IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-1, Jan 2019 E-ISSN: 2347-2693

Delay Analysis of Proposed DMN Algorithm in VANET

Vishnu 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: vish.kingvish@gmail.com, Tel.: +91-86194-28507*

Available online at: www.ijcseonline.org

Accepted: 20/Jan/2019, Published: 31/Jan/2019

Abstract— Wireless networks are the technology changer that has changed the modern communication system. In the field of intelligent transport system, wireless network play an important role in the form of Vehicular Adhoc Network (VANET). VANET is a special type of adhoc wireless network which is characterised with fast moving vehicle node, high vehicle speed, and moving along the road. But the VANETs have the security issues. The different malicious nodes present in the coverage decrease the efficiency of the network. Researchers have performed lot of work to secure the VANET. In this work, a new algorithm is proposed for the detection of malicious nodes in VANET. The proposed algorithm is designed and implemented. The results show that there is improvement in the VANET.

Keywords—VANET, attacks, DMN, ERDV, routing protocol.

I. INTRODUCTION

To fulfil the requirement of mobile users a special kind of network is getting more and more attention which is ad hoc network. Such wireless ad hoc networks use the popular IEEE 802.11 protocol for communication [1]. A vehicular ad hoc network (VANET) is an ad hoc wireless communication system setup between multiple vehicles in a neighbourhood. VANETs are used for infotainment, safety, financial and navigational aid [2]. Vehicles can afford significant computing, communication, and sensing capabilities if provided with continuous transmission of power to work them for functioning [3]. The ad hoc domain is composed of vehicles equipped with the on board units (OBUs) and roadside units (RSUs). An OBU is a mobile node of an ad hoc network and RSU is a fixed node. An RSU can be connected to the Internet via the network devices. RSUs can communicate with each other directly or by using the different intermediate nodes.

The number and distribution of roadside units is dependent on the communication protocol to be used [4]. VANET helps in the situations, when an accident occurs on the road, then vehicles can choose alternate path to avoid congestion on the road [5]. VANETs face highly variable density of traffic, which affects drastically to connectivity and coverage of the ad hoc networking [6]. There are large numbers of problems in VANET. These are High Movement, real time work, Location Awareness etc. [7].

Vehicular networks can be treated as DTNs and defined as vehicular delay tolerant networks (VDTNs) [8]. The VDTNs are characterized by very short contacts between nodes and a highly dynamic network topology, where routing is particularly a challenging problem. For the wireless communication, IEEE 802.11 is used [9].

Security of a network is the key factor in the network design. There are so many problems that are associated with the security issues. The VANET security requirements are availability, authenticity, confidentiality, integrity, non-repudiation, privacy etc. [10]. There are various types of attackers in the VANET that are harmful for network like insider, outsider, active, passive, etc [11]. There are so many routing attacks [12] that create burden in the network like black hole, gray hole, illusion attack, etc. Different misbehaviour detection schemes have been proposed by researchers in order to identify the attackers responsible for misconducts in VANETs. Detection of such malicious nodes and abnormal activities in the network is very significant in order to devise precautionary measures for it. Detection of Malicious Nodes is a technique in which malicious nodes that drops and duplicate packets in the network using monitoring approach are detected effectively[13] [14].

This paper is divided in five sections. Section I contains the introduction of the VANETs. The Section II gives the description of the work performed by different authors. The Section III describes about the proposed work. Section IV contains the results analysis. Section V describes the conclusion of work with future work.

