IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Detection Mechanism for Black hole attacks in MANET

Anjali P.Rathod[1], Nekita A. Chavhan[2]

PG Student, Department of Computer Science& Engineering, G.H. Raisoni College of Engineering, Nagpur, India[1]

Head, Department of Information Technology, G.H. Raisoni College of Engineering, Nagpur, India[2]

Abstract: Security is a key feature in mobile ad hoc networks (MANET) but they are prone to various types of attacks such as network layer attacks. Black hole attack comes under the category of network layer attacks. In Black hole attack, malicious node falsely claims that having shortest path to destination and eventually captures all data packets from source which are intended to forward further to destination. This results into the performance degradation of network and also causes battery problem. In this paper, some of the detection techniques are discussed which are put forward by various researchers. By studying those techniques, new detection mechanism is proposed in this paper.

Keywords: AODV, Black hole attack, Malicious node, Mobile Ad hoc network, Routing protocols etc.

I. INTRODUCTION

Mobile ad hoc network (MANET) composed of mobile nodes that autonomously configure the network. These mobile nodes communicate with each other in radio network without any infrastructure. MANET finds its application in military purpose, disaster area, personal area network, etc. Despite its advantages MANET faces some limitations such as security problem, limited transmission bandwidth, abusive broadcasting messages, unreliable data delivery, etc. MANETs have some special characteristic such as dynamic topology, lack of central monitoring, open medium and management, cooperative algorithms, no clear defence mechanism etc. [6,8].

The nodes are exposed to various types of attacks in dynamic and open environment. One of the security attacks in MANET is the black hole attack. In this attack, without checking routing table, the malicious node sends the dummy reply to the destination node. Then, malicious node absorbs all data packets that are intended to forward to the destination. Due to loss of data packets, the hole is created in the network. Hence, the network faces data loss and its performance reduces [6].

The rest of the paper is categorized as follows. Section II gives brief introduction of Black hole attack. Section III gives related work regarding the detection mechanism. In Section IV gives the brief overview on proposed detection technique. Section V finally concludes the paper.

II. OVERVIEW OF BLACK HOLE ATTACK

Black hole attack comes under the category of the network layer attacks in MANET. Vulnerability in route discovery procedures can be used by malicious nodes in on-demand routing protocols, such as DSR and AODV [15]. In AODV, if source node does not have any route to destination, then the node starts the route discovery process. So, node transmits Route Request message (RREQ) to its neighbours. The adjacent nodes check whether it is the destination node or it has any route to the destination node. The adjacent node sends back Route Reply message (RREP) to the source node, if a route is found. Otherwise, adjacent node forwards the RREQ message to its neighbours by using flooding approach [8].

In Black hole attack, on receiving a RREQ, malicious node advertises itself having the fresh route by sending a Route Reply (RREP) with new destination sequence number larger than current destination sequence number, during the route discovery process [6,7,8]. The source node receives the RREP from the malicious node ahead of RREPs from other adjacent nodes. When the data packets are sent to destination by source node using this route, the malicious node can drop all packets instead of forwarding.

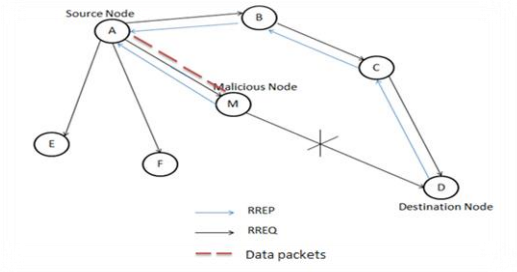

Figure 1 – Black hole Attack

For example, as shown in the Figure 1., the node ‘A’ represents source node, ‘D’ and ‘M’ represent destination node and the malicious node respectively. When ‘A’ wants to send the data packets to destination ‘D’, by broadcasting RREQ message, it starts the route discovery process to the neighbouring nodes. So, the node ‘E’ and ‘F’ receive this message.

Since M is a malicious node, it immediately sends a RREP message to ‘A’ consisting highest sequence number. ‘A’

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

assumes that it is new route, ignores all other RREPs from other nodes and sends any packets to the destination over this new route. As 'M' is a malicious node, it drops all data packets which are intended to send to the destination.

