International Journal of Electronics Communication and Computer Engineering
Volume 9, Issue 6, ISSN (Online): 2249–071X

Improving the performance of mobile nodes in VANET

Rohit singh Rajput[1] and Dr. Rachana Dubey[2*]
[1]M. Tech Scholar, Department of CSE, LNCTE, Bhopal (India).
[2*]Professor & Head, Department of CSE, LNCTE, Bhopal (India).
email id: [1]rajpoot.rohit2010@gmail.com ; [2*]rachanamishra812@gmail.com
[*]Corresponding author

Date of publication (dd/mm/yyyy): 24/12/2018

***Abstract* – In the recent years, car manufacturing industries, academia and government agencies have started putting much joint efforts together towards realizing the concept of vehicular communications in wide scale. Some frameworks are already worked out with the first landmark of standardization processes made by US Federal Communications Communication (FCC) through the allocation of 75 MHz of dedicated short range communication (DSRC) spectrum basically to accommodate V2V and V2I communications for safety-related applications [26]. In this paper we present the new modified MAC layer protocol for the vehicular ad-hoc network and improve the results for the vehicular ad-hoc network.**

***Keywords* – Vehicular Ad-hoc Network, Data Link Layer, V2V, IEEE.**

I. INTRODUCTION

During the last few years we have all witnessed steadily increasing growth in the deployment of wireless and mobile communication networks [1]. Mobile ad-hoc network is basically collection of mobile nodes and further is divided into some class such as wireless sensor networks, wireless mesh networks, vehicle ad-hoc network etc. there are various routing techniques are used to send the packets information from the source to destination. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic [5].

MANETs are also capable of handling topology changes and malfunctions in nodes through network reconfigurati--ons. Examples include on-the-fly conferencing applications, networking intelligent devices or sensors etc. Interest in such dynamic wireless networks is not new. It dates back to the seventies, when the U.S. Defense Research Agency, DARPA worked on PRNET and SURAN projects. They supported automatic route set up and maintenance in a packet radio network with moderate mobility. Interest in such networks has recently grown due to the common availability of wireless communication devices that can connect laptops and palmtops and operate in license free radio frequency bands (such as the Industrial-Scientific- Military or ISM band in the U.S.). In an interest to run internetworking protocols on ad hoc networks, a new working group for Mobile, Ad hoc Networking (MANET) has been formed within the Internet Engineering Task Force (IETF), whose charter includes developing a framework for running IP based protocols in ad-hoc networks. Interest has also been partly fueled by the recent IEEE standard 802.11 that include the MAC and physical layer specifications for wireless LANs without any fixed infrastructure.

Routing protocols in packet-switched networks traditio--nally use either link-state or distance-vector routing algorithm. Both algorithms allow a host to find the next hop neighbor to reach the destination via the "shortest path." The shortest path is usually in terms of the number of hops; however, other suitable cost measures such as link utilization or queuing delay can also be used. Such shortest path protocols have been successfully used in many dynamic packet switched networks.

Most wireless sensor networks (WSNs) are composed of cheap battery-powered devices that are able to sense their environment and to communicate with each other in a wireless manner. Their low-cost and energetic autonomy has enabled environmental monitoring applications to emerge in the recent years. For instance, WSNs have been used for wildlife tracking and monitoring. In order to last for years with the current technology, it is crucial to save nodes energy in a WSN. As the radio module of a sensor node generally needs several times more energy than its processor, many researchers have focused on implement--ing energy-efficient communication protocols, where sensor nodes go to sleep mode periodically [5].

The rest of this paper is organized as follows in the first section we describe an introduction of about the Smart grid and their applications. In section II we discuss about the security services in vanet. In section III we discuss about the experimental result analysis and the comparative study between existing method and proposed methods and their simulation study, finally in section IV we conclude the about our paper which is based on the experimental result study.

II. SECURITY SERVICES OF VANET

- *Authentication:*

The sender of the messages must be authenticated. Nodes should react to the information received from the legitimate users only. As an unauthorized node may transmit false information and mislead others. Therefore we need to authenticate the senders of these messages. . It is a challenging task within the vehicular network to ensure authentication because of unattended nature of the network and wireless nature of the transmission media.

