Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

SAODV: Security Aware Ad-hoc on Demand Distance Vector Routing Protocol for Vehicular Ad-hoc Network

Avinash P. Jadhao
Phd Scholar,
Department of CSE, JDIET
Yavatmal, Maharashtra, India

Dr. D. N. Chaudhari
Professor
Department of CSE, JDIET
Yavatmal, Maharashtra, India

Abstract— Vehicular ad hoc networks (VANETs) are dynamic wireless networks without any infrastructure. The dynamic topology of VANET allows nodes to join and leave the network at any point of time. Wireless VANET is particularly vulnerable due to its fundamental characteristics such as open medium, dynamic topology, distributed cooperation and constrained capability. So security in VANET is a complex issue. This paper analyzes the blackhole attack which is one of the possible attacks in ad hoc networks. In a blackhole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. By doing this, the malicious node can deprive the traffic from the source node. In order to prevent this kind of attack, it is crucial to detect the abnormality occurs during the attack. In this paper, we propose a secure ad hoc on demand vector routing protocol against blackhole attack (SAODV) which detect and prevent the blackhole attack in Vehicular ad hoc network. The proposed modification in AODV protocol against blackhole attack improves the performance of AODV protocol. The packet delivery ratio, average end-to-end delay, routing overhead and normalized routing overhead improves in SAODV protocol. The simulation results show the effectiveness of our proposed modification.

Keywords: VANET, AODV; Black hole attack; packet delivery ratio; End-to-end delay;, Reactive routing; Throughput; RREQ; RREP; RERR.

I. INTRODUCTION

An ad-hoc network has a certain characteristics, which imposes new demands on the routing protocol. The most important characteristics are the dynamic topology, which is a consequence of node mobility. Nodes can change position quite frequently, which means that we need a routing protocol that quickly adapts to topology changes. The node in an ad-hoc network can consist of laptops and personal digital assistants and are often very limited in resources such as CPU capacity, storage capacity, battery power and bandwidth, so the routing protocol should try to minimize control traffic, such as periodic update messages. Instead the routing protocol should be reactive, thus only calculate routes upon receiving a specific request. To be effective, the routing protocols have to

1) Keep the routing table up-to-date and reasonably small,
2) Choose the best route for given destination (e.g., in terms of number of hops, reliability, throughput and cost) and
3) Converge within an exchange of a small amount of messages [8].

A Vehicular ad-hoc network [8] is an autonomous system of Vehicular hosts connected with each other using multi-hop wireless links. There is no static infrastructure such as base stations, each node in the network acts as a router, forwarding data packets for other nodes, which in such a network move arbitrarily thus network topology changes frequently and unpredictably. Nodes are free to move, independent of each other, topology of such networks keep on changing dynamically which makes routing much difficult, therefore routing is one of the most concerns areas in these networks. Normal routing protocol which works well in fixed networks does not show same performance in Vehicular Ad-hoc Networks. In these networks routing protocols should be more dynamic so that they quickly respond to topological changes . If two hosts are not within radio range, all message communication between them must pass through one or more intermediate hosts that double as routers. The hosts are free to move around randomly, thus changing the network topology dynamically. Thus routing protocols must be adaptive and able to maintain routes in spite of the changing network connectivity. Such networks are very useful in military and other tactical applications such as emergency rescue or exploration missions, where cellular infrastructure is unavailable or unreliable.

Commercial applications are also likely where there is a need for ubiquitous communication services without the presence or use of a fixed infrastructure; Examples include conferencing applications, networking intelligent devices or sensors etc.

II. ANALYSIS OF AODV PROTOCOL

The AODV protocol builds on the DSDV algorithm .it is an on demand routing algorithm[3]. But in contrast to DSR it is a not source based routing scheme rather every hop of a route maintains the next hop information by its own. Operation of the protocol is divided into two functions, route discovery & route maintenance. At first all the nodes send

hello message on its interface and receive hello message from its neighbors. This process repeats periodically to determine neighbor connectivity .when a route is needed is to some destination, the protocols start route discovery .It uses two term route request & route reply. This RREP packet is unicast to the next node on RREP path. The intermediate node on receiving the RREP packet make reversal of path set by the RREQ packet. As soon as RREP packet is received by the source, it starts data transmission on the forward path set by RREP packet. Sometimes while data transmission is going on, if path break occurs due to mobility of node out of coverage area of nodes on the active path, data packets will be lost. When the network traffic requires real time delivery (voice, for instance), dropping data packets at the intermediate nodes can be costly. Likewise, if the session is a best effort, TCP connection, packet drops may lead to slow start, timeout, and throughput degradation. It is crucial for AODV to properly handle the sequence numbers A node has to update its own sequence number in two cases: AODV defines three types of control messages for route maintenance as shown in figure 1.

