ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

Security Aware Adhoc on Demand Distance Vector Routing Protocol in Vehicular Adhoc Network

A.P.Jadhao, Dr.D.N.Chaudhari,

Research Scholar, Department of Computer Science & Engineering, J.D.I.E.T, Yavatmal, India

Professor, Head Department of Computer Science & Engineering, J.D.I.E.T, Yavatmal, India

ABSTRACT: Uncovering & Anticipation of malicious attacks in networking field is an important and challenging security issue in Vehicular Adhoc Networks (VANET).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. These networks are weak against many types of attacks. Black hole attack which is one of the possible attacks on AODV routing protocol in vehicular ad hoc networks. In this attack, a malicious node advertises itself as having freshest or shortest path to specific node to absorb packets to itself. The effect of Black hole attack on Adhoc network using AODV as a routing protocol will be studied in this paper. The proposed solution that is capable of detecting and removing Black hole nodes in the VANET at the initial stage itself without any delay. Furthermore, we investigate solution for increasing security in these networks.

KEYWORDS: AODV, Black hole Attack, Packet Delivery Ratio, RREQ, RREP, RERR, VANET Security.

I. INTRODUCTION

A Vehicular Adhoc Network (VANET) is formed dynamically by an autonomous system of vehicular nodes that are connected via wireless links without using an existing infrastructure or centralized administration [1, 2]. VANET nodes are free to move randomly and organize themselves arbitrarily; thus the network's wireless topology may change rapidly and unpredictably. In a VANET, a collection of vehicular hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. A VANET is referred to as an infrastructure less network because the vehicular nodes in the network dynamically set -up paths among themselves to transmit packets temporarily. Nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages. Any routing protocol must encapsulate an essential set of security mechanism. These mechanisms are used to prevent, detect and respond to security attacks. The VANET is more vulnerable to be attacked than wired network. These vulnerabilities are nature of the VANET structure that cannot be removed. As a result, attacks with malicious intent have been and will be devised *to exploit* these vulnerabilities and *to cripple* the VANET operation. The most important characteristics are the dynamic topology, which is a consequence of node mobility. A VANET is a group of vehicular nodes that cooperate and forward packets for each other. One of the most critical problems in VANETs is the security vulnerabilities of the routing protocols. A set of nodes may be compromised in such a way that it may not be possible to detect their malicious behaviour easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic, thus inflicting Byzantine failure in the network. In this paper, we discuss one such attack known as Black Hole Attack on the widely used Ad -hoc On-demand Distance Vector (AODV) routing protocol in VANETs. A mechanism presented shows the method to detect & prevent from Black hole attack in Vehicular ad hoc network. It is an autonomous system, where nodes/stations are connected with each other through wireless links. There is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely. This property of the nodes makes the VANET unpredictable from the point of view of

10.15680/ijircce.2014.0212019

scalability and topology. In Adhoc networks, the routing protocols are divided into three categories: Proactive, Reactive and Hybrid as shown in Figure.1

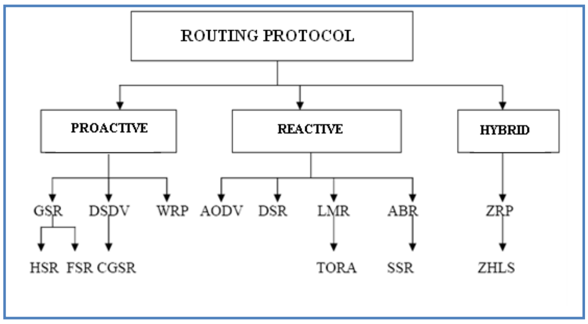

Figure 1: VANET Routing Protocols

II. Related work

The problem of safety & impact of various malicious attacks has received considerable attention by researchers in the vehicular ad-hoc network field. The Ad hoc On-demand Distance Vector (AODV) protocol, one of the on-demand routing algorithms that has receive the most attention, however, does not utilize multiple paths. It joins the mechanisms of DSDV and DSR. The periodic beacons, hop-by-hop routing and the sequence numbers of DSDV and the pure on-demand mechanism of Route Discovery and Route Maintenance of DSR are combined. In AODV at Every instance, route discovery is done for fresh communication which consumes more bandwidth and causes more routing over-head. The source prepares RREQ packet which is broadcast to it's neighboring nodes. If neighboring node will keep backward path towards source. As soon as destination receives the RREQ packet, it sends RREP packet on received path. 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.