- *Integrity:*

The correctness and timely receipt of information is a major vulnerability. This service deals with the consistency of a stream of messages throughout communication. In the vehicular network, data Integrity is needed to ascertain the reliability of the data. It assures that messages are received as sent without insertion, modification, replays or reordering [7]. As a vehicle can act malicious and tamper the information sent, though it may be a legitimate user [10].

➢ *Non-repudiation:*

Non-repudiation service refers that either sender or receiver cannot deny the transmission of a message. It is possible that a node may transmit false traffic alerts, however later it refuses that the messages were sent by it [14]. This service may be crucial for investigation to determine the correct sequence and content of messages exchanged before the accident [19] [27].

➢ *Confidentiality:*

This service ensures that the classified information in the network can never be disclosed to the illegitimate users. Confidentiality protects the privacy of the confidential communication content like name, location, plate number etc. It guarantees the privacy of drivers against unauthorized observers [17]. Pseudonyms techni--que is used in order to preserve the privacy of the drivers in VANETs.

➢ *Availability:*

There can be attacks that can lead to loss or reduction in the availability of VANET services such as bandwidth and connectivity. Even a robust communication channel can still suffer some attacks (such as denial of service) which can bring down the network [7]. Therefore, availability of VANETs resources should be also supported by alternative means [27] so that's communication is not hampered.

➢ *Access Control:*

In VANET, it is essential to define the access privileges for different users. The authorized party needs to define the network policies for the vehicles to access the network [12]. This will help to control the access of different users to various services provided by the VANETs. Access control can be implemented through communication channels, to limit a user's access other vehicles, applications and RSUs.

III. Experimental Result Analysis

In this section we presents the experimental result analysis and their comparative study with the existing approach and research paper, all the experimental results are simulated with the network simulator ns 2.34.

This chapter provides an overview of network simulation and different VANET simulators that can be used to simulate different VANET algorithms to analyze the performance of the network without the need of real systems. This not only saves cost but also provides opportunity to test new protocols and algorithms in a controlled environment which otherwise would have not been possible.

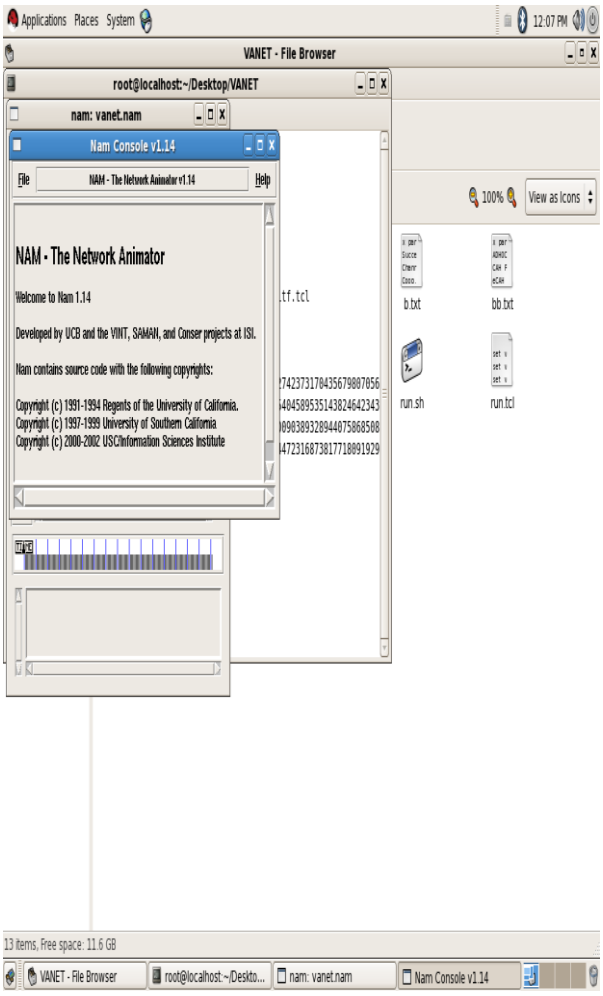

Fig. 2. This figure show that the terminal window for the network animator.

