IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper | Vol.-7, Issue-5, May2019 | E-ISSN: 2347-2693

Securing Vehicular Ad-hoc Network by Two Stage Attacked Node Identification Algorithm

Rajesh Sharma[1*], Ankur Goyal[2]

[1]Department of CSE, Yagyavalkya Institute of Technology, Jaipur, India
[2]Department of CSE, Yagyavalkya Institute of Technology, Jaipur, India

[*]*Corresponding Author: sharma9628@gmail.com, Tel.: +91-99289-01193*

DOI: https://doi.org/10.26438/ijcse/v7i5.10041008 | Available online at: www.ijcseonline.org

Accepted: 21/May/2019, Published: 31/May/2019

Abstract—VANET is a wireless communication system established between multiple vehicles moving on the road. The vehicle nodes are present in network but there are some malicious or attacker nodes whose aim is to harm the network. An attacker vehicle node can raise an alert even if there is no crash on the road or it can falsely divert the traffic in wrong direction for their personal interest. In this paper, the new Two Stage Attacked Node Identification Algorithm (TSANI Algorithm) is proposed. This algorithm identifies the attacker nodes and marks then as unauthentic nodes. The performance of new algorithm is analysed and compared with the existing work.

Keywords—VANET, DTN, MANET, Security, TSANI, Attacks.

I. INTRODUCTION

The wireless ad-hoc networks and the popular IEEE 802.11 protocol are now capable to provide the connectivity to the moving users with the use of Omni directional antenna [1]. A Vehicular Ad-hoc Network (VANET) represents an ad-hoc technology [2]. Wireless network permits its nodes to communicate with each other wirelessly. It can be categorized in Infrastructure less Mode and Infrastructure Mode [3].

Vehicular ad-hoc networks (VANETs) are special class of MANETs which are characterized as distributed and self-organized networks formed by moving vehicular nodes with no central administration. VANETs area network units that are created by applying the principles of mobile ad-hoc networks [4]. VANETs are comprised of On Board Units (OBUs) that are provided with vehicles and Road Side Units (RSUs), which are arranged along the roads [5]. Communication is transmitted from the Roadside Unit to the On-Board unit in the vehicle, and also a vehicle to vehicle communication [6]. The communication can be only vehicle-to-vehicle (V2V) or may also involve some roadside infrastructures [7].

Intelligent transportation systems (ITS) helps in the situations, when an accident occurs on the road and the vehicles coming in the direction of accidental place should be aware of incident so that vehicles can choose alternate path to avoid congestion on the road [8].

Delay tolerant networks (DTN) are those networks which do not require immediate data delivery and can wait for a specific time period before the delivery of data. DTN uses the concept of store and forward. There may be multiple copies of a bundle simultaneously in a DTN network because of store and forward strategy [8].

Vehicular networks can be treated as DTNs and defined as Vehicular Delay Tolerant Networks (VDTNs) [9]. The ERDV is the routing method used in the VANET DTN [8]. In the ERDV scheme, it is considered that each vehicle is equipped with Global Positioning System (GPS) and is able to get the information about its current location. Every vehicle broadcasts HELLO message every time. Each HELLO message has the information about speed and direction of vehicle which has generated it. The packets are transferred to the vehicle that has the highest speed in the coverage. This process continues until the packet reaches at the destination [7].

The security of VANETs [10] is crucial as their very existence relates to critical life threatening situations. It is imperative that vital information cannot be inserted or modified by a malicious person. The system must be able to determine the liability of drivers while still maintaining their privacy. These problems are difficult to solve because of the network size, the speed of the vehicles, their relative geographic position and the randomness of the connectivity between them. There are different attacks on the network like attack on authenticity, attack on availability, attack on confidentiality, attack on Routing Protocol etc. These attacks should be removed from the network to enhance the network.

This paper is divided in five different sections. Section I contains the introduction of the VANET, DTN, ITS, security issues etc. The Section II gives the work performed by different researchers. The Section III discusses about the proposed algorithm for identification of attacker node. Section IV contains the results and their comparison with present algorithm. Section V gives the conclusion of work and future work.

