International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-5, June 2020

Reducing Accidents Through Detection of Black Hole Attack in VANETs

Dekka Satish, K.Narasimha Raju, B.Srinivasa Rao, G.Sita Ratnam, P.Raja

Abstract*: Vehicular ad hoc networks (VANETs) are upcoming prominent technology in the field of communication with vehicles. It is a combination of mobile and sensor network features. The random change in position of vehicles in VANET made the system more vulnerable to attacks. The most important attack in VANETs to be considered is Black hole attack which increases the chances for packet loss and in turn to accidents. There is a necessity to develop the techniques to detect Black hole attacks and reduce number of accidents. In this paper, a technique called "Detection of Black hole in VANET using AODV (DBVANETuAODV)" is proposed to find and prevent Black hole attack and thereby reducing occurrence of accidents. The proposed solution is implemented using AODV Routing protocol in VANET.The experiments are conducted with SUMO and NS2 simulators to depict network environment in an inexpensive way. The proposed method "DBVANETuAODV" is compared with AODV with black hole and the result shows the proposed method provides a significant improvement.

Keywords: Black hole attack, VANETs, SUMO.

I. INTRODUCTION

VANETs are the subset of Mobile ad hoc network (MANET) where the mobile vehicle becomes the nodes of the communication network. In VANET, the network comprises two fundamental units depending on which the whole network works. They are Road Side Units (RSU) and On-Board Units (OBU). Every moving vehicle (node in a network) is attached by a device called On-board unit which is used to transmit data between other OBUs and RSUs. The Road side units, RSUs, are the stationary devices fixed alongside of the road or mounted to the traffic systems, nearby parking areas etc.To communicate with network devices outside the infrastructure, RSUs are used. Vehicle-to-Vehicle communications (V2V) is the vehicular technology designed such that one vehicle is allowed to make communication with another vehicle. V2V communication is needed to reduce accidents counts and it also extends driving vision. In Vehicle-to-Infrastructure communication (V2I), Road Side Units are used to collect the vehicles' information and data regarding traffic and in turn this information is broadcasted to other (receiver) vehicles. Security plays a vital role in designing VANETs system.

The topology of VANET is dynamic in nature i.e. vehicles are highly mobile and they rapidly change the whole topology. If any attack occurs at any vehicular node, then the whole network is disturbed and become resistless towards other attacks. The security details are represented in the below figure.

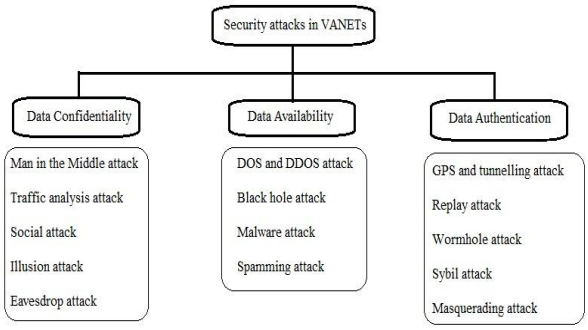

Figure 1: Classification of security attacks in VANET

In majority situations, AODV protocol is the mostly used routing protocol in VANETs as well as in MANETs. This protocol creates path on demand basis and supports unicast as well as multicast routing. Black holes refer to the nodes in the network whose only motive is to silently discard (or "drop") the incoming or outgoing traffic, without letting the source node to know that the sent data packets are not reached its intended destination. Black holes are hard to encounter and they are invisible in the network, and they can only be identified and detected by reviewing and monitoring the lost traffic. . The packet drop is left unknown to source as well as to destination nodes. .

II. RELATED WORK

E. C. Eze et.al [1] described that VANET communication is comprised of V2V and V2I communications which are supported by most used routing protocol, AODV, and various challenges in VANETs. Komal Mehta et.al [2] discussed about various issues such as challenges, routing, and security issues and also

Revised Manuscript Received on June 15, 2020.
* Correspondence Author
Mr.Dekka Satish*, Department of Computer Science and Engineering, Lendi Institute of Engineering and Technology, Viziangaram (A.P), India. E-mail: satishmtech4u@gmail.com
Dr. K. Narasimha Raju, Department of Computer Science and Engineering, Lendi Institute of Engineering and Technology, Viziangaram (A.P), India. E-mail: bcoolmind@gmail.com
Dr.B.SrinivasaRao,Department of Computer Science and Engineering, Dadi Institute of Engineering & Technology(DIET), Visakhapatnam(AP),India.E-mail: ugandarsrinu@gmail.com.
Dr. G.SitaRatnam, Department of Computer Science and Engineering, Lendi Institute of Engineering and Technology, Viziangaram (A.P), India. E-mail: sitagokuruboyina@gmail.com
Mr.P.Raja, Department of Computer Science and Engineering, Lendi Institute of Engineering and Technology, Viziangaram (A.P), India. E-mail: raja.pete99@gmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

performance related parameters. A.D. Devangavi and Gupta [3] said that VANET is the core component of Intelligent Transportation Systems (ITS) which is an integrated approach that is developed to increase the safety of the road transportation systems.

