A Cluster based Technique for Securing Routing Protocol AODV against Black-hole Attack in MANET

[#1]Sonam Yadav, [#2] Kanika Lakhani

[#1]Student, Manav Rachna College of Engineering, Faridabad,
ssonamyadav89@gmail.com
[#2]Assistant Professor, Manav Rachna College of Engineering, Faridabad,
kanikalakhani@yahoo.co.in

ABSTRACT

Mobile ad-hoc networks are prone to various security vulnerabilities because of its characteristics mainly high mobility of nodes, and no well defined architecture. Security measures are difficult to implement as there is no central administration. Several attacks on Mobile ad-hoc network have been identified so far and Black hole attack is one of them. In this paper we discuss black hole attack on Ad-hoc network and propose a solution to the hijacked node behaving as black hole node. A scenario has been considered where a node inside network has been intruded and compromised to cause black hole attack. The proposed security solution modifies original AODV using a hierarchical based intrusion detection method to identify hijacked node and exclude the particular node from network.

KEYWORDS

Black hole, cluster, hijacked node.

1. Introduction

Mobile Ad-hoc network is an autonomous system in which nodes are connected over wireless links. Whenever nodes coexist in neighbourhood they instantly establish a network in order to communicate with each other. Mobile Ad-hoc network do not posses any concrete infrastructure as there is no centralized administration, nodes are highly mobile and lack of infrastructure, routing protocols and security measures are difficult to implement. Usually nodes follow dynamic topology concept, where nodes are allowed to move freely in the network. Any node can either join or leave the network at any time without prior notification. If two nodes lie within transmission range of each other, they can communicate through intermediate nodes. Mobile ad-hoc network are more vulnerable to security threats than wired network due to following characteristics:

1 highly dynamic topology
2 No centralize administration
3 No concrete infrastructure
4 Limited resources viz. battery power,
5 Limited bandwidth
6 Energy constrained operations

DOI : 10.5121/ijdps.2013.4202

a. Ad hoc On Demand routing Protocol

In ad hoc network routing protocols are classified under two categories by Royer and Toh(1999):

a) Proactive or periodic
b) Reactive or on-demand routing protocol

[2] describes that in proactive routing protocol, nodes exchange routing information with each other periodically to know the current routes to all other nodes[3]. In reactive protocols, routing information is exchanged only when a particular node needs to send data packet to destination node. DSR[5], AODV[6], LAR[9] are some existing examples of On demand routing protocols.

Ad-hoc On Demand Distance Vector (AODV) has been discussed in [12]. It is an on demand routing protocol which discovers path form one node to destination node only when sender node needs to send data packets. Route is discovered through intermediate nodes with the help of control messages such as Route Request (RREQ) and Route Reply(RREP). Dest_seq_no and hop_count is associated with each node. Node having highest Dest_seq_no specifies fresh route to the destination. When sender node wants to establish path to destination node, it broadcast RREQ message. Intermediate nodes rebroadcast the RREQ to their corresponding neighbour nodes. The node which has fresh route to the destination generates RREP and unicast to the sender node. [12] Describes the complete structure of AODV along with header information. If RREP message is not received within a certain threshold, RREQ is broadcasted again. Traffic control and route discovery is straightforward.

b. Black Hole attack

Generally attacks can be classified as External and Internal. Nodes that are not part of network, attacks inside nodes cause external attack. Legitimate nodes that are compromised to attack other nodes within same network causes internal network. There can be Passive and Active attacks too. In active attack normal functioning of network is disrupted whereas in passive attack information is snooped by intruder, functioning of network operations are not interrupted.

[1] Classified security attack in ad hoc networks according to the network protocol stack. There are numerous attacks mentioned in table below, our main purpose behind this paper is to highlight the black hole attack.

APPLICATION LAYER	Repudiation, Data corruption
TRANSPORT LAYER	Session hijacking, SYN flooding
NETWORK LAYER	Wormhole attack, Black hole attack, location disclosure attack
DATALINK LAYER	Traffic analysis, Disruption MAC(802.11)
PHYSICAL LAYER	Eavesdropping, interceptions, jamming

Black hole attack has been discussed by Deng et.al.[8] , it acts upon network layer which is imperative in establishing connection in a network. Black hole attack hinders the data transmission by not forwarding the data packets towards destination. When malicious node receives RREQ, it advertises itself as having shortest path to destination by quickly generating RREP with highest dest_seq_no, source node dumps all other RREP perceiving that malicious

node has fresh route to the destination. Malicious node receives data packets from sender but do not forward it further. Malicious node or the black hole node degrades performance, deprives traffic from source node and causes denial of service. In [13] performance of a network under the effect of black hole node has been compared by simulating ad-hoc network with and without black hole node.

