reached to destination through route having colluding nodes due less number of hops and low latency as compared to other normal available normal routes.

(*vi*) The RREP packet is created by destination node and is unicasted through the reverse route.

(*vii*) The receiving node of RREP on reverse route will check if there exists an ID of the sending node of RREP in its maintaining information, if yes it will forward the RREP to next hop on reverse route towards the source node, otherwise, the receiving node regards that node as malicious and is blacklisted and future communication through that node is blocked.

(*viii*) Another alternative route having no malicious node is then selected for data communication.

Parameters	Description
Examined Protocol	AODV
Simulation Time	1000 sec.
Simulation Area	80x80 m
Number of Nodes	18
Malicious Nodes	02
Number of Wormholes	01



4. CONCLUSION AND FUTURE WORK

In this paper a practical solution called AODV-DR, that use uses neighbor ID for detection and reaction of wormhole attack with accuracy. The solution we have proposed is practical in the sense that it does not require any additional hardware. The memory and computational cost is reasonable enough to be supported by nodes in MANETs. Also instead of simulation we implemented it on test bed containing 8 nodes using existing hardware. Although our schemes detect and handle open wormhole attack successfully, however, incase of impersonation attack when a malicious node hides its identity with some normal node, our scheme fails, for which we require strong authentication scheme. In future we plan to embed some authentication scheme to overcome this deficiency in our scheme.

References

[1] Corson, M.S, Maker, J.P. and Cernicione, J.H. (1999). Internet-Based Mobile Ad Hoc Networking. *IEEE Internet Computing*, pp. 63-70.

[2] Perkins,C.E., Belding Royer, E.M. and Das, S.R. (2003). Ad-hoc On-Demand Distance Vector (AODV) Routing. Mobile Ad-hoc Networking Group, Internet Draft, Draft-Ietf-Mendatory-00.txt.

[3] Jhonson, D.B. and Maltz, D.A. (1996). "Dynamic Source Routing in Ad Hoc Wireless Networks". *In Mobile Computing, edited by Tomasz Imielinski and Hank Korth*, Chapter 5, Kluwer Academic Publishers, pp. 153/181.

[4] Perkins, C.E. and Bhagwat, P. (1994). "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", *Proceedings of the SIGCOMM 94 Conference on Communication Architecture, Protocols and Applications*, pp. 234-244.

[5] Argyroudis, P.G. and O'Mahony,D. (2003). "Secure Routing for Mobile Ad Hoc Networks", *IEEE Communications Surveys, the Electronic Magazine of Original Peer-Reviewed Survey Articles*, **7**(3).

[6] Jhaveri, R.H., Parmar, J.D., Patel, A.D., and Shah, B.I. (2010). "MANET Routing Protocols and Wormhole Attack Against AODV", *International Journal of Computer Science and Network Security, 10*(4).

[7] Roy, D.B., Chaki, R & Chaki, N. (2009). A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad Hoc Networks. *International Journal of Network Security and its Applications* (*IJNSA*), **1**(1).

[8] Shang-Ming Jen, Chi-Sung Laih and Weh-Chung Kuo. (2009). "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", Sensors, ISSN 1424-8220, 9, 5022-5039; doi:10.3390/s90605022, 2009.

[9] Panaousis, E.A., Nazaryan, L. & Politis, C. (2009). "Securing AODV Against Wormhole Attacks in Emergency Manets Multimedia Communications", Mobimedia'09, 2009, London, UK. Win, K.S. & Gye,P. (2008).

[10] Analysis of Detecting Wormhole attack in Wireless Networks. *World Academy of Science, Engineering and Technology* **48.** Tun, Z & Maw, A.H. (2008).

[11] Wormhole Attack Detection in Wireless Sensor Networks. *World Academy of Science, Engineering and Technology* **46.** Ming-Yang Su and Kun-Lin Chiang. (2010).

[12] Prevention of Wormhole Attacks in Mobile Ad Hoc Networks by Intrusion Detection Nodes. Springer Berlin / Heidelberg, 6221, pp. 253-260.

[13] AODV-UU.(n.d.). http://core.it.uu.se/AdHoc/AodvUU Impl

[14] Azer, M., El-Kassas, S. & El-Soudani, M. (2009). "A Full Image of the Wormhole Attacks: Towards Introducing Comlex Wormhole Attacks in Wireless Ad Hoc Networks". *International Journal of Computer Science and Information Security* (*IJCSIS*), **1**(1).