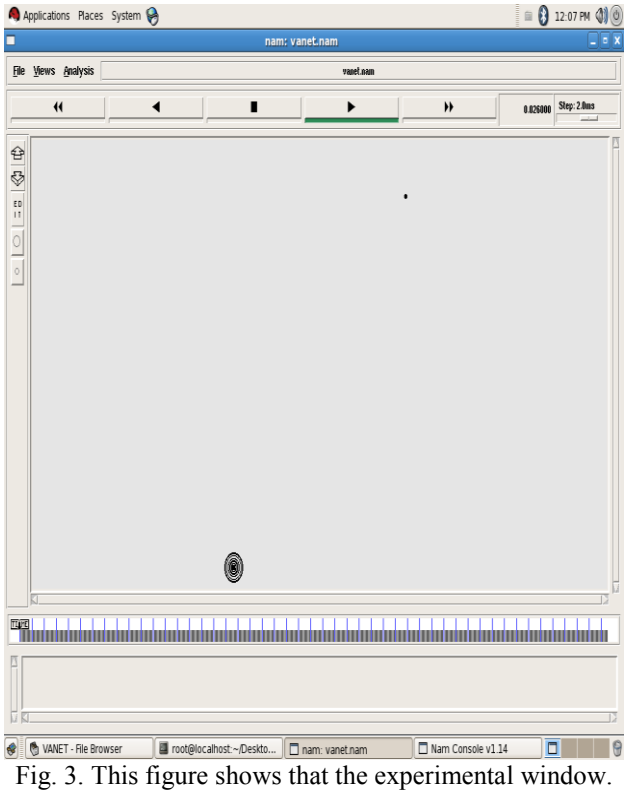

Fig. 3. This figure shows that the experimental window.

IV. CONCLUSIONS

The time-based scheme is another approach to control the media access. In this approach, the time is divided into frames, which are divided into time slots. This approach is called Time Division Multiple Access (TDMA). The TDMA mechanism is a contention free method that relies on a slotted frame structure that allows high communication reliability, avoids the hidden terminal problem, and ensures, with high probability, the QoS of real-time applications. In this paper we improve the quality of services parameters for the vehicular ad-hoc network using dedicated short range communication protocol.

REFERENCES

[1] Mengying Ren, Jun Zhang, Lyes Khoukhi, Houda Labiod, and Veronique Veque, "A Unified Framework of Clustering Approach in Vehicular Ad Hoc Networks", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, 2017. Pp 1-14.

[2] Elias C. Eze, Sijing Zhang, Enjie Liu, Joy C. Eze, "Advances in Vehicular Ad-Hoc Networks (VANETs): Challenges and Road-map for Future Development", IEEE 2016. Pp 1-17.

[3] Elias C. Eze, Sijing Zhang and Enjie Liu, "Vehicular Ad Hoc Networks (VANETs): Current State, Challenges, Potentials and Way Forward", Proceedings of the 20th International Conference on Automation & Computing, Cranfield University, Bedfordshire, UK, 12-13 September 2014. Pp 1-7.

[4] Marthinus J. Booysen, Sherali Zeadally, Gert-Jan van Rooyen, "A Survey of Media Access Control (MAC) Protocols for Vehicular Ad-hoc NET works (VANETs)", IEEE 2012. Pp 1-26.

[5] Hao Ye, Le Liang, and Geoffrey Ye Li, Joon Beom Kim, Lu Lu, and May Wu, "Machine Learning for Vehicular Networks", 2018. Pp 1-16.

[6] Linghe Kong, Bowen Wang, Xi Chen, Xue Liu, Xiao-Yang Liu, Jiadi Yu, Guangtao Xue, Guihai Chen, " Joint adaptation framework in mobile ad hoc networks: A control theory perspective", Elsevier ltd. 2017. Pp 66-74.

[7] Mohamed Hadded, Paul Muhlethaler, Anis Laouiti, Rachid Zagrouba, Leila Azouz Saidane, "TDMA-based MAC Protocols for Vehicular Ad Hoc Networks A Survey, Qualitative Analysis and Open Research Issues", IEEE COMMUNICATION SURVEYS AND TUTORIALS , VOL. , NO. , FEBRUARY 2015. Pp 1-36.

