International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 9 – No.4, July 2015 – www.ijais.org

Performance Evaluation of the Techniques to Mitigate Blackhole Attack in VANETs

Lalit Kumar
M.Tech Scholar, ECE Department,
DCRUST, Murthal, Sonipat, Haryana, India

Pawan Kumar Dahiya
Assistant Professor, ECE Department,
DCRUST, Murthal, Sonipat, Haryana, India

ABSTRACT

Vehicular Adhoc Network (VANET), an integrated part of Intelligent Transportation System (ITS), is a real-life illustration of a self-organized Adhoc network for communication between vehicles and roadside infrastructure. VANETS has several security issues and Blackhole attack is one of those. The paper discusses Blackhole attack in VANETs and various solutions for it.

Keywords

Blackhole, VANET, AODV, ERDA, RREQ, RREP, DOS, DPRAODV and ABM

1. INTRODUCTION

In the present time, the sheer volume of road traffic has influenced the safety and proficiency of traffic environment. Approximately 1.2 million people lose their lives due to road accidents [5]. One effective method is making the traffic information accessible to the vehicles, by using that they can analyze the traffic conditions [5]. Vehicular Adhoc Network (VANET) is a sort of network which is supposed to provide a large range of mobile distributed applications operating in vehicles. The most prominent services in VANETs are that it can give drivers safety and information about road and traffic situations [6]. VANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, no clear defense mechanism. These factors have changed the battle field situation for the VANETs against the security threats. In order to provide secure network, one must understand different types of attacks and their effects on the VANETs. Wormhole attack, Blackhole attack, Sybil attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that VANETs can suffer from [17]. Black hole attack is one such attack to which VANET is always vulnerable.

The contribution of the paper is as follows:

- The paper details the Blackhole attack in VANETs
- The paper presents a state-of-the-art survey of the techniques to mitigate the Blackhole attack in VANETs.
- Based on the literature survey, an evaluation of the techniques to mitigate the Blackhole attack is presented.

Rest of the paper is organized as under:

In section II, VANETs and its properties are discussed. In section III, Blackhole attack is studied. In section IV, Blackhole attack in VANETs is described. In section V, Techniques for Detection and Mitigation of Blackhole Attack are studied. In section VI, Performance Evaluation of Techniques for Detection and Mitigation of Blackhole Attack are discussed.

2. VANET

In VANET, a subpart of MANET, each node represents a vehicle or Road Side Unit (RSU) which can move freely within the network range accessing the connection [10]. These vehicles are outfitted with wireless On-Board Units (OBUs), which carry out the communication process [3].

In precise, a VANET is a self-organized network that is formed by connecting vehicles, with the aim to enhance driving safety and traffic management providing internet access to drivers and programmers [1]. For VANET operations, IEEE has established the standard 802.11p and 802.16 (Wi-Max). It uses Dedicated Short Range Communication (DSRC) which operates on 5.9GHz band with 802.11 access methods. Its diminished latency in short range communication is a prime aspect [5]. In USA, Intelligent Transportation Systems (ITS) uses DSRC with 75 MHz of spectrum allocated; while in Europe 30 MHz of spectrum has been allocated in the 5.9 GHz band [20].

The security of VANET is the most critical issue because propagation of information takes place in open access (wireless) environments. So it is highly demanded that all transmitted data should not be inserted or modified by users who have harmful objectives [20]. These issues in VANETs are hard to solve because of very large size of network, high speed of the vehicles, their relative geographic positions, and the irregular connectivity between nodes. Four objectives should be achieved by VANET security, Ensuring the information received is appropriate (information authenticity), the source is same who he claims to be (source authentication and message integrity), the node who sends the message cannot be recognized and tracked (privacy) and robustness of the system is maintained [17].

3. BLACKHOLE ATTACK

In this attack, either a node refuses to get involved in the network or an existing node drops out the packets to form a Blackhole [1]. A malicious node waits for neighboring nodes to send route request (RREQ) messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false route reply (RREP) message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one[21]. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes [13]. Therefore all packets are sent to a point when they are not forwarding anywhere. To succeed a Blackhole attack, malicious node should be positioned at the center of the wireless network [21].