2. Related Work

M.Umaparvathi et.al in [2] has proposed two-tier secured AODV to detect single node acting as a black hole along with group of nodes collectively contributing to black hole attack. Tier 1 detects single black hole node using verification message. Whereas tier 2 detect group of nodes creating black hole attack using Rc number of Control messages and Rm number of data packets.

Various Intrusion Detection Systems in Manet has been proposed so far. In [11] Sevil has raised various issues in implementing Intrusion Detection System in ad-hoc networks.

[1] has surveyed various types of Ids in manet such as Distributed and Co-operative IDS proposed by Zhang and Lee[7], Hierarchal based IDS which provides multilayered architecture, Distributed Intrusion Detection System using multiple sensors[4] etc .

[3] Murugan et.al has proposed cluster based technique to detect misbehaviour, isolate and authenticate nodes using cluster based technique and threshold cryptography. The proposed scheme has used Proactive Secret sharing technique to share secret key among nodes which is deployed along with threshold cryptography to provide more security.

3.Proposed work

Proposed method works upon Hierarchal based IDS in which nodes are divided in clusters. Using threshold cryptography and Proactive sharing scheme [12] key is distributed among member nodes. Node with maximum 1 hop count is chosen as Cluster Head (CH). Proposed work modifies original AODV using cluster based technique to detect hijacked node causing black hole attack inside network.

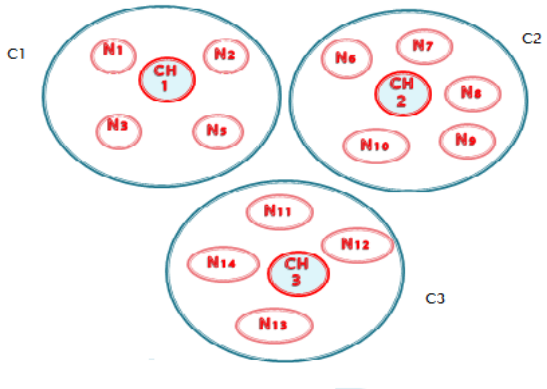

Fig 1. Cluster of Nodes

Let us suppose N1 be the source node, D is the destination node which can be either in same cluster or different cluster. IMn be the intermediate nodes where n= 2, 3, 4…

During route discovery phase source node N1 request cluster head (CH1) to issue certificate. CH issues certificate to source node, after checking its trust value. Source node broadcast RREQ (route request) to all its neighbours. RREQ would be of following format:

RREQ< IPs, IPd, IDb, Seqs, Seqd, Cert, Hop_count >

Here IPs, IPd, is the IP address of source and destination respectively. IDb denotes the broadcast Id, Cert represents Certificate issued by Cluster Head. Hop_count depicts number of nodes message have passed. When RREQ reaches IMn there can be three cases, which are as follows:

CASE1: Intermediate node (IMn) has no route to destination.

In this case IMn would rebroadcast RREQ to its neighbours; a reverse path pointer is set to the node from which it received RREQ or source node. Hop_count field is incremented by 1. IMn would also add its own IP address to the rebroadcasted RREQ.

CASE2: IMn is Destination itself.

Destination unicast Reply to next hop towards source node. Source node on receiving Reply from source node, transfers the data packet to destination and waits for acknowledgement.

CASE3: IMn has fresh route to destination.

If IMn has fresh route to destination, it generates RREP and forwards it towards source along with IP address of the nodes which comes in between the path from source to destination. Source node chooses IMn with higher sequence number and extracts the path details mentioned in RREP. Source stores the path details until it receives acknowledgement from destination. The format of RREP will be as such:

RREP < IPs, IPd, IDb, Seqs, Seqd, SeqIM, Cert, Hop_count , detail (IPi) > where i=1, 2, 3, 4…
IPi is the IP address of all the nodes which comes in between the path. i denotes the number of nodes. IPi is stored temporarily and dumped once source gets assure that data packet has reached to destination.

In proposed method all the nodes receiving data packet send acknowledgement to the node from which it received it. If source node receives acknowledgement from destination within threshold time, path is found to be secure against black hole node and originator takes no action. Otherwise source starts verifying nodes. Source node unicast verification message to all the nodes whose details it has stored. Through verification message Source asks the corresponding nodes to reply either TRUE or FALSE. If IMn has received acknowledgement from its next node it replies TRUE otherwise FALSE. We assume that hijacked node would always intend to hide itself.

