

Dynamic Environment Improvement for Vanets

Ratan Deep Singh*, Pankaj Gugnani

CSE, ITM University Gwalior, Madhya Pradesh, India

ABSTRACT

Article Info

Volume 7, Issue 2

Page Number: 79-82

Publication Issue :

March-April-2021

Article History

Accepted : 20 March 2021

Published : 25 March 2021

Vehicular Ad-Hoc Network (VANET) are dynamic network because no fixed topology available in this environment, in this paper we try to check VANET environment and studied how we create the message with the help of simulator and send message source to destination simulator used dedicated short range protocol (DSRC) for communication. We check the efficiency of the environment and collect the data for improvement of the network.

Keywords : VANET, RSU, V2V, I2V and DSRC.

I. INTRODUCTION

Now a day Transport is very essential area to research. For developing smart city, we need better transport system. If we want to establish better transportation system we use VANET (Vehicular Ad-hoc network) is a good area, with the helping of VANET we developed good communication network.

Traffic congestions, road accidents and maintenance, square measure the foremost necessary problems with current traffic systems, inside those drivers need to be wholly alert to the surrounding surroundings. Conveyance unexpected networks (VANET) area unit a class of ad- hoc networks. In VANETs, there square measure 2 styles of communication [1]: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) to boot mentioned as vehicle to wayside unit (V2R). In V2V communication vehicles mail and

accept communication to and from one another. These messages could also be coverage road congestion, accidents ahead, etc., mentioned as safety messages.

II. RELATED WORK

In this paper[1] Current routing protocols used in Vehicular Ad hoc Networks(VANET) such as OLSR [1], In paper[2] Ad hoc On Demand Distance Vector (AODV).and paper[3] Dynamic Source Routing(DSR) are designed without considering security. Hence, they are susceptible to a wide range of attacks and misbehaviours. Amongst the network security attributes, authentication is particularly important for ad hoc networks due to their cooperative nature. Restricting unauthorized node access to the network is not sent, as legitimate nodes may behave abnormally when compromised or hijacked (e.g. if the secret keys necessary to generate legitimate messages are captured by an attacker). Therefore, the issue to determine could be not only "is the message's originator authentic?" but also "is the message

authentic?" A number of trust establishment mechanisms have been proposed as extensions of Mobile Ad Hoc Network (MANET) routing protocols or as stand-alone secure routing protocols. Schemes proposed for distributed authenticated routing [4], [5] and trust-group-based authentication service [6] use distributed authentication authorities and distributed trusted groups to assist the authentication process. However, these proposals do not authentication introduces high delay. Some secure routing protocols or protocol extensions provide message authentication using different digital signature schemes, such as OLSR extensions proposed in [7], [8], SAODV [9], Secure Link State Protocol (SLSP) [10] and the secure on-demand routing protocol Ariadne [11].

Securing control messages using digital signatures enables the receiver to verify sender's identity and message integrity, but it cannot prevent a compromised node from tampering with the network. The advanced signature system for OLSR proposed in [12] uses link atomic information of surrounding nodes to prevent link spoofing. However it is based on the assumption that all intermediate nodes are authentic, which is not always the case. In this paper we focus on designing a distributed trusted routing framework that achieves authentication of messages, nodes and routes. Our main contributions are in enabling verification of routes, rather than just securing routing protocol messages or authenticating individual nodes (which is conceptually similar to [12]) and in proposing a new framework for trusted routing. The architecture is distributed and uses limited assistance from a Certificate Authority (CA) which may only be used for initial distribution of keys and certificates, or for infrequent certificate updates. As an example, we have applied the framework to OLSR, evaluated the performance, and overhead introduced by the trust related extensions. We note that the generic mechanism is also

applicable to several other VANET routing protocols. Various studies have established the fact that the number of lives lost in motor vehicle crashes worldwide every year is by far the highest among all the categories of accidental deaths [1].

III. PROBLEM FORMULATION

Vehicular Ad-hoc Network it is a type of dynamic network. That means no fix Topology available for Vehicular Ad-Hoc Network. In Vehicular Ad-hoc Network, time is very important factor. Time factor is very crucial factor in this type communication. Therefore, we need to develop good framework to reduce the communication delay.

IV. PROPOSED METHODOLOGY

We proposed a framework to improve communication in terms of time. The proposed methodologies has taken minimize delay and able to provides a better network for information transmission. In this paper we work on the real scenario we design the road condition and vehicle scenario and put the simulator active vehicles, speed, travel distance , travel time , wireless vehicles, known vehicle, created unique messages and failed forwarded message after find out the throughput and packet delay for betterment for vehicle environment.

