ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 8, August 2016

A Novel Approach of Mitigation of Jamming Attack in VANET

Kalyani Singh [1], Mamta Martolia[2]

M-Tech Student [#1] Assit. Prof. [#2] & Uttarakhand Technical University.
Dehradun, Uttarakhand , India

ABSTRACT

Vehicular Ad-Hoc Networks (VANETs) is an indivisible I.T.S component, where nodes are self-organizing, autonomous and self-managing information in a distributed manner. Its foundation is based on the vehicles co-ordination and/or roadside units by which information is distributed in network in organized manner. In recent years, VANET has been obtained more attention of automotive industries and researchers because of life saving factor. But always coin has two faces, when we know about its life saving factors simultaneously security attacks for VANET is also arises, so now VANET requires security to implement the ad hoc atmosphere and serves subscribers with safety and commercial applications.Thus we try to concentrate on examining and enhancing the routing protocol security for VANETS i.e. the Ad hoc On Demand Distance Vector (AODV) routing protocol. We introduce changes to the CTS/RTS mechanism we introduce an algorithm to mitigate the jamming attack on the VANET routing protocols. All the routes has unique sequence no. and the malicious node has the maximum Destination Sequence no. and it is the first RREP to reach. So the comparison is built only to the first entry in the table without examining other entries in the table

Keywords **- AODV, receive reply, Black hole, sequence no., routing table**

I. INTRODUCTION

Routing in ad hoc networks faces a no. of challenges i.e. node mobility, dynamic topology, low battery life, lack of infrastructure, insecure medium and restricted channel capacity, causing an important reduction of routing performance. A no. of reviews cover the security problems and intrusion detection techniques in MANETs [1]. All nodes keep maintaining their routing tables depending on information flood by other nodes. Thus, routing table overflow attacks are possible that can interrupt the routing mechanism. Reactive protocols are more robust against replay attacks due to the behavior of routing messages included, such as with AODV [2]. We introduce an algorithm to determine Black hole attack against the AODV routing protocol. By examine we realize that by appending timer component time is saved and if destination sequence no. is higher than source i.e. value greater than threshold the malicious node is determined at the initial phase itself and immediately eliminated so that it cannot take part in further procedure.

II. GENERAL PROPOSED ALGORITHM

The solution that we introduce here is generally only changes the source node working without changing intermediary and destination nodes by utilizing a method known as Prior_Receive Reply. In this technique three things are appended, 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 actual AODV Protocol.

2.1 Algorithm: Prior-Receive Reply Method

DSN – Destination Sequence Number, NID – Node ID, MN-ID – Malicious Node ID(M node).

Step 1: (Initialization Process) fetch the current time and add the current time with waiting time.

Step 2: (Storing Process) Store all the Route Response DSN and NID in RR-Table(R) table. Replicate the above procedure until the time exceeds.

Step 3: (Identify and Remove Malicious Node) Fetch the first entry from RR-Table, If DSN is much greater than SSN then drop entry from RR-Table and record its NID in MN-ID.

Step 4: (Node Selection Process) Sort the contents of RR-Table entries according to the DSN choose the NID having maximum DSN among RR-table entries.
Step 5: (Continue default process) Call Receive Reply mechanism of default AODV Protocol. The above algorithm initiates from the initialization procedure, first set the waiting time for the source node to obtain the RREQ coming from other nodes and then append the current time with the waiting time. Then in storing procedure, record all the RREQ Destination Sequence No. (DSN) and its Node Id in RR-Table until the calculated time exceeds. Basically the first route response will be from the malicious node with large destination sequence no., which is recorded as the first entry in the RR-Table. Then compare the first destination sequence no. with the source node sequence no., if there available much more differences among them, certainly that node is the malicious node, immediately eliminate that entry from the RR-Table. This is how malicious node is determined and eliminated. Final procedure is choosing the next node id that has the greater destination sequence no., is achieved by sorting the RR-Table according to the DSEQ-NO column, whose packet is forwarded to Receive Reply method for continuing the default operations of AODV protocol. Additionally, the introduced solution manages the malicious node identity as MN-Id, so that in future, it can drop any control messages coming from that node. Now however, malicious node is determined, the routing table for that node is not managed. Additionally, the control messages from the malicious node, too, are not sent in the network. Furthermore, for maintaining freshness the RR-Table is flushed once a route request is selected from it[13]. Hence, the operation of the introduced protocol is similar to original AODV, once the malicious node has been determined.