Suppose in above figure N6 is the source node and N10 is the destination. N7, N8, N9 are the intermediate nodes whose details has been stored by N6.

N6 unicast verification message to N7, N8, N9 and N10. Upon receiving verification message each IMn replies either TRUE or FALSE to source. N6 might receive TRUE, FALSE or no reply.

Suppose a scenario where N7 replies TRUE, N8 and N10 replies FALSE, and N9 does not reply at all. In that case N9 is assumed to be hijacked node which acted as black hole node and did not forward the data packet. Alarm has been raised by source node and N9 is excluded from network. Source node analyse black hole node by considering different combination of TRUE or FALSE messages.

4. Conclusion

The proposed algorithm uses Hierarchal based Intrusion Detection system along with threshold cryptography. It detects the hijacked node and raises an alarm to alert other nodes inside network. The process of verification would be quick and small to reduce overhead and compatible with mobility of nodes. Proposed algorithm would be suitable for military battleground as chances of node being hijacked are more there.

5. Future Work

The proposed work would be implemented in a software programming language and it would be compared with original AODV using Network Simulator on the basis of cost, throughput, end to end delay, packet delivery ratio etc. Future work will also include improvement in proposed algorithm regarding network congestion other perspectives.

References

[1] H.N.Pratihari, “Intrusion Detection System (IDS) for Secure MANETS: A Study,” Department of Electronics & Telecommunication from Orissa Engineering College,Jan-Feb 2012.

[2] M.Umaparvathi,Dharmishtan K.Varughese, “Two Tier Secure AODV against Black Hole Attack in MANETs” European Journal of Scientific Research, ISSN 1450-216X Vol.72 No.3(2012),pp,369-382

[3] R.Murugan, A.Shanmugam“Cluster Based Node Misbehaviour Detection, Isolation and Authentication Using Threshold Cryptography in Mobile Ad Hoc Networks”International Journal of Computer Science and Security ISSN 1985-1553 volume :6;Issue:3;Start page:188;Date:2012

[4] O. Kachirski and R. Guha, “Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), p. 57.1, January 2003

[5] David B. Johnson, David A. Maltz, Yih-Chun Hu, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), Internet-Draft, draft-ietf-manet-dsr-09.txt, 15 April 2003, http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt

[6] Charles E. Perkins , Elizabeth M. Belding-Royer , and Samir R. Das, Ad hoc On-Demand Distance Vector(AODV) Routing, RFC 3561,July 2003http://www.ietf.org/rfc/rfc3561.txt.

[7] Y. Zhang, W. Lee, and Y. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks, "ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[8] Haining Wang, Danlu Zhang, and Kang G. Shin, Detecting SYN Flooding Attacks, IEEE INFOCOM'2002, New York City, 2002

[9] Deng, H., Li, W., Agrawal, D., "Routing Security in Wireless Ad Hoc Networks" IEEE Communication Magazine (October 2002) pp. 70-75

[10] Young-Bae Ko and Nitin Vaidya, Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. In Proceedings of the Fourth International Conference on Mobile Computing and Networking (MobiCom’98), pages 66–75, October 1998.

[11] Shree Murthy and J.J.Gracia-Luna-Aceves, “ An Efficient Routing Protocol for Wireless Network”, Mobile Networks and Applications, 1(2):183-197,1996

[12] Perkins, C.E., Royer, E.M., "Ad-hoc on-demand distance vector routing",www.cs.ucsb.edu/~ravenben/classes/papers/aodv-wmcsa99.pdf

[13] Dokurer,Erten,Acar, “Performance analysis of ad-hoc networks under black hole attacks”.

Authors

Sonam Yadav is currently pursuing Mtech in Computer Science from" Manav Rachna College of Engineering", Faridabad. She is B.Tech in Information Technology from "Gurgaon Institute of Technology and Management", Bilaspur. Her areas of interest include Networking and Artificial Intelligence.

Kanika Lakhani is currently working as Assistant Professor at Manav Rachna College of Engineering, Faridabad and is pursuing P.hd in the field of Mobile Ad hoc Networks. She has 5 years of teaching experience and 2 years industry experience. She has over 20 publications in various national/ international journals/ conferences. She has attended various workshops and seminars. She has also presented expert lectures in various institutions. Her areas of interest include MANET, Neural Networks, Artificial Intelligence and Security.