In above figure 1, S and D are assumed to be source and destination nodes respectively. Let M be the malicious node. S being the source node would initiate the route discovery process and broadcasts a RREQ that is received by the nodes B, M and E being the neighbors of node S. Upon receiving the RREQ from the node S, node B and E makes a search to their cache for a fresh route to the destination. Non-availability or older entry in their route table causes nodes to rebroadcast the RREQ and this process is continued till the RREQ arrives at node D [21]. But node M claims to have the fresh route to destination and sends RREP packet to the source node S. The reply from the malicious node reaches the source node much earlier than other legitimate nodes, as the malicious nodes does not have to check its routing table [1]. Nodes those have route to the destination would update their route table with the accumulated hop count and the destination sequence number of the destination node and generate a RREP control message. The destination sequence number that determines the freshness of a route is a 32-bit integer associated with every route [13]. The malicious node claims to have a fresher route by including a very high destination sequence number in RREP packet. The source node chooses the path provided by the malicious node and starts sending the data packets, which are dropped by the malicious node [8].

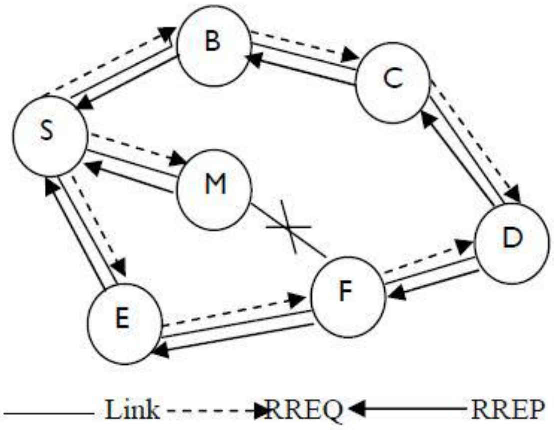

Fig.1: Blackhole attack [8]

4. BLACKHOLE ATTACK IN VANETs

The Blackhole attack in VANETs is an active insider attack. The Blackhole has two main properties:

1. First the node announces itself when having a suitable route to a destination node and second one the node consumes the intercepted packets [7].
2. The second type of black hole attack is External Blackhole attack in which attack physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network [17].

External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in VANETs. External Blackhole attack in VANETs can be summarized in following points:

- Malicious node detects the active route and notes the destination address.
- Malicious node sends a RREP including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
- Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
- The RREP received by the nearest available node to the malicious node will be relayed via the established inverse route to the data of source node.
- The new information received in the route reply will allow the source node to update its routing table.
- New route selected by source node for selecting data.
- The malicious node will drop now all the data to which it belong in the route [11].

In VANETs, Blackhole attack is most dangerous in AODV routing protocol.

5. TECHNIQUES FOR DETECTION AND MITIGATION OF BLACKHOLE ATTACK

There are various solutions proposed for Blackhole attack. Some of them are discussed below as:

- **DPRAODV (Detection, Prevention and Reactive AODV) scheme:** DPRAODV prevents from Blackhole attack by informing other nodes in the network [18]. In normal, ad-hoc on demand distance vector (AODV), the node that receives the RREP packet first checks the value of sequence number in its routing table. If its sequence number is higher than the one in routing table, this RREP packet is accepted. In this solution, it has an addition check whether the RREP sequence number is higher than the threshold value. If it is higher than the threshold value, then the node is considered to be malicious node and it adds to the black list. As the node detected as anomaly, it sends alarm packet to its neighbors [19]. The routing table for that malicious node is not updated, nor is the packet forwarded to another node. The threshold value is dynamically updated using the data collected in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The main advantage of this protocol is that the source node announces the Blackhole to its neighbors in order to be ignored and eliminated [2].
- **ABM (Anti-Blackhole Mechanism) scheme:** Malicious nodes perform selective Blackhole attack by deploying IDSs in VANETs. All IDS nodes perform an ABM, which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. With the prerequisite that intermediate nodes are forbidden to reply to RREQs, if an intermediate node, which is not the destination and never broadcasts a RREQ for a specific route, forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS's suspicious node table (SN) [13]. When the suspicious

value of a node exceeds a threshold, a Block message is broadcasted by the detected IDS to all nodes on the network in order to cooperatively isolate the suspicious node [2].