III. MAIN BENEFITS

(1) The malicious node is detected at the initial phase itself and immediately eliminated so that it cannot play role in further mechanism [14].
(2) With no delay the malicious node is easily detected i.e. as we mentioned before all the routes has unified sequence no.
Basically the malicious node has the maximum Destination Sequence no and it is the first RREP to reach. So the comparison is built only to the first entry in the table without examining other entries in the table.
(3) No change is made in other default operations of AODV Protocol.
(4) Better performance created in little change.
(5) Less memory overhead takes place because only few new things are appended.

For each RREP control message obtained, the source node would first analyze whether it has an entry for the destination in the route table or not. If it discovers one, the source node would examine whether the destination sequence no. in the incoming control message is greater than one it forwarded last in the RREQ or not. If the destination sequence no. is greater, the source node will maintain its routing table with the new RREP control message; else the RREP control message will be dropped [15]. In Route Maintenance stage, if a node detects a connection break or failure, then it forwards RERR message to all the nodes that utilizes the route.

IV. PROPOSED METHODOLOGY

The attacker nodes in the wireless network keep the channel busy for an additional time by changing the duration field value of the RTS packets. Since legitimate nodes will obviously respond to RTS request with CTS frame, an attacker could exploit legitimate nodes to disseminate CTS with manipulated duration field, which causes the attack automatically. These types of attacks on RTS /CTS frame can be identified and removed in order to improve performance efficiency, throughput of network. The packet synchronization mechanism can be applied to do so. The algorithm is as follows:
1. Start
2. Create MANET Scenario with 100,200 Mobile Nodes.
3. Apply Simulation Statistics.
4. Set Threshold = Value;
5. Packet Sent = Value;
6. Run and analyze Results
7. If (Packet Sent > Packet Threshold && Packet Sent < Packet Threshold)
8 Then
9 Declare the Node as a Attacker Node and go to step 12.
10 Else
11 End
12 Apply Proposed Algorithm.
13 f (Packet Sent > Packet Threshold && Packet Sent < Packet Threshold)
{
14. Then Block that Node and go to Step 12.
15 else
{
16 end
17 Display the list of all Blocked Nodes in the MANET that Blocked Node will not be able to participate in further communication.

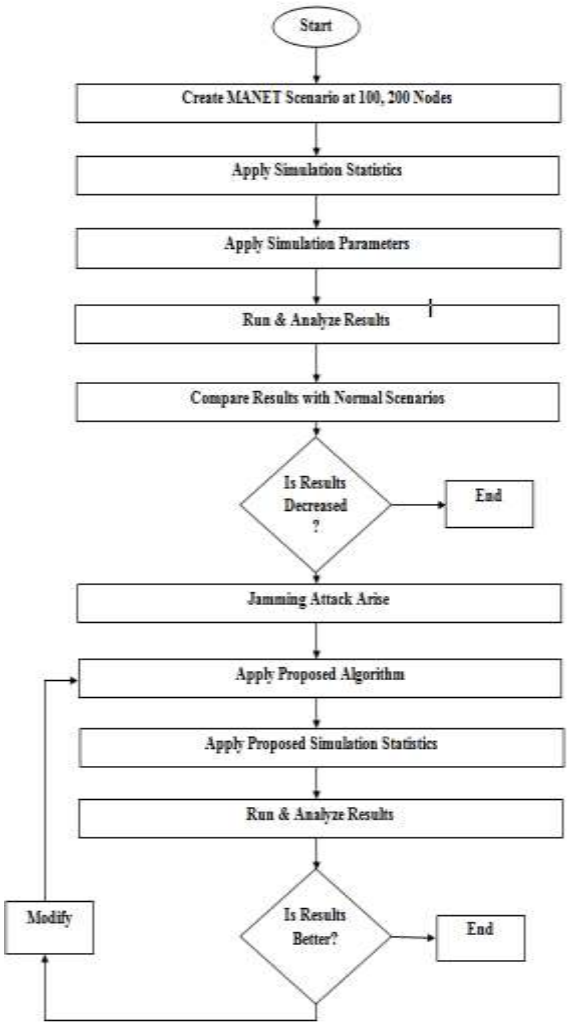

Figure: 1 Flowchart of proposed methodology

V. PROPOSED ALGORITHM

The solution that we introduce here is generally only changes the source node working without changing intermediary and destination nodes by utilizing a method known as Prior_Receive Reply. In this technique three things are appended, 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 actual AODV Protocol.