[8] Xiaomin Ma, Jinsong Zhang, Xiaoyan Yin, and Kishor S. Trivedi, "Design and Analysis of a Robust Broadcast Scheme for VANET Safety-Related Services", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 1, JANUARY 2012, Pp 46-62.

[9] Imad Jawhar, Nader Mohamed, and Liren Zhang, "Inter-Vehicular Communication Systems, Protocols and Middleware", Fifth IEEE International Conference on Networking, Architecture, and Storage, IEEE 2010. Pp 282-287.

[10] Antonio Fonseca, Teresa Vazao, "Applicability of position-based routing for VANET in highways and urban environment", Preprint submitted to Network and Computer Application, 2011. Pp 1-15.

[11] Mildred M. Caballeros Morales, Choong Seon Hong, Young-Cheol Bang, "An Adaptable Mobility-Aware Clustering Algorithm in Vehicular Networks", IEEE 2011. Pp 1-6.

[12] Kaan Bur, Maria Kihl, "Evaluation of Selective Broadcast Algorithms for Safety Applications in Vehicular Ad Hoc Networks", Hindawi Publishing Corporation International Journal of Vehicular Technology, 2011. Pp 1-14.

[13] Sławomir Kuklinski, Adrian Matei, Grzegorz Wolny, "NGVN: A Framework for Next Generation Vehicular Networks", IEEE, 2010. Pp 297-301.

[14] Sailesh Bharati, Weihua Zhuang, Lakshmi V. Thanayankizil, Fan Bai," Link-Layer Cooperation Based on Distributed TDMA MAC for Vehicular Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 66, NO. 7, JULY 2017, pp 6415-6427.

[15] Mustafa Bani Khalaf, Ahmed Y.Al-Dubai and William Buchanan "A New Adaptive Broadcasting Approach for Mobile Ad hoc Networks", 978-1-4244-7071-6/10, 2010 IEEE.

[16] Zhimu Huang, Ryo Yamamoto, Yoshiaki Tanaka, "A Multipath Energy-Efficient Probability Routing Protocol in Ad Hoc Networks" Feb 16-19 ICATE2014.

[17] Akshay Aggarwal, Savita Gandhi, Nirbhay Chaubey, Keyurbhai A Jani "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs", 2014 Fourth International Conference on Advanced Computing & Communication Technologies

[18] Aarfa Khan Prof. Shweta Shrivastava, Prof. Vineet Richariya, "Normalized Worm-hole Local Intrusion Detection Algorithm (NWLIDA)" 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA.

[19] Jyoti Joshi, Vidhate Amarsinh, "Enhanced 2ACK Scheme to Prevent Routing Misbehavior Using OLSR Protocol." 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA.

[20] Seema Verma Pinki Nayak and Rekha Agarwal" Energy Efficient Routing in Mobile Adhoc Networks based on AODV Protocol " in IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 2, November 2012.

[21] Benjie Chen, Kyle Jamieson, Hari Balakrishnan, and Robert Morris. Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks. In Mobile Computing and Networking, 20012.

[22] Zhengming Li and Chunxiao Chigan" AWF-NA: A Complete Solution for Tampered Packet Detection in VANETs" in IEEE conference 2009.

[23] Soufiene Djahel, Farid Na¨ıt-abdesselam, and Zonghua Zhang "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges" in IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 13, NO. 4, FOURTH QUARTER 2011.

[24] Lei Huang and Lixiang Liu" Extended Watchdog Mechanism for Wireless Sensor Networks" in Journal of Information and Computing Science in Vol.3, No. 1, 2008.

[25] Satoshi Kurosawa and Hidehisa Nakayama" Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" in International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[26] Eze, Elias C., Sijing Zhang, and Enjie Liu. "Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward", 2014 20th International Conference on Automation and Computing, 2014.

[27] Wang, N.W, Yueh-MinHuang, Wei-MingChen "A novel secure communication scheme in vehicular ad hoc networks", Computer Communications, 20080730.