- *RREQ*- A route request message is transmitted by a node requiring a route to a node. As an optimization AODV uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded.
- *RREP*- A route reply message is unicast back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address.
- *RERR*- Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of

the loss of the link. In order to enable this reporting mechanism, each node keeps a "precursor list", containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination

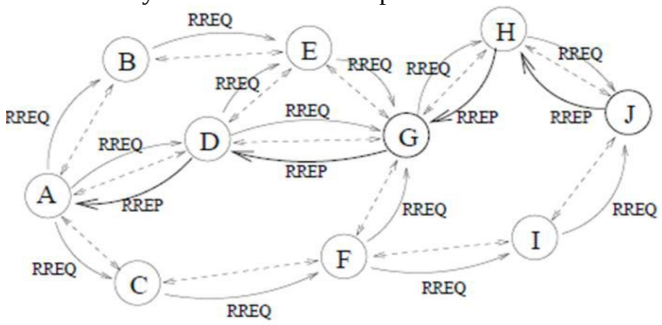

Figure 1: RREQ-RREP in AODV

Routing protocols are exposed to a variety of attacks. Black hole attack [6],[7],[18] is one such attack and a kind of Denial Of Service (DoS)in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept . This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the *Route Discovery process*, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires. As an example, consider the following scenario in figure 4. We illustrate a typical scenario of the protocol packet exchanges, depicting the generation and traversal of RREQ and RREP control messages. The node S is assumed to be the source node desiring to communicate with node D. Thus, as per the explanation earlier, node S would generate the RREQ control message and broadcast it. The broadcasted RREQ control message is expected to be received by the nodes 1, 2 and 3. Assuming that the node 3 has a route to node D in its route table, the node 3 would generate a RREP control message and update its routing table with the accumulated hop count and the destination sequence number of the destination node. Destination Sequence Number [10] is a 32-bit integer associated with every route and is used to decide the freshness of a particular route. The larger the sequence number, the fresher is the route [4]. Node 3 will now send it to node. Since node 1 and node 2 do not have a route to node D, they would again broadcast the RREQ control message. RREQ control message broadcasted by node 3 is also expected to be received by node M (assumed to be a malicious node). Thus, node M being malicious node, would generate a false RREP control message and send it to node 3 with a very high destination sequence number, that subsequently would be sent to the node S. However, since, the destination sequence number is high, the route from node 3 will be considered to be fresher and hence node S would start sending data packets to node 3. Node 3 would send the same to the malicious eventually reach node D (destination node), which would generate RREP control message and route it back. However, since the node S has a RREP control message with higher destination sequence number to that route, node S will ignore two genuine RREP control messages. If any link is disconnected during the transfer of packets then RERR control message is generated. For every RREP control message received, the source node would first check whether it has an entry for the destination in the route table or not. If it finds one, the source node would check whether the destination sequence number in the incoming control message is higher than one it sent last in the RREQ or not. If the destination sequence

number is higher, the source node will update its routing table with the new RREP control message; otherwise the RREP control message will be discarded. In *Route Maintenance phase*, if a node finds a link break or failure, then it sends RERR message to all the nodes that uses the route.

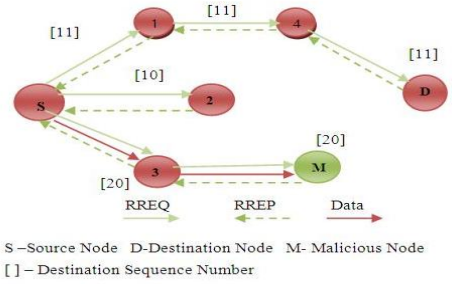

Figure 2: Protocol Packet Exchange

III. PROPOSED SAODV

In proposed solution, we modified the working of the source node in AODV protocol, using recvReply() and sendReply() function. When a packet is received by the "*recv*" function of the AODV protocol, it processes the packets based on its type. If packet type is any of the many AODV route management packets, it sends the packet to the receive AODV function. If the received packet is a data packet, normally AODV protocol sends it to the destination address, but behaving as a Black Hole it drops all data packets as long as the packet does not come to itself. In the code below, the first "*if*" condition provides the node to receive data packets if it is the destination. The "*else*" condition drops all remaining packets.