1. **Pre Receive Reply (Packet P)**
2. **{**
3. **T0 = Get(Current Time Vlaue)**
4. **T1= T0 + M_WAIT_TIME**
5. **While(current time<= t1)**
6. **{**
7. **Store P. Dest. Seq No. and P_Node_ID in C_RREP_T Table**
8. **}**
9. **While(C-RREP_T is not empty)**
10. **{**
11. **Select Dest_Seq_No. from Table**
12. **If (Dest_seq_No >>= Src_Seq_No)**
13. **{**
14. **M_node = Node ID**
15. **Discard entry from table**
16. **}**
17. **}**
18. **Select packet Q for node ID having higest value of Dest._seq_No.**
19. **Receive Reply (Packet Q)**
20. **}**

VI ALGORITHM: PRIOR-RECEIVE REPLY METHOD

DSN – Destination Sequence Number, NID – Node ID, MN-ID – Malicious Node ID(M node).

Step 1: (Initialization Process) fetch the current time and add the current time with waiting time.

Step 2: (Storing Process) Store all the Route Response DSN and NID in RR-Table(R) table. Replicate the above procedure until the time exceeds.

Step 3: (Identify and Remove Malicious Node) Fetch the first entry from RR-Table, If DSN is much greater than SSN then drop entry from RR-Table and record its NID in MN-ID.

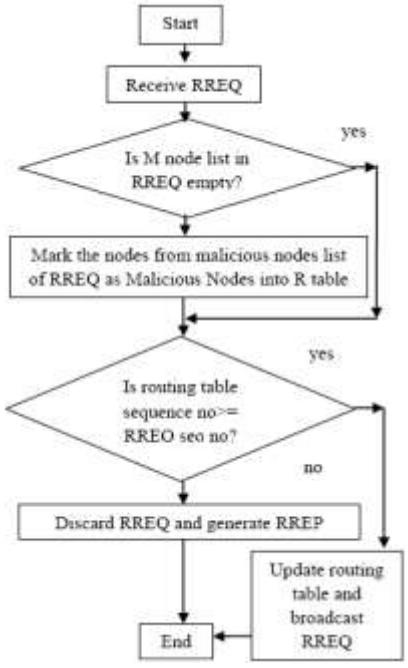

Fig 2: Basic Flow-chart for node broadcasting RREQ

Step 4: (Node Selection Process) Sort the contents of RR-Table entries according to the DSN choose the NID having maximum DSN among RR-table entries.

Step 5: (Continue default process) Call Receive Reply mechanism of default AODV Protocol. The above algorithm initiates from the initialization procedure, first set the waiting time for the source node to obtain the RREQ coming from other nodes and then append the current time with the waiting time. Then in storing procedure, record all the RREQ Destination Sequence No. (DSN) and its Node Id in RR-Table until the calculated time exceeds. Basically the first route response will be from the malicious node with large destination sequence no., which is recorded as the first entry in the RR-Table. Then compare the first destination sequence no. with the source node sequence no., if there available much more differences among them, certainly that node is the malicious node, immediately eliminate that entry from the RR-Table.