II. Literature Survey

In [7] authors proposed a Misbehaviour Detection Scheme (MDS) and analyze the dependence of its reliability performance on the micro-mobility model of the vehicles and its parameter estimation. In [11] authors proposed several solutions for securing safety messages. The significant below against the security of VANET is a Sybil attack. In [12] authors proposed algorithm DMN-Detection of Malicious Nodes in VANETsimproves DMV Algorithm in terms of effective selection of verifiers for detection of malicious nodes and hence improves the network performance. In [13] authors present the performance analysis of the black hole attack in Vehicular Ad-hoc Network. Authors elaborate the different types of attacks and their depth in ad-hoc network. In [14] authors proposed an Attacked Packet Detection Algorithm (APDA) which is used to detect the DOS (Denial of Service) attacks before the verification time. In [15] authors proposed to overcome the Sybil and prankster attacks on the VANETs. The new solution is capable of detecting the fake information injections by verifying the VANET node behaviour in the cluster. In [16] authors analyzed the performance of VANET in presence of black hole node by using different routing protocols AODV, DSR and AOMDV. In [17] authors proposed a two-phase model that is able to motivate nodes to behave cooperatively during clusters formation and detect misbehaving nodes after clusters are formed. In [18], authors proposed provide trust based on TRIP (Trust and Reputation infrastructurebased proposal) algorithm for traffic analyzing. In [19] authors introduced genetic algorithm for optimization of fake nodes then again check the value on the basis of some specific parameters. In [20] authors presented a geometric model to predict the recommended maximum range of a one hop broadcast message. In [21] authors proposed a method to remove the malicious node from the network. AODV Routing Protocol is analysed in VANET with and without malicious attack. In [22] authors proposed a new Modified Sybil Attacked Node Identification Algorithm(MSANI Algorithm). In [23] authors proposed a new algorithm to enhance the security mechanism of AODV protocol and to introduce a mechanism to detect Black Hole Attacks and to prevent the network from such attacks.

III. Proposed Work

Although a work was performed to improve the VANET by identification of the attacking node but it has different problems that are associated with it. The MSANI algorithm [22] has problems that algorithm has no method to check the node at the RSU level. There is no method to check the vehicle node between the two RSUs. There is no third party checker is situated between the two RSUs to authenticate the vehicle nodes. These limitations make the MSANI Algorithm weak to handle the attacker node.

To remove the problems, a new algorithm is proposed called Two Stage Attacked Node Identification Algorithm (TSANI Algorithm). It uses the two stages for securing the VANET:

i. At the entering RSU

RSU selects all the nodes which are in the coverage range of RSU. Now it selects the node which has the nearest position. The direction of the selected node is calculated and compared with the received direction. If both are correct then selected vehicle node is authentic node and packet can be transferred otherwise new vehicle node is selected.

ii. Between the two RSUs

To check the authenticity of the vehicle nodes, the RSU will appoint the Checker Ferry (CF) that will check the nodes between two RSUs. The RSU checks the vehicle nodes which are in the coverage area of the RSU. It selects the node as CF which is far from RSU. The selected node will work as Checker. It will fix during the life time of CF. CF checks the nodes in the coverage area on the basis of direction calculated and received from the vehicle nodes. If directions are same, then CF assigns the CFCheckValue=1 and authenticates the vehicle node otherwise CF assigns the CFCheckValue=0. This indicates that the node is not valid node. Now during the ERDV packet transferring process, the value of CFCheckValue will be used. The packets will be transferred to vehicle nodes as DF that has the CFCheckValue =1. If value is zero, no packets will be transferred.