A] Sequence Number and Routing Table Management

A node has to update its own sequence number in two cases:

- Before starting a route discovery process, the node has to increment its own sequence number.
- A destination node has to update its own sequence number to the maximum of its current sequence number and the destination sequence number in RREQ packet immediately before transmitting the RREP packet.

The sequence numbers in the routing table entries may be changed by the node only in the following circumstances:

- Offer of a new route to itself, if it is the destination node.
- Reception of an AODV message with new information about the sequence number for a destination.
- Expiration of path or path breaks.

When a node receives an AODV control message, either to create or to update a route for a particular destination, it searches its routing table for an entry to the destination. If there is no route entry, it creates a new one with the sequence number contained in the control packet, or else the sequence number is set invalid. Otherwise, the node compares the existing entry with the new information and updates it if either

- The new sequence number is higher than in the routing table entry,
- The sequence numbers are equal and the new hop count plus one is smaller than in the existing route, or
- The sequence number is unknown.

Besides the destination sequence numbers, the routing entry for each valid route contains a precursor list. This list contains all precursor of the node which are able to forward packets on this route. All neighbouring nodes to which a

10.15680/ijircce.2014.0212019

RREP was generated or forwarded are included in this list. In the event of a next hop link breakage, notifications are sent to those nodes.

III. ANALYSIS OF AODV PROTOCOL

The AODV protocol builds on the DSDV algorithm .it is an on demand routing algorithm. 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.

A] Control Messages in AODV:

• Route Request Message RREQ:

Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

• Route Reply Message RREP:

A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

• Route Error Message RERR:

Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, Route error (RERR) message is generated by the node in order to notify other nodes that the link is down.

B] Route Discovery in AODV:

When a node "A" wants to initiate transmission with another node "G", it will generate a route request message (RREQ). This message is propagated through a limited flooding to other nodes. This control message is forward to the neighbors, and those node forward the control message to their neighbors' nodes. This process of goes on until it finds a node that has a fresh enough route to the destination or destination node is located. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "A" and destination node "G". Once the route is establish node "A" and "G" can communicate with each other. The following diagram show exchange of control messages between source node and destination node.

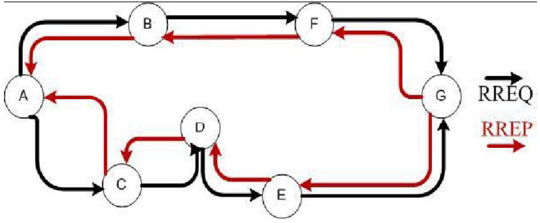

Figure 2: Route Discovery in AODV

When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbors nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating destination node i.e. from node "A" to the neighbors nodes, at node "E" the link is broken between "E" and "G", so a route error RERR message is generated at node "E" and transmitted to the source node informing the source node a route error.

10.15680/ijircce.2014.0212019

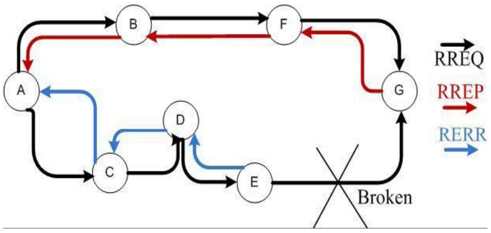

Figure 3: Route Error Message in AODV

c] Black Hole Attack:

Every node maintain a routing table that stores the next hop node information for a route a packet to destination node ,When a source node want to route a packet to the destination node , it uses a specific route if such a route is available in it's routing table.otherwise , nodes initiates a route discovery process by broadcasting *Route Request* (RREQ) message to it's neighbours. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node.A *Route Reply* (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination.We now describe the Black hole attack[10] on VANET'S .The Black hole attack has two phases , In first phase, a mallicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intension of interupting or corrupting packets, event though route is spurious.In second phase ,nodes drops the interupted packets with a certation probability.detection of Black hole is difficult process.