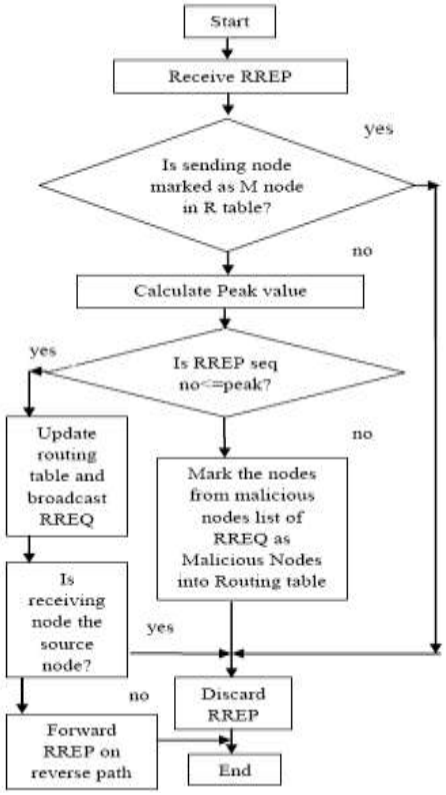

Fig 3 flow-chart for node receiving RREP

This is how malicious node is determined and eliminated. Final procedure is choosing the next node id that has the greater destination sequence no., is achieved by sorting the RR-Table according to the DSEQ-NO column, whose packet is forwarded to Receive Reply method for continuing the default operations of AODV protocol. Additionally, the introduced solution manages the malicious node identity as MN-Id, so that in future, it can drop any control messages coming from that node. Now however, malicious node is determined, the routing table for that node is not managed. Additionally, the control messages from the malicious node, too, are not sent in the network. Furthermore, for maintaining freshness the RR-Table is flushed once a route request is selected from it[13]. Hence, the operation of the introduced protocol is similar to original AODV, once the malicious node has been determined.

VI. CONCLUSION

In comparison of the other techniques, we believe the introduced algorithm is simple and effective and has very less congestion and delay in implementation .We also underline that the introduced algorithm will be implemented and modeled for the mitigation of jamming attack.

REFERENCES

[1] Fatima Ameza, Nassima Assam and Rachid Beghdad, "Defending AODV Routing Protocol Against the Black Hole Attack", International Journal of Computer Science and Information Security, Vol. 8, No.2, 2010, pp.112-117.

[2] Nital Mistry, Devesh C. Jinwala and Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.

[3] Payal N. Raj and Prashant B. Swadas,"DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp: 54-59.

[4] Hoang Lan Nguyen and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 2006, pp. 149-149

[5] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.

[6] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, "Study of Different Attacks on Multicast Mobile Ad hoc Network", Journal of Theoretical and Applied Information Technology, December 2009, pp. 45-51.

[7] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security, vol. 4 issue 3, July 2010, pp. 265-274.

[8] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 14th IEEE International Conference on Network Protocols, November 2006, pp.75-84.

[9] Mahdi Taheri, Dr. majid naderi, Mohammad Bagher Barekatain, "New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks", 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.

[10] Dang Quan Nguyen and Louise Lamont, "A Simple and Efficient Detection of Wormhole Attacks", New Technologies, Mobility and Security, November 2008, pp. 1-5.

[11] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, "Analysis of Wormhole Intrusion Attacks in MANETs", Military Communications Conference, November 2008, pp.1-7.

[12] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, "Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis", Military Communications Conference, October 2006, pp. 1-7.

[13] Mani Arora, Rama Krishna Challa and Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, 2010, pp. 102-104.

[14] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

[15] W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole

[16] Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

[17] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath," IEEE Wireless Commuunication. and Networking Conference,

[18] I. Khalil, S. Bagchi, N. B. Shroff," A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", International Conference on Dependable Systems and Networks, 2005.

[19] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC 2005.

[20] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 11th Network and Distributed System Security Symposium, pp.131-141, 2003.

[21] L.Lazos, R. Poovendran, "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks",ACM Workshop on Wireless Security, pp. 21-30, October 2004.

[22] W. Wang, B. Bhargava, "Visualization of Wormholes in sensor networks", ACM workshop on Wireless Security, pp. 51-60, 2004.

[23] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96- 97.

[24] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, 2009, pp. 141-145.

[25] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp. 21-26.

[26] Geng Peng and Zou Chuanyun,"Routing Attacks and Solutions in Mobile Ad hoc Networks", International Conference on Communication Technology, November 2006, pp. 1-4.

[27] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks", International Conference on Parallel Processing Wowrkshops, August 2002.

[28] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato1, Abbas Jamalipour, and Yoshiaki Nemoto1," Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, vol..5 no..3, Nov. 2007, pp.338–346.

[29] Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols", Chapter 19, pp. 219-229.

[30] G.S. Mamatha and S.C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS", International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.

[31] Preetam Suman, Dhananjay Bisen, Poonam Tomar, Vikas Sejwar and Rajesh Shukla, "Comparative study of Routing Protocols for Mobile Ad- Hoc Networks", International Journal of IT & Knowledge Management, 2010.