IV. Simulation and Result Analysis

A. TSANI Algorithm

The experiments are performed by taking nodes 10, 20, 30, 40 and 50. The Delay and % of identified attacked node are measured. The minimum delay is 25.2782 ms and maximum delay is 30.5514 ms for Packet = 1. The minimum delay is 34.5541 ms and maximum delay is 37.5338 ms for Packet = 5. The identified minimum attacked node % is 46.98 % and maximum is 61.83% for Packet = 1. The identified minimum attacked node % is 37.89% and maximum is 56.44% for Packet = 5. The delay graph in the TSANI Algorithm for Packet = 1 and Packet = 5 is shown in fig. 1 and fig. 2 respectively. The percent of identified attacked node graph in the MSANI Algorithm for Packet = 1 andPacket = 5 is shown in fig. 3 and fig. 4 respectively.

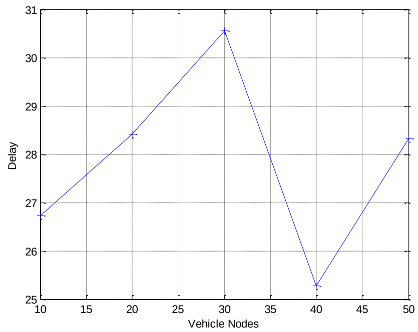

Fig. 1 Delay Graph for Proposed Algorithm at Packet = 1

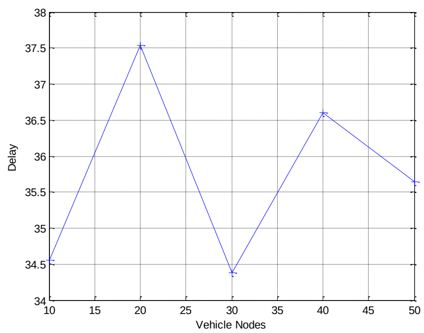

Fig. 2 Delay Graph for Proposed Algorithm at Packet =5

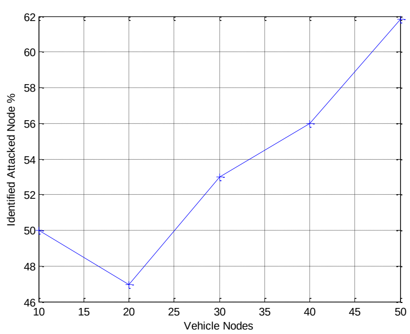

Fig. 3 Percent ofIdentified Attacked Node Graph for Proposed Algorithm at Packet = 1

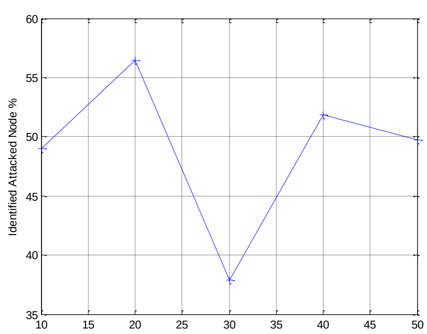

Fig. 4 Percent of Identified Attacked Node Graph for Proposed Algorithm at Packet = 5

B. Comparative Analysis of Results

The delay analysis for existing algorithm and Proposed Algorithm (TSANI Algorithm) for Packet=1 and Packet=5 is shown in the fig. 5 and fig. 6 respectively. It is concluded from the figures that the delay is reduced in the TSANI algorithm in comparison to existing algorithm. The percent of identified attacked node analysis for existing algorithm and proposed algorithm (TSANI Algorithm) for Packet=1 and Packet=5 is shown in the figure 7 and fig. 8 respectively. It is concluded from the figures that the percent of identified attacked node is increased. The proposed algorithm is better to identify the attacker node.