IV. SIMULATION ENVIRONMENTS

To evaluate the effectiveness of the proposed scheme, we simulated the scheme in NS-2 [13]. The simulation parameters are listed in Table 1. We implement the random waypoint movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity chosen between 0 m/s and the maximum simulation speed. Here, we assume that the blackhole attack take place after the attacking node received RREQ for the destination node that it is going to impersonate. We also assume that the communication started from a source node to a destination node and the node numbers of the source node, destination node and attacking node are 0, 1 and 9, respectively, as shown in Figure 5 (for 10 nodes). We have carried out the simulation by considering the different number of nodes 10, 15, 20, 25, and 30. First, we investigate the packet delivery ratio of packet from source node 0 to destination node 1 in case there are connections from other nodes to the destination node. For the experiment, in Figure 2, nodes which are selected randomly from 2 to 8 (for 10 nodes), 2 to 18 (for 20 nodes) etc. (except the source node, destination node, and attacking node) generate traffic toward the destination node. Here, we perform experiment by changing the number of nodes generating the traffic from one to nine.

Table 1: Values of RREQ and RREP

Simulator	Ns-2(version 2.32)
Simulation Time	500 (s)
Number of Vehicular	10, 15,20,25,30
Topology	750 * 750 (m)
Routing Protocol	AODV, IAODV-BH
Traffic	Constant Bit Rate
Pause Time	10 (m/s)
Max Speed	20 (m/s)
No of Malicious Node	1

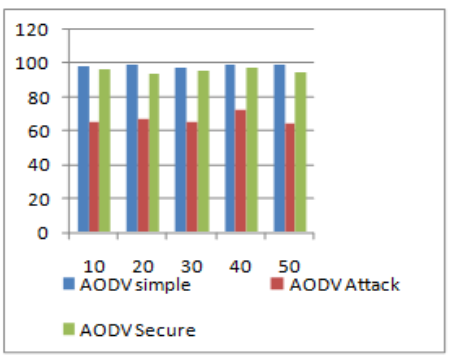

Figure 3 Packet delivery ratio

V. RESULTS

To evaluate the Packet Delivery Ratio, End-to-End Delay Routing Overhead and Normalized Routing Overhead; simulation is done with varying number of nodes. Figure 3 shows the graph for packet delivery ratio for network size (number of nodes) is varying

VI. CONCLUSION

Blackhole attack is one of the most important security problems in VANET. It is an attack that a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In this paper, we have analysed the blackhole attack and introduced the feature in order to define the normal state of the network. We have presented a new modification in AODV protocol i.e. SAODV which shows significant effectiveness in detecting and preventing the blackhole attack.

REFERENCES

[1] Ho Ting Cheng, et.al,"Infotainment and road safety service support in vehicular networking: From a communication perspective ", www.elsevier.com/locate/jnlabr/ymssp, (2011) / page no. (2020–2038) /doi:10.1016/j.ymssp.2010.11.009

[2] Hannes Hartenstein, "A Tutorial Survey on Vehicular Ad Hoc Networks ",IEEE Communications Magazine June 2008/ page no.(164-171)

[3] A. Shastri et.al,"Performance Analysis of on-demand routing protocol for Vehicular Ad-hoc Networks", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011 DOI : 10.5121/ijwmn.2011.3407 page no.(103-111)

[4] Josiane Nzouonta,et.al,"VANET Routing on City Roads Using Real-Time Vehicular Traffic Information", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 7, SEPTEMBER 2009 page no.(3609-3626)

[5] Boangoat Jarupan , et. al "A survey of cross-layer design for VANETs",Ad Hoc Networks 9 (2011) page no (966–983),www.elsevier.com/locate/adhoc

[6] YASSER TOOR, et al."Vehicle Adhoc Networks: Applications And Related Technical Issues",IEEE COMMUNICATIONS 3RD QUARTER 2008, VOLUME 10, NO. 3 page no (74-87).

[7] Jinyuan Sun, et.al,,"Location-Based Secure and Dependable VANETs for Disaster Rescue", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3, MARCH 2011 page no (659-669).

[8] Sherali Zeadally, et. al ,"Vehicular ad hoc networks (VANETS): status, results,and challenges", Springer Science 2010

[9] Halabi Hasbullah,"Denial of Service (DOS) Attack and Its Possible Solutions in VANET", World Academy of Science, Engineering and Technology 41 2010 page no (411-415).

[10] Vimal Bibhu, et. al ,"Performance Analysis of Black Hole Attack in Vanet", I. J. Computer Network and Information Security, 2012, 11, page no (47-54).

[11] Harbir Kaur, et. al,"An Approach To Detect The Wormhole Attack In Vehicular Adhoc Networks", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN No. 2248-9738 Volume-1, Issue-4, 2012 page no (86-89).