© 2019, IJCSE All Rights Reserved

II. RELATED WORK

In [15], the authors proposed a general approach to detecting and correcting errors that have been maliciously introduced by the malicious nodes into data in a VANET. In [16], the authors proposed an approach to detect the fake messages by malicious nodes. In [17], authors presented the important and unique characteristics of VANET. Architecture of the VANET has been designed with a Centralized Authority to which every vehicle and RSU registers. In [18], authors proposed an Attacked Packet Detection Algorithm (APDA) which is used to detect the DOS (Denial of Service) attacks before the verification time. In [19], 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 [20], the authors detected the malicious node in a network with malicious vehicle node detection (MVND) algorithm. In [21], authors proposed solutions for securing the safety messages. In [22], the authors introduced genetic algorithm for optimization of fake nodes. In [23], the authors proposed system to handles the various attacks in the VANET. In [24], the authors proposed an Enhanced Prediction-based Authentication protocol to secure and robust the VANETs. In [25], the authors observed that VANET has been facing many problems mainly in terms of security. In [26], authors described two new variants of attacks in which multiple malicious nodes undertake a black hole attack on a network. In [27], author proposed a new technique to detect the malicious node in VANET. In [28], authors proposed a new algorithm for detection of Sybil attack. In [29], authors performed the performance analysis of VANET.

III. PROPOSED WORK

The different networks like VANET, MANET [30], etc. are having the security issues. To secure the network, detection of malicious node is required. A new DMN algorithm is proposed for VANET.

In the proposed DMN Algorithm, the base ferry (BF) checks every node in two ways to detect the malicious node. The authentication of the vehicle node is performed in these two steps by the BF. The node has the GPS location and it is denoted by the (X, Y) coordinates. The vehicle node has coordinate (Xp,Yp) and the BF node (Xc,Yc). Vehicle nodes are moving on the road with a specific speed. Each vehicle has OBU with antenna that is mounted on the vehicle node.

Each vehicle node broadcasts the GPS location, its speed, its Direction and its position whether it is in coverage area or not. The BF receives the broadcasted information and calculates the distance with every vehicle node. Now compare this distance with the transmission range of the BF and find that whether it is in the coverage area or not. If the calculated position and the received position of the vehicle node are same then the vehicle node is authentic, otherwise the vehicle node is malicious node and the Alarm Value should be 1. The node is removed from the network.

In the next step, the BF node calculates the direction of the vehicle node by taking the GPS location coordinates. The direction of the vehicle node is also received by BF node. Now it is compared with the calculated direction. If both are equal then it indicates that the vehicle node is authentic otherwise the node is malicious node. In this case the Alarm Value should be 1 and node is identified as the Malicious node. It is removed from the network. Now the packets are transferred using the ERDV protocol.

IV. RESULTS AND DISCUSSION

To obtain the results, the numbers of packets are taken as 1, 5 and 10. The experiments are performed. It is observed from results that the delay varies from 20.515 sec. to 24.032 sec. when value of packet is taken 1. Delay varies from 20.3424 sec to 26.4076 sec when value of packet is taken 5. The delay varies from 20.1592 sec to 25.6351 sec for packet value 10. The delay graphs are shown in fig. 1, 2 and 3 for Packet =1, Packet =5 and Packet=10 respectively.