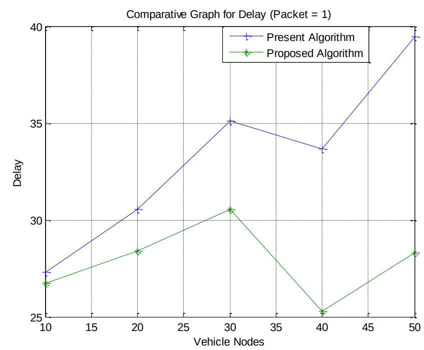

Fig. 5 Delay Comparative Graph for Packet = 1

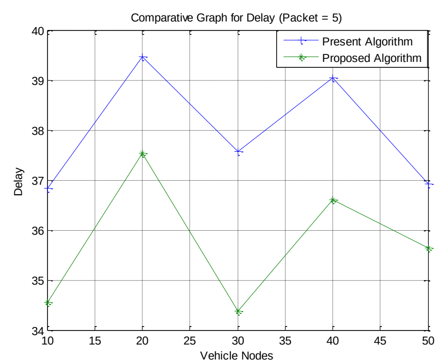

Fig. 6 Delay Comparative Graph for Packet = 5

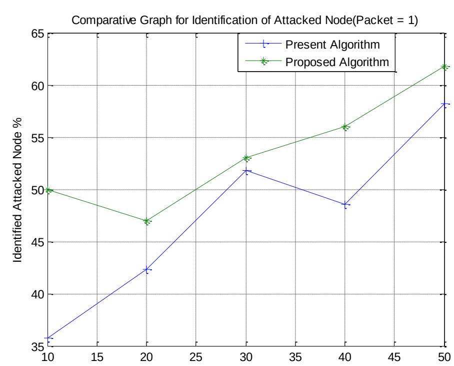

Fig. 7 Attacked Node Comparative Graph for Packet = 1

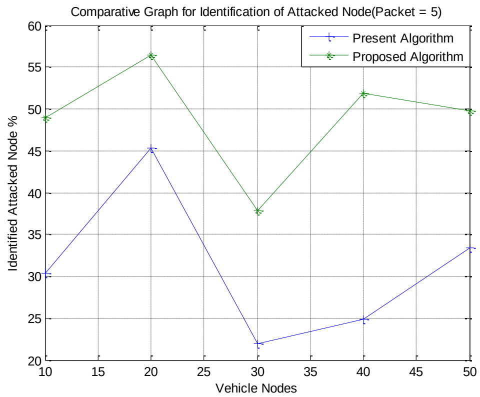

Fig. 8 Attacked Node Comparative Graph for Packet =5

V. Conclusion and Future Scope

The security of network is more challenging task. Lot of work is performed to identify the attacker nodes. In this paper, the TSANI Algorithm is proposed which works on the concept of two stage authentication of the vehicle nodes. The delay reduction varies from 2.16% to 28.19% for Packet=1 and varies from 3.48% to 8.52% for Packet =5. The identification of attacked nodes varies from 2.38% to 40.02% for Packet=1 and varies from 24.4% to 108.44% for Packet =5. From the analysis of results, it is concluded that proposed TSANI algorithm gives the less delay and identifies attacked nodes in better way than the existing algorithm. In future other quality of service parameters can be considered to improve the network.

References

[1] Geetha Jayakumar, Gopinath Ganapathi, "*Reference Point Group Mobility and Random Waypoint Models in Performance Evaluation of MANET Routing Protocols*", Journal of Computer Systems, Networks, and Communications, Volume 2008.

[2] A Peppino Fazio, Floriano De Rango, Cesare Sottile, and Amilcare Francesco Santamaria, "*Routing Optimization in Vehicular Networks: A New Approach Based on Multi objective Metrics and Minimum Spanning Tree*", International Journal of Distributed Sensor Networks, Volume 2013, Article ID 598675, 2013

[3] Jochen H. Schiller, "*Mobile Communications*", Second Edition, Pearson Education Limited, 2003

[4] R. Yogapriya, A. Subramani, "*A Survey on Vulnerabilities, Attacks and Issues in MANET, WSN and VANET*", International Journal of Computer Sciences and Engineering,Vol.-6, Issue-11, Nov - 2018.

[5] [2p] Deepak Rewadkar, Dharmpal Doye, "*Adaptive-ARW: Adaptive Autoregressive Whale Optimization Algorithm for Traffic-Aware Routing in Urban VANET*", International Journal of Computer Sciences and Engineering, Volume-6, Issue-3, March 2018.

[6] Arif Sari, Onder Onursal, Murat Akkaya, "*Review of the Security Issues in Vehicular Ad-hoc Networks (VANET)*", Int. J. Communications, Network and System Sciences, 2015, 8, 552-566, December 2015.