They have also discussed about various types of routing protocols and also detailing their advantages and disadvantages.

S.Yadav et.al [4] discussed about the reliable and secure routing protocols that can be used in VANETs for safe exchange of data and also described that it is very difficult to implement an expeditious routing protocol in a high mobility network due to incentive features of vehicular network.C.E. Perkins et.al [5] discussed about AODV protocol in VANETs. P. S. Gautham et.al [6] discussed the method to find a malicious node that causes black hole attacks. N. Kalia et.al [7] described that there can be many black holes present in a single network. These multiple black holes advertise as they have shortest path to intended destination.

III. METHODOLOGY

In the basic mechanism of AODV the intended nodes checks their routing tables to reach the destination. If a valid path is found it travels the path and reaches the target node the above process involves RREQ, RREP and RERR Messages.RREQ and RREP are uses full for root establishment and RERR is use full to notify route failures when a source node has a data packet addressed to a destination node, the source node checks its routing table first which contains the next hop to use to reach the destination node. However, if a valid route is found, the source node sends the data packet to the next hop to forward it to the target node. If route is not found, the source starts route discovery phase to discover new & fresh route to the destination.

In the proposed system Detection of Black hole in VANET using AODV (DBVANETuAODV),The source node first checks if it received a reply that has a higher destination sequence number (DSN) than its own source sequence number. If source node found any such reply then it shows that the reply came from the black-hole and it discards the RREP reply as there is a rule that all nodes in the network should have a lower DSN than SSN of the source node and then again the source node starts route discovery process and same process follows until it gets a reply having lower DSN than its own SSN. Once getting such reply packet, it checks whether the arrival time of RREP packet is less than the specific time limit, already defined for a node in a particular network, if yes then it indicates that the reply came from the black-hole and it discards the RREP reply and then again the source node broadcasts the RREQ packets. If the received reply packet arrival time is more than the specified time limit, then the source node will update its routing table about the path to the destination node (destination vehicle) including the hop count and source node sends the data packet to the next hop to forward it to the target node. The following algorithm and flowchart in figure summarizes the above mechanism.

Algorithm:

BEGIN
Source node broadcasts RREQ packets
Intermediate nodes receive RREQ packets
Node sends RREP packets to source node
Source node makes entry in its routing table about the RREP packet
Source node checks:
IF (DNS >>> SSN)
THEN
Identify node as a malicious and malevolent node
Node →→ MN
Drop Malicious Node Entry from Routing Table
SN_RT → {Drop (MN)}
Restarts broadcasting RREQ packets for path discovery
ELSE IF (AT (RREP) < STL)
THEN
Identify node as a malicious node
Node →→ MN
Drop Malicious and Malevolent Node Entry from Routing Table
SN_RT → {Drop (MN)}
Restarts broadcasting RREQ packets for route discovery
ELSE
Node →→ Normal Node
Initialize route maintenance to the destination node
Path established and data will be transmitted
END

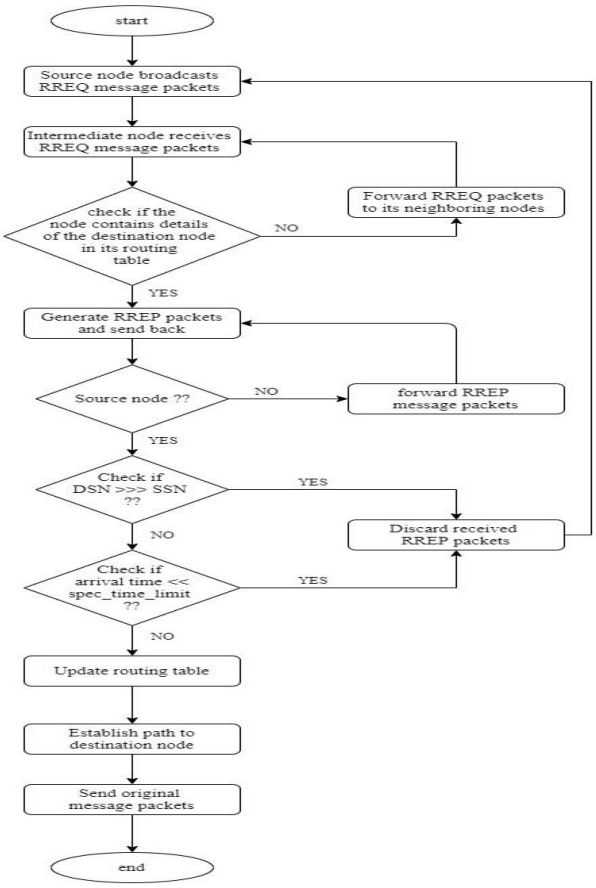

Figure 2: Flowchart

© Copyright: All rights reserved.

