Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Remote Sensing 74 (2014) 26794-26796

ISSN: 2229-712X

Intelligent self adaptive routing mechanism for AODV against black hole attack in manet

Rashmi Mishra* and Harsh Khatter

CSE Department, ABES Engineering College, Ghaziabad, U.P, India.

ARTICLE INFO

Article history:

Received: 19 April 2014;

Received in revised form:

21 August 2014;

Accepted: 29 August 2014;

Keywords

Manet, Aodv, Routing algorithms, Network Security, Black Hole.

ABSTRACT

Ad Hoc Network provides quick communication among knob to convey the packets from one knob to other. These networks are independent of any fixed infrastructure or central entity like cellular networks [10] which requires fixed infrastructure to operate. Any malicious knob in the network can disturb the whole process or can even stop it. Several attacks like Replay attack, black hole, wormhole, rushing etc [13], in which legitimate knob behaves like malicious knob and disturbed whole the network. To define and detect the malicious behavior of a knob, it becomes obligatory to define the regular and malicious behavior of a knob. Whenever a knob exhibits a malicious behavior under any attack, it assures the breach of security principles like availability, integrity, confidentiality etc [13].

Introduction

Literature Review

In Year 2012 Ms. Nidhi Sharma et. al. proposed solution for Black hole attack in MANETs- Source node waits for the RREP packet to arrive from more than two nodes. During this time, the two or more nodes/hops shared the redundant paths. From these shared hops the source node can recognize the safe route to the destination. If no shared nodes appear to be in these redundant routes, the sender will wait for another RREP until a route with shared nodes identified or routing timer expired. This solution can guarantee to find a safe route to the destination, but the main drawback is the time delay. If there are no shared nodes or hops between the routes, the packets will never been sent[2][6].

In year 2012 Mr. Rutvij H. Jhaveri et. al. proposed a noval approach for black hole and gray hole attacks in Mobile ad-hoc Network. proposed approach, an intermediate node dynamically calculates a PEAK value after every time interval that uses three parameters for calculation: RREP sequence number, routing table sequence number and number of replies received during the time interval. when an intermediate node receives RREP having sequence number higher than the calculated PEAK value, it is marked as DO_NOT_CONSIDER [4] [9].

Proposed Methods To Detect Different Types Of Attack

Numerous methods have been proposed to detect the status of knob which are as follows:

Intrusion Detection Systems (IDS) – Anomaly based IDS is mainly used in MANETs to detect any kind of intrusion in the network. Profiles are maintained in databases of IDS to match the anomaly. These profiles can be static or dynamic in nature. The problem with such system is that it is difficult to make a perfect profile. Moreover false alarm rate is higher [5][12].

Random Walker Detectors (RWD) – This detector moves randomly from one knob to other knob to detect the knob's activities. It monitors each knob for a malicious behavior and migrates to the selected knob. This RWD has a specification based detection engine for comparing the behavior of knob [6].

2.3 Watchdog – This method proposed the concept of a watchdog knob which has high power and high transmission range than other ordinary knob. This knob watches and monitors the surrounding knob. It keeps the knob's data in its buffer and compares it after a new knob receives it. Watchdog knob is also called path rather [7].

A securing routing protocol against black hole attack in manet problem

According to the original AODV protocol, any intermediate node may respond to the RREQ message if it has a fresh rough route, which is checked by the destination sequence number contained in the RREQ packet. This Mechanism is used to decreases the routing delay, but makes the system a target of a malicious node. The malicious node easily disrupts the correct functioning of the routing protocol and makes at least part of the network crash.

Previously the works done on security issues i.e. attacks (Black Hole attack) involved in MANET were based on reactive routing protocol like AODV. Black Hole attack is studied under the AODV routing protocol and its effects are elaborate by stating how this attack disrupt the performance of MANET.

Mitigation Scheme

Different scheme is used in MANET to overcome the effect of black hole attack. Here, I have used behavioral based scheme in which the destination sequence no is traced. Since the malicious node always try to send the big destination sequence no. , it is easy to trace out the black hole node and after detecting the node the legitimate node just discards the RREP packet sent by the malicious node. Hence, the effect of the black hole attack can be minimized.