[12] Gilles Guette et. al ,"On the Sybil attack detection in VANET", 1-4244-1455-5/07/ 2007 IEEE 13. Hafez Maowad et. al ,"Efficient Routing Protocol for VehicularAd Hoc Networks", page no(209-215)/ 2012 IEEE

[14] Alpana Dahiya et. al ,"Path Discovery In Vehicular Ad hoc Network", 2012 Second International Conference on Advanced Computing & Communication Technologies / 2012 IEEE /DOI 10.1109 /ACCT.2012.83/ page no.(551-555).

[15] Ben Ding et. al"An Improved AODV Routing Protocol for VANETs" 978-1-4577-1010-0/11/ 2011 IEEE.

[16] Min-Hsuan Wei,"A Reliable Routing Scheme Based on Vehicle Moving Similarity for VANETs", 978-1-4577-0255-6/11/page no.(426-430)/2011 IEEE.

[17] Won-Il Lee et. al ,"Performance Evaluation of Reactive Routing Protocols in VANET", 2011 17th Asia-Pacific Conference on Communications (APCC) 2nd – 5th October 2011 IEEE page no (559-564).

[18] Gongjun Yan, et. al,"An Efficient Geographic Location-based Security Mechanism for Vehicular Adhoc Networks",978-1-4244-5113-5/09/page no (804-809)/2009 IEEE.

[19] R. Yu,"Distributed geographical packet forwarding in wireless sensor and actuator networks – a stochastic optimal control approach", IET Wirel. Sens. Syst., 2012, Vol. 2, Iss. 1, page no(63–74) 63 doi: 10.1049/iet-wss.2011.0093.

[20] YUN-WEI LIN,"Routing Protocols in Vehicular Ad Hoc Networks: A Survey and Future Perspectives", JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 26, page no (913-932) (2010).

[21] Sanjay S. Dorle,"Wireless Transmission Impact on the Lifetime of Routing Path in VANET", 978-0-7695-4246-1/10/ page no(101-105) 2010 IEEE DOI 10.1109/ICETET.2010.117.

[22] Samina Ehsan et. al ,"A Survey on Energy-Efficient Routing Techniques with QoS Assurances for Wireless Multimedia Sensor Networks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 14, NO. 2, SECOND QUARTER 2012 page no.(265-278).

[23] Farzad Sabahi,"The Security of Vehicular Adhoc Networks", 978-0 -7695-4482-3/11 2011 IEEE DOI 10.1109/CICSyN.2011.77/ page no.(338-341).

[24] Jorg Buhler,"Traffic-Aware Optimization of Heterogeneous Access Management", IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 58, NO. 6, JUNE 2010 page no.(1737-1747).

[25] Qing Yang et. al,"Connectivity Aware Routing in Vehicular Networks", 1525-3511/08/2008 IEEE page no.(2218-2223).

[26] Brijesh Kadri Mohandas,"Vehicle Traffic Congestion Management in Vehicular ad-hoc networks", 978-1-4244-4487-8/09/2009 IEEE page no.(655-660).

[27] Omid Abedi,"Enhancing AODV Routing Protocol Using Mobility Parameters in VANET", 978-1-4244-1968-5/08/2008 IEEE page no.(229-235).

[28] Noppakun Yawan et. al,"AODV Improvement for Vehicular Networks with Cross Layer Technique and Mobility Prediction" , 978-1-4577-2166-3/11/ 2011 IEEE.

[29] Wenjing Wang et. al,"TOPO: Routing in Large Scale Vehicular Networks", 1-4244-0264-6/07/2007 IEEE page no.(2106-2110).

[30] Xi Yu,"A Reliable Routing Protocol for VANET Communications", 978-1- 4577-9538-2/11/2011 IEEE page no.(1748-1753).

[31] Hang guo et. al"Research of Security for Vehicular Ad Hoc Networks" 201O International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE), 978-1-4244-7956-6/1 0/2010 IEEE page no.(144-147).

[32] D.Sutariya et. al"An Improved AODV Routing Protocol for VANETs in City Scenarios", IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012 page no.(575-581).

[33] S. S. Manvi et. al "Performance Analysis of AODV, DSR, and Swarm Intelligence Routing Protocols In Vehicular Ad hoc Network Environment" 2009 International Conference on Future Computer and Communication, 2009 IEEE page no.(21-25).

[34] S.Mohammad Safi,"A Novel Approach for Avoiding Wormhole Attacks in VANET",2009 IEEE.

[35] Jianping Wang et. al,"A Secure DSR Protocol Based on the Request Sequence-Number", 978-1-4244-3693-4/09/2009 IEEE.