IV. RESULTS

The DBVANETuAODV is implemented in SUMO simulator and NS2 simulator. The layout is illustrated with the help of open street map and figures 3, 4 and 5 provide the various views of simulation. The comparative results are shown in the figure 6. The results clearly show improvement of the proposed approach over the existing work.

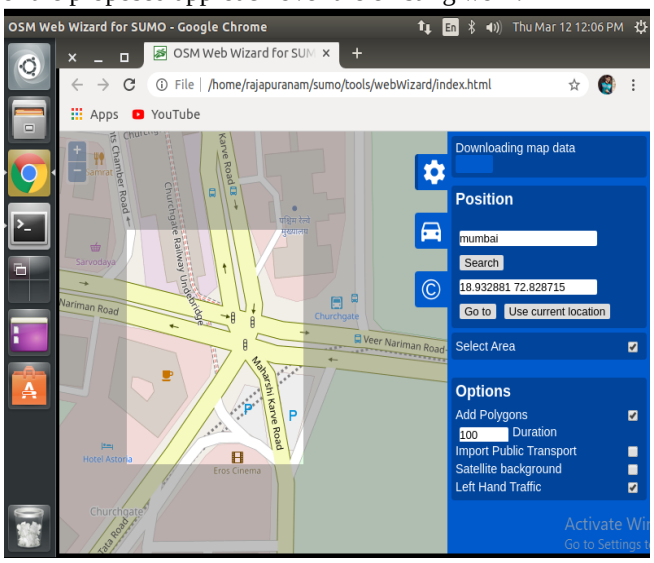

Figure 3: OSM – Open Street Map (Web View)

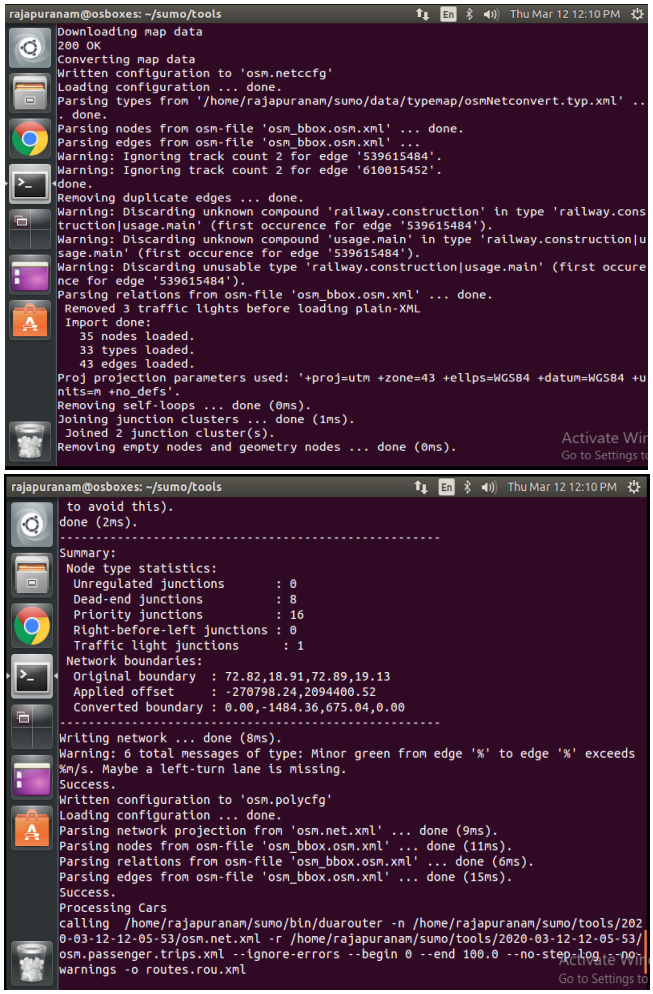

Figure 4: OSM – Open Street Map (Terminal View)