Destination sequence no. sent from the malicious node is compared with the expected destination sequence no. If the destination sequence no is greater than the expected sequence no then it is found that the RREP is malicious

Evaluation Criteria

To evaluate the black hole I have considered the mobility patterns that are very realistic and close to the real world scenario. I have used different parameters such as Throughput, Packet Drop Ratio and End to end delay to analyze the black hole attack effect on the network.

Tele:

E-mail addresses: rashmi.mishra@abes.ac.in

$$\text{Avg Throughput} = \frac{\text{Sum of bytes sent through the data packets}}{\text{time}}$$

$$\text{End to end delay} = \frac{\sum(\text{Arrival time of packet} - \text{Sending time of the packet})}{\sum \text{No. of connection}}$$

$$\text{Packet Drop Ratio} = \frac{\sum(\text{Sent Packet} - \text{Received Packet})}{\text{Sent Packet}}$$

Proposed Algorithm

Parameters: DSN- Destination Sequence Number, NID: Node ID, MN-ID- Malicious Node ID, ESN-Expected Sequence Number, NRC- Node Route Counter.

- Start the route discovery phase with the source node S.
- Store the Route Replies DSN and NID in RR-Table.
- If DSN is much greater than ESN then discard entry from RR-Table as Select Dest_Seq_No rom table
- If(Dest_Seq_No>= ESN_Seq_No)

{
Mal_Node=Node_Id;
Discard entry from table;
}
If Node=Good // if route is fine and Node is fine
Then NRC=NRC+1;

- If Node=Mal

Then NRC=NRC-5; //if packet is unable reach Destination (black node)

- Call Receive Reply method of default AODV Protocol.

References

Radhika Saini and Manju Khari, An Algorithm to Detect Attacks in Mobile Ad Hoc Network, J.M. Zain et al. (Eds.): ICSECS 2011, Part III, CCIS 181, pp. 336–341, 2011. © Springer-Verlag Berlin Heidelberg 2011

Ms.Nidhi Sharma et.al., "The Black-hole node attack in MANET", 978-0-7695-4640-7/12 2012 IEEE.

Rutvij H. Jhaveri et.al., "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks", 978-0-7695-4640-7/12 2012 IEEE.

Rutvij H. Jhaveri et.al., "Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs", INFOCOMP, vol. 11, no. 1, p. 01-12, March of 2012.

Rutvij H. Jhaveri et.al., "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs", 978-0-7695-4941-5/12 2013 IEEE.

Attacks against routing message and its defensive method

Table 1. Malicious behavior affecting the security principle & its Defensive methods

S.No.	Malicious Behavior	Affected Security Principle	Suggested Defensive Methods
1	Message Tampering, Information Disclosure Attack	Integrity	Cryptography- MD5 [16], Polynomial based personal keys[26][1]
2	Stealing Information	Confidentiality	Cryptography [16][1]
3	Bandwidth consumption, Battery Drained Buffer Overflow, Node Not Available	Availability	TTP (RWD, Watchdog) [12][19] and IDS [20][21][1]
4	Entering Malicious node in the Network	Authentication	PKICertification System [17][1]
5	Node Denies of sending message	Non-Repudiation	Digital Signature [16][1]

Table 2. Attacks on Routing Message And its Suggested Defensive Methods

S.No.	Attack	Suggested Defensive Methods
1.	All Network Layer Attack	Model using acknowledgment approach[14], Cross-validation of nodes using certificates[8]
2.	Wormhole Attack	Connectivity Graph[16], Enhanced OLSR[17], EDWA[18], Distance method based on RSS[19],Public key cryptography
3.	Blackhole Attack	Authentication of node using PKI[21], Trust value of neighboring nodes[22], ABM using IDS[23], Enhancement of AODV[26]
4.	Byzantine Attack	Public key using cryptographic mechanism[25]
5.	Routing Attack	CRADS[27] and SRDV[15]
6.	Flooding attack	uses a statistical analysis to detect malicious RREQ floods, CUSUM algorithm, each node is to monitor its neighbors' RREQ. If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist.
7.	Message with holding attack	intrusion detection system to detect TC link, TC message and a HELLO message(if TC message < Hello message ,then node is suspicious)
8.	Link Spoofing attack	detection method by using cryptography with a GPS and a time stamp
9.	Replay Attack	time stamp with the use of an asymmetric key
10.	Colluding Misrelay attack	conventional acknowledgment-based approach might detect this type of attack in a MANET

Ms.Nidhi Sharma et.al., "The Black-hole node attack in MANET", 978-0-7695-4640-7/12 2012 IEEE.