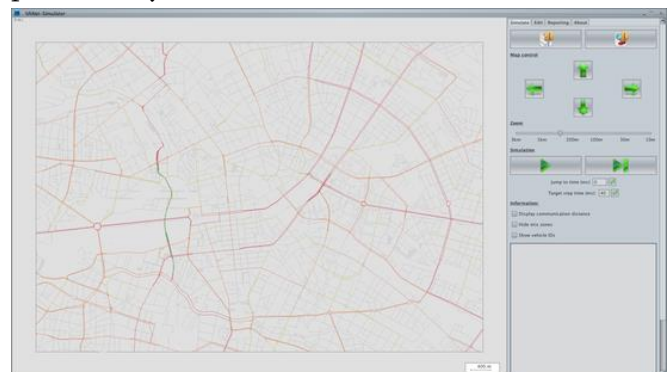


Figure 1: road scenario and road map

VI. REFERENCES

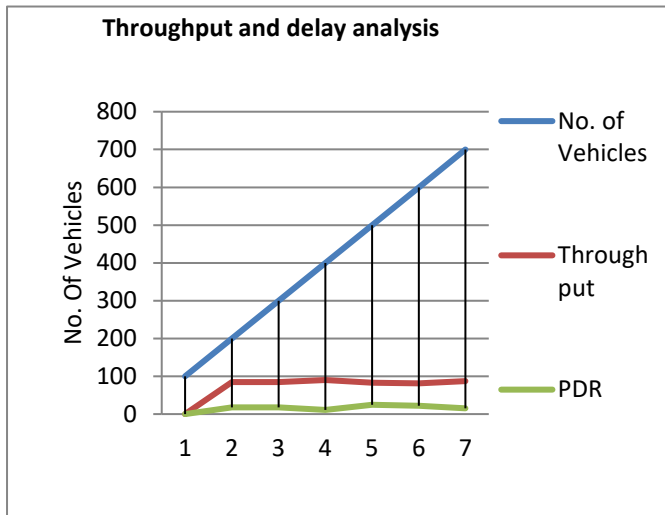


Figure 2 : Throughput and packet delay analysis

In figure 2 we see that the throughput and packet delivery analysis to calculate the behaviour of VANET environment and after analysis we improve the VANET environment to speed up the transfer information one vehicle to another vehicle and reduce the death rate cause of vehicles.

V. CONCLUSION

In this paper we see that if improve throughput and decrease the packet delay in VANET environment. So we capable to decrease the death rate due to poor information exchange in real time so we work on this direction in this paper with some simulation result. Simulation result shows the failed messages out of total numbers of created messages. In this paper, we find out the overall throughput and packet delay ratio to improve the network topology. In future we try to apply some other algorithm to improve VANET scenario.

- [1]. <http://www.car-accidents.com/pages/fatal-accident-statistics.html>
- [2]. Md Mahbubul Haque, Jelena Mistic, Vojislav Mistic, Subir Biswas, and Saeed Rashwand "Vehicular Network Security," Encyclopedia of Wireless and Mobile Communications
- [3]. P. Papadimitratos, L. Buttyan, T. Holczer, et al., "Secure vehicular communication systems: design and architecture," IEEE Communications Magazine, vol. 46, no. 11, pp. 100–109, 2008.
- [4]. "Vehicle infrastructure integration." [Online]. Available: http://www.its.dot.gov/vii/docs/vii_factsheet.pdf
- [5]. J. Guo and N. Balon, "Vehicular ad hoc networks and dedicated short-range communication," Book Chapter, 2006.
- [6]. Philipp Wex, Jochen Breuer, Albert Held, Tim Leinmüller and Luca Delgrossi "Trust Issues for Vehicular Ad Hoc Networks" 2008 IEEE
- [7]. Anup Dhamgaye, 2Nekita Chavhan "Survey on security challenges in VANET" IJCSN International Journal of Computer Science and Network, Vol 2, Issue 1, 2013.
- [8]. A. Boukerche and Y. Ren, "A trust-based security system for ubiquitous and pervasive computing environments," In Computer Communications, Vol. 31, No. 18, pp. 4343-4351.
- [9]. M. Gerlach, "Trust for vehicular applications," In Proceedings of the International Symposium on Autonomous Decentralized Systems, pp. 295-304, 2007.
- [10]. U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad-hoc networks," In International Journal of Computational Intelligence Theory and Practice (IJCITP), Vol. 5, No. 1, 2010.

- [11]. J. P. Keener, "The Perron-Frobenius Theorem and Ranking of Football Teams," SIAM Review, Vol. 35, No. 1, pp. 80-93, 1993.
- [12]. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET," In Proceedings of VANET, pp. 89–98, 2009.

Cite this article as :

Ratan Deep Singh, Pankaj Gugnani, "Dynamic Environment Improvement for Vanets", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 2, pp. 79-82, March-April 2021. Available at doi : <https://doi.org/10.32628/CSEIT217216>
Journal URL : <https://ijsrcseit.com/CSEIT217216>