- **ERDA (Enhance Route Discovery for AODV) scheme:** ERDA scheme improves AODV protocol with minimum modification to the existing route Discovery mechanism recvReply () function. The proposed method is able to mitigate the foresaid problem by introducing new conditions in the routing table update process and also by adding simple malicious node detection and isolation process to the AODV route discovery mechanism. The proposed method does not introduce any additional control message and moreover, it does not change the existing protocol scheme. There are three new elements introduced in modified recvReply() function namely: table rrep_table to store incoming RREP packet parameter mali_list to keep the detected malicious nodes identity and parameter rt_upd to control the process of updating the routing table. When RREQ packet is sent out by the source node S to find a fresh route to the destination node D. RREP packet received by node S will be captured into rrep_tab table. Since the malicious node M is the first node to response, the routing table of node S is updated with RREP information from node M Since the value of parameter rt_upd is true, node S accepts the next RREP packet from other node to update the routing table although it arrives later and with a lower destination sequence number than the one in the routing table [16]. The current route entry in routing table will be overwritten by the later RREP coming from other node. ERDA method offers a simple solution by eliminating the false route entry and replaced the entry with later RREP [2].

- **Cryptographic based technique:** Cryptographic techniques cannot prevent a malicious node from dropping packets supposed to be relayed, there are basically three defense lines devised here to protect VANETs against the packet dropping attack. The first defense line (for prevention purposes) aims to forbid the malicious nodes from participating in packet forwarding function. Whenever the malicious node exceeds this barrier, a second defense line (for incentive purposes) is launched, which seeks to stimulate the cooperation among the router nodes via an economic model [15]. Finally, once the two previous defense lines have been broken, a third one (for detection/reaction purposes) is launched aiming to reveal the identity of the malicious node and excludes it from the network [2].

- **Isolator Algorithm based technique:** This method is used to detect the malicious node and then mitigating the Blackhole attack from VANETs. In this method, we use the following rules to detect the malicious node:

  Rule 1: If a node delivers many data packets to destinations, it is assumed as an honest node.

  Rule 2: If a node receives many packets but do not sent same data packets, it is possible that the current node is a misbehavior node.

  Rule 3: When the rule2 is correct about a node, if the current node has sent number RREP packets; therefore surely the current node is misbehavior.

  Rule 4: When the rule2 is correct about a node, if the current node has not sent any RREP packets; therefore the current node is a failed node [3].

After detection of a malicious node, the properties of malicious node are changed using the isolator program to make its behavior very near to a honest node. Thus, throughput of the VANET is increased and packet drop is decreased. Isolator program is basically a set of programs which have the ability to control the behavior of a node.

6. PERFORMANCE EVALUATION OF TECHNIQUES FOR DETECTION AND MITIGATION OF BLACKHOLE ATTACK

The various techniques discussed in the preceding section have their own pros and cons. A complete evaluation of these techniques is detailed as under:

- **DPRAODV scheme:** In this scheme the packet delivery ratio is improved from 80 to 85% hanAODVunder Blackhole and 60% when traffic load increases. However, an overhead of updating threshold value at every time interval along with the generation of alarm packet will considerably increase the routing overhead. This method is not support cooperative Blackhole nodes [2].

- **ABM scheme:** In this scheme, IDS nodes are specially located within each other’s transmission range, which is not always feasible in normal case. Special security mechanism needed to safe communication between special IDS nodes. The role of special IDS nodes became very confusing [2].

- **ERDA scheme:** This scheme cannot detect cooperative Blackhole attack [2].

- **Cryptographic based scheme:** technique, most of the proposed solutions are built on a number of assumptions which are either hard to realize in a hostile and energy constrained environment like MANETs or not always available due to the network deployment constraints. Moreover, these solutions are generally unable to launch a global response system whenever a malicious node is identified. In contrast, they either punish the malicious node locally without informing the rest of the network or divulge its identity to the network through costly cryptographic computations. Moreover, even though the malicious node is punished in a part of the network it can move to another part and continues causing damage to the network until it is detected again [2].

- **Isolator algorithm based scheme:** The advantage of the isolator algorithm method is that it raises the throughput of the network quite efficiently. The packet drop of the VANETs is also decreased up to a large extent. But this method cannot detect cooperative Blackhole attack.

7. CONCLUSION AND FUTURE DIRECTIONS

The Blackhole attack is one of the serious security problems in VANETs. Although many solutions have been presented in literature but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes. In the presence of cooperative Blackhole attack, the performance of these methods falls down rapidly. So, there is a dire need for improving the performance in the case of cooperative Blackhole attack. The researcher must take a cue from this and work on this problem.

8. REFERENCES

[1] Lalit Kumar, Pawan Kumar Dahiya, “Security issues in VANETs: A Review,” TEQIP Sponsored National Conference on Advances in Electronics and Communication Technologies, 29-30 January, 2015.