Rutvij H. Jhaveri et.al., "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks", 978-0-7695-4640-7/12 2012 IEEE.

Rutvij H. Jhaveri et.al., "Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs", INFOCOMP, vol. 11, no. 1, p. 01-12, March of 2012.

Rutvij H. Jhaveri et.al., "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs", 978-0-7695-4941-5/12 2013 IEEE.

C.Siva Ram Murthy and B S Manoj, ―Mobile Ad Hoc Networks-Architecture and rotocolsǁ , Pearson Education, ISBN 81-317-0688-5 ,2004.

Jangra1,A. Goel,N. Priyanka and Bhati,K. - Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture, International Journal of Electronics Engineering, pp. 189- 196, 2010

Sahu, S., Shandilya, S.K.: A Comprehensive Survey On Intrusion Detection In Manet.International Journal of Information Technology and Knowledge Management 2(2), 305–310 (2010)

Panos, C., Xenakis, C., Stavrakakis, I.: IEEE Fellow - A Novel Intrusion Detection System for MANETs (2009)

Mamatha, G., Sharma, S.: A Highly Secured Approach against Attacks in MANETS. International Journal of Computer Theory and Engineering 2(5), 1793–8201 (2010)

S. Y. Ni, Y. C. Tseng, Y. S. Chen, and J. P. Sheu, "The broadcast storm problem in a mobile ad hoc network," in Proc. of the 5th annual ACM/IEEE international conference on Mobile computing and networking, pp. 151-162, Aug. 15-19, 1999.

Patcha,A and Mishra,A - Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks, IEEE. 2003

Panos,C Xenakis,C and Stavrakakis,I - A Novel Intrusion Detection System for MANETs International Conference on Security and Cryptography (SECRYPT) 2009

Sahu, S and Shandilya, S K - A Comprehensive Survey On Intrusion Detection In Manet, International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 305-310July-December 2010

S. Rajavaram, H. Shah, V. Shanbhag, J. Undercoffer, and A. Joshi, "Neighborhood Watch: An Intrusion Detection and Response Protocol for Mobile Ad Hoc Networks," Student Research Conference, University of Maryland at Baltimore County (UMBC), May 3, 2002.

A. Burg, "Ad hoc networks specific attacks," Technische Universität München, Institut für Informatik, Seminar Paper, Seminar Ad Hoc Networking: concept, applications, and security, Nov., 2003.

PRADIP M. JAWANDHIYA, MANGESH M. GHONGE "A Survey of Mobile Ad Hoc Network Attacks". International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071

Y.C.Hu, A.Perrig, and D.B.Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Networks," Proceedings of 22nd Annual Joint Conf. IEEE Computer and Communications Societies (Infocom'03), San Francisco, CA, vol.3, pp. 1976-1986, April 2003.

Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma," A Survey of Routing Attacks and SecurityMeasures in Mobile Ad-Hoc Networks", JOURNAL OF COMPUTING, VOLUME 3, ISSUE 1, JANUARY 2011, ISSN,2151-9617, HTTPS://SITES.GOOGLE.COM/SITE/JOURNALOFCOMPUTING/WWW.JOURNAL OF COMPUTING.ORG

S. Rajavaram, H. Shah, V. Shanbhag, J. Undercoffer, and A. Joshi, "Neighborhood Watch: An Intrusion Detection and Response Protocol for Mobile Ad Hoc Networks," Student Research Conference, University of Maryland at Baltimore County (UMBC), May 3, 2002.

A. Burg, "Ad hoc networks specific attacks," Technische Universität München, Institut für Informatik, Seminar Paper, Seminar Ad Hoc Networking: concept, applications, and security, Nov., 2003.

Jinghua, L., Peng, G., Yingqiang, Q., Gui, F.: A Secure Routing Mechanism in AODV for Ad Hoc Networks. IEEE, Los Alamitos (2007)