III. RELATED WORK

A. Exponential Trust based mechanism:

Dr.Deepali Virmani, Manas Hemrajani, Shringarica Chandel [1] proposed detection mechanism on the basis of Exponential Trust Based Mechanism. In their proposed method one factor is defined to calculate the number of packets dropped at each node and named it as Streak counter and also trust factor is maintained at each node. The trust factor decreases at each consecutive packet drop and with the help of this malicious node is detected.

B. Using Advanced DRI Table:

Ankurmishra, RanjeetJaiswal, Sanjay Sharma[2] presented a mechanism to detect various types of black hole attacks. In their proposed novel approach, concept of DRI (Data Routing information Table) table with additional bit is introduced. A proposed methodology consists of four steps:

1. Collection of network data and malicious node detection.
2. Finding the trust-worthy node to destination and eliminating the black hole nodes.
3. Set up secure route to destination.
4. Arising Alarm and creating list of malicious node.

C. Using crosschecking with True-link concept:

GayatriWahane, Ashok M. Kanthe, Dina Simunic[3] modifies AODV for detection of co-operative black hole attack. The concepts of DRI table and crosschecking True-link are combined in presented methodology. True-link crosschecking integrated MAC layer and network layer. In proposed architecture, the information stored in DRI table according to entry in DRI table the behavior is monitored with the help of true-link crosschecking concepts. This helps to detect real black hole node.

D. Using MD5 algorithm:

S.Vidhya and T. Sasilatha [4] proposed Black hole detection scheme using MD5 algorithm. This paper overcomes the security problems in WSN and detects Black hole attack during routing of data packets from source to destination. They provided the solution through message digest and public key encryption. In this way the detection of Black hole attack and packet transmission rate are improved. But this may lead to overhead in network and so bandwidth is inefficiently utilized.

E. Using table routing and sequence number:

Nidhi Sharma and Alok Sharma [5] proposed two possible solutions to detect the Black hole node. First to find out more than one route to destination and the second one is to exploit packet sequence number include in any packet header. The future work suggests analyzing black hole attack in other MANETs routing protocols like DSR, TORA and GRP. Other types of attacks like Jellyfish, Sybil and wormhole attacks are needed to study in comparison with Black hole attack.

IV. PROPOSED METHODOLOGY

From the review of detection techniques, it is observed that mostof the detection techniques use cryptographic operations for authentication. The proposed methodology used to detect black hole attack with the help of routing table. By studying the entries in routing table, black hole node is detected. The flow chart for detection is given below:

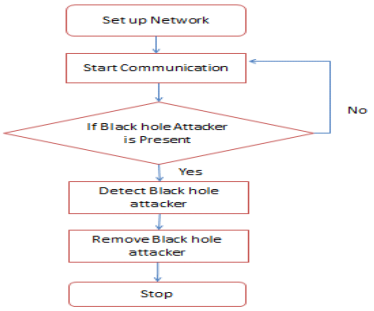

Figure 2- Flow chart for detection mechanism

In AODV protocol, routing table entries consists of the following fields:

- Destination IP address
- Destination sequence number
- Next-hop IP address
- Hop count
- Session expiry time

By checking the table entries, the detection of black hole node is easily done. If in network black hole node is present, it captures all data packets from source which are intended to forward to destination. So in routing table entry, the field 'Next-hop IP address' contains the address of the node which captures the data packets. By observing the table entries, the detection of black hole is easily completed.

SIMULATION

Simulation is done on NS 2.35. Sensor network with 52 nodes is created. Normal communication between nodes, sink nodes and base station takes place. Figure 3 shows network set up and communication.

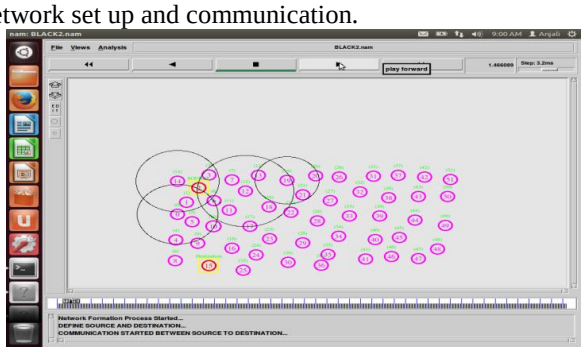

Figure 3 – Network set up and communication

DOI 10.17148/IJARCCE.2016.5427

Figure 4 shows detection of black hole node in the network.