[2] Bhoomika Patel, Khushboo Trivedi, “A Review - Prevention and Detection of Black Hole Attack in AODV based on MANET,” International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2816-2818.

[3] Rashmi Raiya, Shubham Gandhi, “Survey of Various Security Techniques in VANET,” International Journal of Advanced Research in Computer Science and Software Engineering, volume 4, Issue 6, June 2014.

[4] Priyambada Sahu, Sukant Kishoro Bisoy, Soumya Sahoo,” Detecting and Isolating Malicious Node in AODV Routing Algorithm,” International Journal of Computer Applications (0975 – 8887) Volume 66– No.16, March 2013.

[5] Ram Shringar Raw, Manish Kumar, Nanhay Singh, “Security Challenges, Issues and Their Solutions for VANET,” International Journal of Network Security & Its Applications (IJNSA), vol.5, No.5, September 2013.

[6] Mostofa Kamal Nasir, A.S.M. Delowar Hossain, Md. Sazzad Hossain, Md. Mosaddik Hasan, Md. Belayet Ali, “Security Challenges And Implementation Mechanism For Vehicular Ad Hoc Network,” International Journal Of Scientific & Technology Research volume 2, Issue 4, April 2013.

[7] Harjeet Kaur, Manju Bala and Varsha Sahni, ”Study of Blackhole Attack Using Different Routing Protocols in MANET,” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013.

[8] Harmandeep Singh, Manpreeet Singh, ”Effect of Black Hole Attack on AODV, OLSR and ZRP Protocol in MANETs,” Volume 2, No.3, May - June 2013 International Journal of Advanced Trends in Computer Science and Engineering.

[9] Himani Yadav and Rakesh Kumar, “ Identification and Removal of Black Hole Attack for Secure Communication in MANETs,” **I**nternational **J**ournal of **C**omputer **S**cience and **T**elecommunications [Volume 3, Issue 9, September 2012.

[10] Ajay Rawat, Santosh Sharma and Rama Sushil, “VANET: Security Attacks and Its Possible Solutions,” Journal of Information and Operations Management, volume 3, Issue 1, 2012, pp-301-304.

[11] Vimal Bibhu, Kumar Roshan, Dr. Kumar Balwant Singh and Dr. Dhirendra Kumar Singh, ”Performance Analysis of Black Hole Attack in VANETs,” I. J. Computer Network and Information Security, 2012, 11, 47-54.

[12] Gagandeep, Aashima and Pawan Kumar, “ Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review,” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[13] Priyanka Goyal, Vinti Parmar, Rahul Rishi, ”MANET:Vulnerabilities, Challenges, Attacks, Application,”International Journal of Computational Engineering &Management (IJCEM), pp. 32-37, 2011.

[14] Ming-Yang Su, ”Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems,” Elsevier, Computer Communications 34 (2011) 107–117.

[15] Soufiene Djahel, Farid Na¨ıt-abdesselam, and Zonghua Zhang, “Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges,” Ieee Communications Surveys & Tutorials, Vol. 13, No. 4, Fourth Quarter 2011.

[16] Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail AbManan,“Mitigation of Black Hole Attacks for AODV Routing Protocol”, Society of Digital Information and Wireless Communications (SDIWC) Vol01_No02_30, 2011.

[17] G. Samara, et al., "Security Issues And Challenges Of Vehicular Ad Hoc Networks (VANET)," 4th International Conference on New Trends in Information Science and Service Science (NISS), 2010, pp. 393-398.

[18] E. A. Mary Anita and V. Vasudevan, ”Performance Evaluation of mesh based multicast reactive routing protocol under black hole attack,” IJCSIS, Vol.3, No.1, 2009.

[19] Payal N. Raj, Prashant B. Swadas, ” DPRAODV: A Dyanamic Learning System Against Blackhole Attack In AODV Based Manet,”arXiv:0909.2371,2009.

[20] Yaseer Toor et al., “Vehicle Ad Hoc Networks: Applications and Related Technical issues,” IEEE Communications surveys & Tutorials, 3rd quarter 2008, vol 10, No 3, pp. 74-88.

[21] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, ” Detecting Blackhole Attack on AODV based Mobile Ad hoc networks by Dynamic Learning Method,” International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov 2007.

[22] Bo, M. S., Xiao, H., Adereti, A., Malcolm, A. J.,Christianson, B, ”A Performance Comparison of Wireless Ad hoc Network Routing Protocols under Security Attack,” Third International Symposium on Information Assurance and Security, pp. 50-55, 2007.