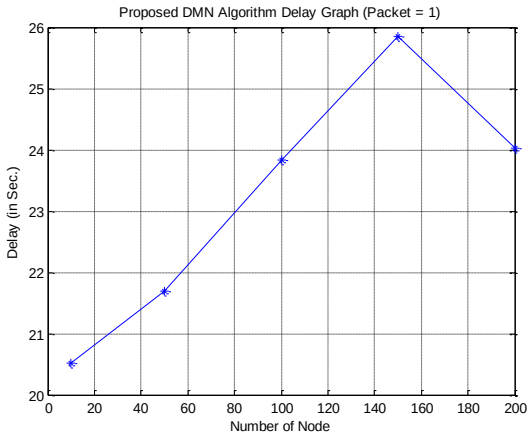

Fig. 1 Proposed DMN Algorithm Delay Graph for Packet = 1

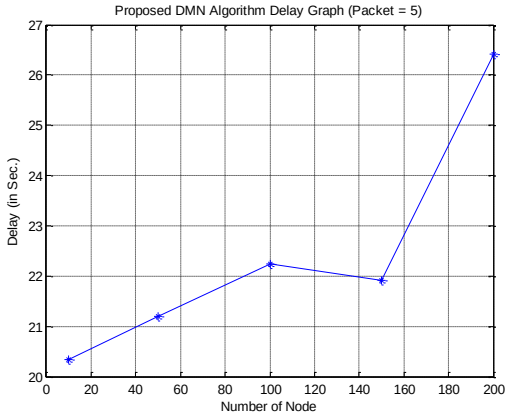

Fig. 2 Proposed DMN Algorithm Delay Graph for Packet = 5

© 2019, IJCSE All Rights Reserved

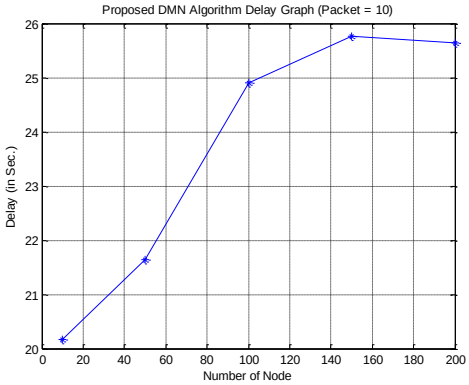

Fig. 3 Proposed DMN Algorithm Delay Graph for Packet = 10

The results of ERDV and proposed DMN Algorithm are analyzed. The percentage improvement is shown in fig. 4. There is maximum 19.07% improvement in the delay. The delay is reduced and the network quality of services improved.

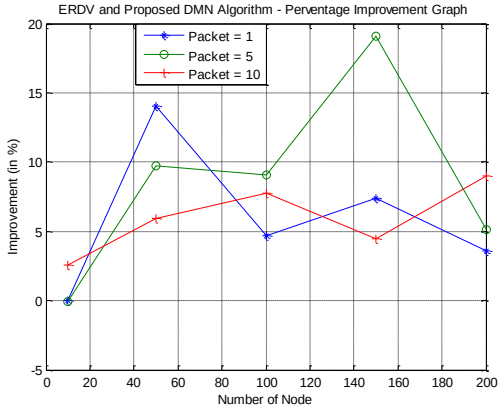

Fig. 4 Percentage Improvement in Delay Graph

V. CONCLUSION AND FUTURE SCOPE

The VANETs are facing different problems of security, authentication, malicious nodes etc. These problems degrade the network efficiency. In the malicious node problem, the false information is transmitted by the nodes which create overload of the packets in the network and security issues. In this work new DMN algorithm is proposed. The proposed DMN Algorithm detects the malicious nodes and improves the network by reducing the delay. There is maximum 19.07% improvement in the delay. The delay is reduced and the network quality of services improved. By performing new designs, vehicular ad hoc network can be improved. Different simulation tools can be used to implement VANET.

ACKNOWLEDGMENT

Thanks to Er. Tara Chand Soni (Member IETE) for their support.

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

[3] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie, "*Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends*", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, Volume 2015, Article ID 745303.

[4] 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.

[5] 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.

[6] Jani Kurhinen, Jukka Janatuinen, "*Delay Tolerant Routing in Sparse Vehicular Ad Hoc Networks*", Acta Electrotechnica et Informatica, Vol. 8, No. 3, 2008, 7–13.

[7] Archana Harit, N C Barwar, "*Comparative Analysis of Identification of Malicious Node in VANET using FFRDV and ERDV Routing Algorithm*", 6th International Conference on Recent Innovation in Science, Engineering and Management, IIMT College of Engineering, 20 August 2016.

[8] Hyunwoo Kang, Syed Hassan Ahmed, Dongkyun Kim, and Yun-Su Chung, "*Routing Protocols for Vehicular Delay Tolerant Networks: A Survey*", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2015, Article ID 325027.

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

[10] Chaker Abdelaziz Kerrache, Carlos T. Calafate, Juan-Carlos Cano, Nasreddine Lagraa, Pietro Manzoni, "*Trust Management for Vehicular Networks: An Adversary-Oriented Overview*", IEEE Access, Received December 1, 2016, accepted December 20, 2016, date of publication December 26, 2016, date of current version January 27, 2017.