[7] Mainak Ghosh, Anitha Varghese, Arzad A. Kheraniand, Arobinda Gupta, "*Distributed Misbehavior Detection in VANETs*", WCNC 2009 proceedings, IEEE 2009.

[8] Arun Kumar, "*Enhanced Routing in Delay Tolerant Enabled Vehicular Ad-hoc Networks*", International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012.

[9] Vishnu Sharma, Ankur Goyal, "*Delay Analysis of Proposed DMN Algorithm in VANET*", International Journal of Computer Sciences and Engineering, Vol.-7, Issue-1, Jan 2019.

[10] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, "*Vehicular ad-hoc networks (VANETS): status, results, and challenges*", Springer Science Business Media, LLC 2010.

[11] RAVNEET KAUR, Nitika Chowdhary, Jyoteesh Malhotra, "*Sybil Attacks Detection in Vehicular Ad-hoc Networks*", International Journal of Advanced Research, Volume 3, Issue 6, 1085-1096, 2015.

[12] Uzma Khana, Shikha Agrawal, Sanjay Silakaria, "*Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks*", Procedia Computer Science 46, 965 – 972, 2015.

[13] Vimal Bibhu, Kumar Roshan, "*Performance Analysis of Black Hole Attack in VANET*", I. J. Computer Network and Information Security, 11, 47-54, 2012.

[14] S. Roselin Mary, M. Maheshwari, M. Thamaraiselvan, "*Early Detection Of DOS Attacks In VANET Using Attacked Packet Detection Algorithm (APDA)*", International Conference on Information Communication and Embedded Systems, ICICES 2013.

[15] Mandeep Kaur, Manish Mahajan, "*Movement Abnormality Evaluation Model in the Partially Centralized VANETs for Prevention Against Sybil Attack*", I.J. Modern Education and Computer Science, 11, 20-27, 2015.

[16] Sonia, Padmavati, "*Performance analysis of Black Hole Attack on Vanet's Reactive Routing Protocols*", International Journal of Computer Applications (0975 – 8887) Volume 73– No.9, July 2013

[17] Omar Abdel Wahab, Hadi Otrok, Azzam Mourad, "*A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles*", Elsevier, Computer Communications 41, 43–54, 2014.

[18] Gómez Mármol, Félix, and Gregorio Martínez Pérez, "*TRIP, a trust and reputation infrastructure-based proposal for vehicular ad-hoc networks*", Journal of Network and Computer Applications 35 springer, no. 3, pp- 934-941, 2012.

[19] Harsimrat Kaur, Preeti Bansal, "*Efficient Detection & Prevention of Sybil Attack in VANET*", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 9, September 2015.

[20] Khalid Abdel Hafeez, Lian Zhao, Zaiyi Liao, Bobby Ngok-Wah Ma, "*A New Broadcast Protocol For Vehicular Ad-hoc Networks Safety Applications*", IEEE Globecom 2010 proceedings, 2010.

[21] Taskeen Zaidi, Shubhang Giri, Shivam Chaurasia, Pragya Srivastava and Rishabh Kapoor, "*Malicious Node Detection through AODV in VANET*", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), Vol.9, No.2, April 2018.

[22] Archana Harit, N C Barwar , " *Comparative Analysis of Identification of Malicious Node in VANET using FFRDV and ERDV Routing Algorithm*", International Journal of Advanced Technology in Engineering and Science, Vol. 4, Issue 8, August 2016.

[23] Parul Tyagi, Deepak Dembla, "*Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)*", Egyptian Informatics Journal, 18, 133–139, 2017.

Authors Profile

Mr. Rajesh Sharma is pursuing his M.Tech from Y.I.T., Jaipur in Computer Science and Engineering. He completed his B.Tech. from Rajasthan Technical University, Kota. His area of interest is VANET, DTN, etc.

Mr Ankur Goyal pursued B.E. from University of Rajasthan, Jaipur and M.Tech. from RTU Kota. Presently he is working as Associate Professor in Y.I.T., Jaipur. His area of interest is Wireless network.