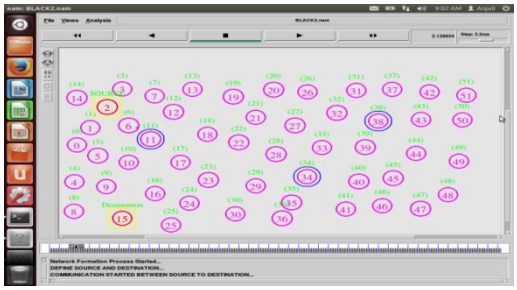

Figure 4 – Detection of Black hole nodes

V. CONCLUSION

The various techniques are studied for detection of black hole attack. By studying the various techniques, new methodology is proposed for detection of attack. In proposed methodology, routing table is used for detection. This methodology reduces the cryptographic operations (e.g., encryption and decryption) for authentication as compare to other methodologies.

REFERENCES

[1]. Dr. DeepaliVirmani ,ManasHemrajani , ShringaricaChandel, "Exponential Trust Based Mechanism to Detect Black Hole attack in Wireless Sensor Network".
[2]. Ankurmishra, RanjeetJaiswal, Sanjay Sharma, "A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network", 2013 3rd IEEE International Advance Computing Conference (IACC).
[3]. GayatriWahane, Ashok M. Kanthe, Dina Simunic, "Detection of Cooperative Black Hole Attack using Crosschecking with TrueLink in MANET", 2014 IEEE International Conference on Computational Intelligence and Computing Research.
[4]. S. Vidhya and T. Sasilatha, "Performance analysis of Blackhole attack detection scheme using MD5 algorithm in WSN", ICSSS-2014.
[5]. Ms.Nidhi Sharma and Mr.Alok Sharma, "The Black-hole node attack in MANET", 2012 Second International Conference on Advanced Computing & Communication Technologies.
[6]. Ei Ei Khin and Thandar Phyu, "Impact Of Black Hole Attack On AODV Routing Protocol", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014.
[7]. Anand A. Aware KiranBhandari, "Prevention of Black hole Attack on AODV in MANET using hash function", In FEB 2014 IJACSA.
[8]. Adhoc Wireless Networks Architectures and Protocols, C.Siva Ram Murthy, B.S.Manoj, page: 320-322.
[9]. Adnan Nadeem member, IEEE, and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE communications surveys & tutorials, vol.15, no.4, fourth quarter 2013.
[10]. NiteshGondwal and Chander Diwaker, " Detecting Black hole Attack in WSN by Check Agent using Multiple Base Stations", American International Journal of Research in Science, Technology, Engineering & Mathematics.
[11]. Dr. G. Padmavathi and Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanism and Challenges in Wireless Sensor Network", International Journal of Computer Science and Information Security, Vol. 4 No.1&2, 2009.
[12]. Om Shree and Francis J. Ogwu, "A Proposal for Mitigating Multiple Black hole Attack in Wireless Mesh Networks".
[13]. Mohammad Wazid, Student Member, IEEE, AvitaKatal, Student Member, IEEE, Roshan Singh Sachan, Student Member, IEEE, "Detection and prevention mechanism for Blackhole attack in WSN", International Conference on Communication Single Processing, April 2013.

BIOGRAPHIES

Anjali P. Rathod received the bachelor's degree in Computer science and engineering from the SRTM University, Nanded, Maharashtra, India in 2013. Presently sheis pursuing her master's in mobile technology in the department of Computer Science from G. H. Raisoni College of Engineering, Nagpur Maharashtra, India. Her research interests include wireless sensor networks, cryptography and network security, wireless security etc.

Nekita Chavhan received the Master of Engineering (ME) in Wireless Communication and Computing from G.H. Raisoni College of Engineering, Nagpur, and Maharashtra, India. She is working as Head in Department of Information Technology in G.H. Raisoni College of Engineering, Nagpur. Her research area includes Ad-hoc Wireless networks, Wireless Sensor Networks, Mobile Technology and multi criteria decision making & optimization.

DOI 10.17148/IJARCCE.2016.5427