IV. PROPOSED MECHANISM

We consider a VANET consisting of similar types of nodes. Each node may freely roam, or remain stationary in a location for an arbitrary period of time. In addition, each node may join or leave the network, or fail at any time. The nodes perform peer-to-peer communication over shared, bandwidth constrained, error-prone, and multi-hop wireless channel. For the purpose of differentiation, we assume that each node has a unique nonzero ID. All the links in the network are assumed to be bi-directional. However, unlike most of the current security frameworks for VANETs, the proposed mechanism does not assume promiscuous mode of operation of the wireless interfaces of the nodes. The promiscuous mode may not only incur extra computation overhead and energy consumption in order to process the transit packets, but also it will not be feasible in cases where the nodes are equipped with directional antennas. There may be varying number of Black hole nodes in the network at different points of time and these malicious nodes may cooperate with each other to disrupt the communication in the network. The proposed mechanism involves both local and cooperative detection to identify any malicious Black hole node in the network. Once a node is detected to be really malicious, the scheme has a notification mechanism for sending messages to all the nodes that are not yet suspected to be malicious, so that the malicious node can be isolated and not allowed to use any network resources. The mechanism consists of local anomaly security procedures which are invoked sequentially.

V. PROPOSED SOLUTION

The solution that we propose here is basically only modifies the working of the source node without altering intermediate and destination nodes by using a method called Prior_ReceiveReply. In this method three things are added, a new table RR-Table (Request Reply), a timer WT (Waiting Time) and a variable MN-ID (Malicious Node ID) to the data structures in the default AODV Protocol.

VI. ALGORITHM PRIOR-RECEIVE REPLY METHOD
DSN – Destination Sequence Number, NID – Node ID,
MN-ID – Malicious Node ID.
Step 1: (Initialization Process)
Retrieve the current time
Add the current time with waiting time

10.15680/ijircce.2014.0212019

```
Step 2: (Storing Process)
Store all the Route Replies DSN and NID in RR-Table
Repeat the above process until the time exceeds

Step 3: (Identify and Remove Malicious Node)
Retrieve the first entry from RR-Table
If DSN is much greater than SSN then discard entry from RR-Table and store its NID in MN-ID
Step 4: (Node Selection Process)
Sort the contents of RR-Table entries according to the DSN
Select the NID having highest DSN among
RR-table entries
Step 6: (Continue default process)
Call Receive Reply method of default AODV Protocol
```

The above algorithm starts from the initialization process, first set the waiting time for the source node to receive the RREQ coming from other nodes and then add the current time with the waiting time. Then in storing process, store all the RREQ Destination Sequence Number (DSN) and its Node Id in RR-Table until the computed time exceeds. Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table. This is how malicious node is identified and removed. Final process is selecting the next node id that has the higher destination sequence number, is obtained by sorting the RR-Table according to the DSEQ-NO column, whose packet is sent to Receive Reply method in order to continue the default operations of AODV protocol.

VI. CONCLUSION & FUTURE WORK

In this paper we have presented the impact of Black hole attack in Vehicular Adhoc Network & its consequences. VANET has been active research based area over the past few years. But it is vulnerable to various types of attacks. Misbehaviour of nodes causes the damage to the nodes & packet also. Black hole attack cause damage to the network & also it is difficult to detect. Proposed approach can be integrated on the basic of routing protocols such as AODV.To show the effectiveness and result of proposed approach, implementation work on Network Simulator 2 still in progress. Future works will include some mechanism so as to detect & prevent from the Black hole attack in vehicular ad-hoc network.

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)
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).

10.15680/ijircce.2014.0212019

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 HocNetworks”, 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).