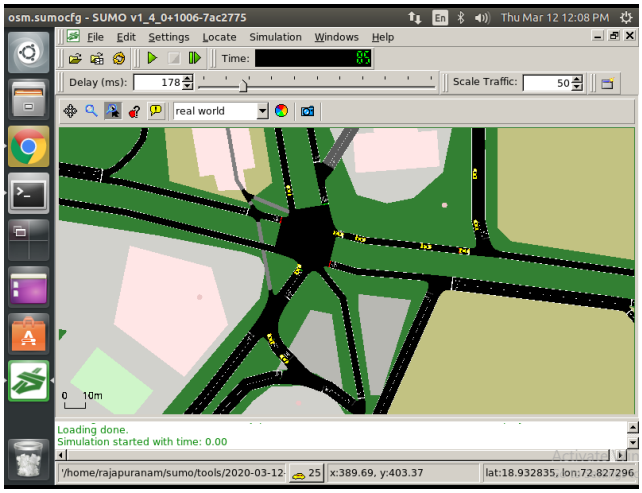

Figure 5: SUMO GUI simulation of the exported map

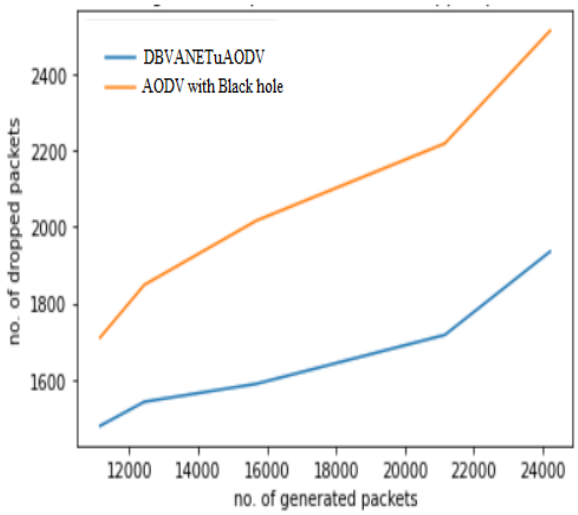

Figure 6: Comparison of dropped packet for DBVANETuAODV and AODV with block hole

V. CONCLUSION AND FUTURE SCOPE

VANET has great impact on road safety and progress passenger convenience in vehicles by exchanging traffic information among the vehicle. On the other hand it is highly exposed to several attacks such as black hole. The proposed work DBVANETuAODV works on the sequence numbers and specified time already set to receive RREP packet. This method provides better and improved communication in VANET over the existing AODV. The future aim of the work is to implement with other protocols.

REFERENCES

1. E. C. Eze, S. Zhang and E. Liu, "Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward," In Proceedings of International Conference on Automation and Computing, IEEE, pp. 176-181, September 2014.
2. Komal Mehta, L. G. Malik and Preeti Bajaj, "VANET: Challenges, Issues and Solutions", In Proceedings of International Conference on Emerging Trends in Engineering and Technology, IEEE , December 2013.
3. Anil D. Devangavi and R. Gupta, "Routing protocols in VANET — A survey," In proceedings of International Conference on Smart Technologies for Smart Nation (SmartTechCon), IEEE, pp. 163-167, August 2017.

© Copyright: All rights reserved.

4. S. Yadav, N. K. Rajput, A. K. Sagar and D. Maheshwari, "Secure and Reliable Routing Protocols for VANETs," In proceedings of International Conference on Computing Communication and Automation , IEEE, pp. 1-5, December 2018.
5. C.E. Perkins, E.M. Royer, S. Das, “Ad hoc On-demand Distance Vector (AODV) Routing”, RFC 3561, July 2003.
6. P. S. Gautham and R. Shanmughasundaram, "Detection and isolation of Black Hole in VANET," In proceedings of International Conference on Intelligent Computing, Instrumentation and Control Technologies, IEEE, pp. 1534-1539, July 2017.
7. N. Kalia and H. Sharma, “Detection of Multiple Black hole nodes attack in MANET by modifying AODV protocol,” International Journal on Computer Science and Engineering, vol. 8, no. 5, pp. 160–174, 2016.

AUTHORS PROFILE

Satish Dekka, M.Tech., (Ph.D.),Associate Professor, CSE Department, Lendi ,Vizianagaram. Expertise and interest Include:Computer Networks, Wireless Sensor networks & internet of things(IoT).

Dr.K.NarasimhaRaju,Professor, CSE Department LENDI, Viziangaram, Expertise and interest include: Computer Networks, Mobile Ad-hoc Networks & Soft Computing.

Dr.B.SrinivasaRao,AssociateProfessor, Department of Computer Science and Engineering, Dadi Institute of Engineering & Technology(DIET),Visakhapatnam(AP), Expertise and interest include: Computer Networks, Mobile Ad-hoc Networks & Communication Networks.

Dr.G.SitaRatnam,AssociateProfessor,CSE Department LENDI, Viziangaram, Expertise and interest include: Computer Networks, Mobile Ad-hoc Networks & Communication Networks.

Mr.P.Raja,Student CSE Dept, Lendi Institute of Engineering and Technology, Viziangaram (A.P), Expertise and interest include: Computer Networks.

© Copyright: All rights reserved.