[11] Amit Mane A., "*Privacy Aware VANET Security: - Sybil Attack Detection in VANET*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 4, April 2017 ISSN: 2277 128X.

[12] Jayant Vasu, Gaurav Tejpal, Sonal Sharma, "*Review on Various outing Attacks in Vehicular Adhoc Networks*", International Journal of Computer Applications (0975 – 8887), Volume 167 – No.1, June 2017.

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

[14] Uzma Khan, Shikha Agrawal and Sanjay Silakari, "*A Detailed Survey on Misbehavior Node Detection Techniques in Vehicular Ad Hoc Networks*", Information Systems Design and Intelligent Applications, Advances in Intelligent Systems and Computing 339, Springer India, 2015

[15] Philippe Golle, Dan Greene, Jessica Staddon, "*Detecting and Correcting Malicious Data in VANETs*", VANET'04, October 1, 2004, Philadelphia, Pennsylvania, USA. ACM, 2004

[16] Gurpreet Singh, Seema, "*Malicious Data Detection in VANET*", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 7, September 2012

© 2019, IJCSE All Rights Reserved

[17] V. Lakshmi Praba, A. Ranichitra, "*Detecting Malicious Vehicle in a VANET scenario by Incoporating Security in AODV Protocol*", ICTACT Journal on Communication Technology, Vol: 03, Issue: 03, Sept. 2012

[18] S. RoselinMary, 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

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

[20] Miss S.A. Ghorsad, Dr. V. M. Thakare Dr. R.V Dharaskar, "DoS Attack Detection in Vehicular Ad-Hoc Network Using Malicious Node Detection Algorithm", International Conference on "Advances in Computing, Communication And Intelligence" ICACC 2014 Special Issue of International Journal of Electronics, Communication & Soft Computing Science and Engineering, 2014.

[21] Ravneet Kaur, Nitika Chowdhary, Jyoteesh Malhotra, "*Sybil Attacks Detection in Vehicular Ad Hoc Networks*", International Journal of Advanced Research, Volume 3, Issue 6, 2015, pp.1085-1096.

[22] 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.

[23] Adity, Dalveer Kaur, "Detection and Prevention of Malacious Node using Data Centric Technique", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 5, Issue 2, March - April 2016.

[24] J.Nethravathy, Dr.G. Maragatham, "*Malicious Node detection in Vehicle to Vehicle Communication*", International Journal of Engineering Trends and Technology (IJETT), Volume 33 Number 5- March 2016.

[25] Zaid Abdulkader, Azizol Abdullah, Mohd Taufik Abdullah, Zuriati Ahmad Zukarnain, "*Malicious Node Identification Routing and Protection Mechanism for VANET against Various Attacks*", Journal of Information Security Research, Volume 8, Number 4, December 2017.

[26] John Tobin, Christina Thorpe, Damien Magoni, Liam Murphy. "An Approach to Mitigate Multiple Malicious Node Black Hole Attacks on VANETs", 16th European Conference on Cyber Warfare and Security, Dublin, Ireland. Proceedings of the 16th European Conference on Cyber Warfare and Security. <hal-01577471>, Jun 2017.

[27] Vishal Shrivastava, Ajay Samota, "*A Framework for Detecting Malicious Node in VANET*", International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN: 2454-4248, Volume: 4, Issue: 6, June 2018.

[28] Kanwalprit Singh, Harmanpreet kaur, "*Evaluation of proposed technique for detection of Sybil attack in VANET*", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.5, pp.11-15, October (2018)

[29] R. Kumari, P. Nand, "*Performance Analysis for MANETs using certain realistic mobility models: NS-2*", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.1, pp.70-77, February (2018).

[30] P. Chouksey, "*Introduction to MANET*", Introduction of MANET. International Journal of Scientific Research in Network Security and Communication, 4(2), 15-19.

Authors Profile

Mr. Vishnu 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.

Mr Ankur Goyal pursed 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.

© 2019, IJCSE All Rights Reserved