International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

Road Condition Monitoring with Source Authentication in VANET

Vijayakumar.V, Praveen Benjamine.S, Karthikeyan.M, Ragul Kumar.M, Ram Kishore.A

Abstract: ***In recent technologies, it has been said that, to improve the travel efficiency and safety of transportation systems, vehicular ad-hoc network (VANET) has been used as the promising technology where each vehicle is able to collect and communicate the information about current road or traffic condition at a particular location using an embedded on-board unit with the help of distributed roadside units. Examples are: While detection of some accident, congestion, jam, etc., vehicles broadcast warning signals to the nearby vehicles which would give a better awareness to every nearby vehicles about the driving environment and these nearby vehicles would change the driving plan if needed. The VANET technology has gained great attentions from both industry and academics in the recent days.***

Keywords **: *Dynamic topology, Roadside units, Sub authority, Trusted authority, VANET.***

I. INTRODUCTION

The Vehicular Ad-hoc Network is based on the principle of Mobile Ad-hoc Network (MANET). In 2001, VANET has been introduced and evolved in which it lead to the ability of connecting and communicating with other vehicles thus forming a car to car ad-hoc mobile network. The road safety and other navigation related services has been provided by V2V and V2R communication. Vehicular ad-hoc network plays a major important role in intelligence transport system (ITS). At last in 2015, the VANET come to use in inter-vehicle communication (IVC), but the aspect of spontaneous networking was mainly focused and the infrastructures such as Road Side Units (RSUs), legal authorities and cellular networks are less concentrated. The mobile network has been formed in MANET where the cars involved in the networks acts as a mobile node. The public safety is ensured by VANET by determining the driver's activity in the car.

II. VANET ARCHITECTURE

A. Vehicle to Vehicle communication (V2V):

In V2V communication, the information is exchanged between various vehicles so that they can know about the warnings and critical information such as traffic alerts, avoiding collisions etc. Since VANET is dynamic topology the infrastructure is not stable and it can only exchange information only if there is a presence of vehicles around it [3].

B. Vehicle to Road Infrastructure (V2I) communication:

This type of communication is done between the vehicles which is participating in the network and the infrastructure present in the road side. The information mainly carried out in this communication are real time traffic and weather updates by the sensors [1].

C. Vehicle to Broadband cloud (V2B) communication:

The V2B communication is made over broadband connectivity by either 4G/5G connections which is established by e-SIM in the vehicles [1]. This communication helps in assisting the driver over navigation and traffic updates based on the information stored in the cloud.

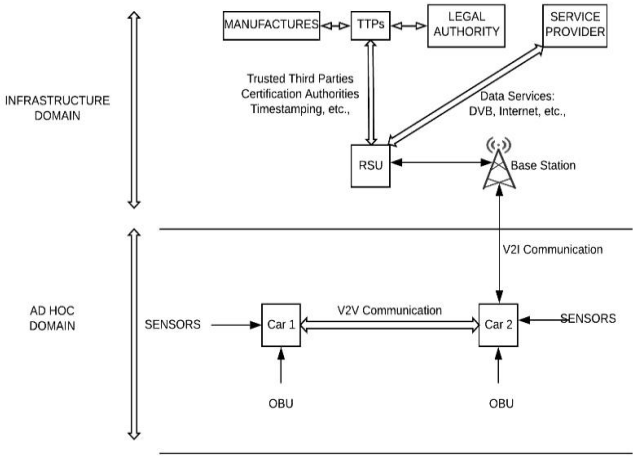

Fig 1. Vehicular Ad-hoc Network [2]

Revised Manuscript Received on April 18, 2020.
* Correspondence Author
Dr.Vijayakumar.V*, Assistant Professor, Department of Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India. vijayakumarv@smvec.ac.in
Praveen Benjamine.S, Department of Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India. benjaminepraveen@gmail.com
Karthikeyan.M, Department of Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India. karthikeyanvijay066@gmail.com
Ragul Kumar.M, Department of Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India. ragulkumar5898@gmail.com
Ram Kishore.A, Department of Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India ramkishore771998@gmail.com

III. LITERATURE SURVEY

PAPER TITLE	AUTHOR	PAPER DESCRIPTION
Enhancing VANET connectivity through roadside units on highways	S. Ian and O. Tonguz	For safety measures, if a vehicle is under an accident it should send an emergency broadcast signals to the nearby RSUs as fast as possible even when there is sparse availability of RSU present in that area [8].
A Fuzzy multi-metric QOS-balancing gateway selection algorithm in a clustered VANET to LTE advanced hybrid cellular network	G. Zhioua, N. Tabbane, H. Labiod, and S. Tabbane	It proposes that in order to improve the QoS rather than focusing in safety related issues by providing high fidelity LTE network infrastructure. The algorithm of the proposed paper states that using fuzzy logic to make a gateway selection in clustered VANET [9].
Survey on various mechanisms for secure and efficient VANET communication	V. Vijayalakshmi, M. Sathya, S. Saranya and C. Selvaroopini	VANET is derived from the application of MANET which as the ability to enhance road safety. VANET is emerging to create an interest in wireless and mobile communications fields [4].
Privacy-preserving authentication framework using bloom filter for secure vehicular communications	A. Malhi and S. Batra	If a message received by the infrastructure network it may or not contain malicious content. In order to safe guard the network from these activity, use of pseudonym make anonymous communication. A digital signature based scheme is used [6].

IV. EXISTING SYSTEM

The main issue is that the location privacy of a vehicle has been a questionable problem when the data is received from a authenticated vehicle. The existing system imposes that the pseudonym can be renewed automatically whenever possible without the help of any trusted authority.

This authentication problem can be a root vulnerability for many attackers to make an anonymous communication in the network. The user's information can be easily seen by any attacker without any leaving his/her trace with the help of this anonymous pseudonym communication. Also, the information send from the user vehicle are not monitored and compared with the genuine information obtained from the trusted vehicle.

Issues in the system:

- Data integrity
- Authentication is not satisfactory.
- Privacy of vehicle is questionable.

V. PROPOSED SYSTEM

Here we propose our contribution over privacy preserving Road condition with the help of source authentication to ensure stay away from the malicious attackers. Some of the functionalities provided by the proposed system are as follows:

A. Reporting in an authorised manner:

The real time report of a road condition can be obtained from a vehicle. The collected report must be encrypted. The encrypted details being done by the trusted authority by its public key [2]. Before uploading the encrypted data to the cloud server, the secret key and token must be issued by the nearby roadside units (RSUs). In case, any vehicle needs to generate a road condition report a valid token is a must. Without a valid token, a vehicle cannot be able to send the data to the roadside units.

B. Monitoring the privacy of vehicles:

The monitoring of the road condition reports will be carried out by the cloud server. The reports coming from the same road domain are grouped into equivalent classes or sections in the cloud server. Those are in the same equivalence class and contains same road condition information. The report received from a new vehicle will be compared with the road condition reports present in its location equivalent classes. For this purpose, only one road condition report must be compared with the new report. The report to which new report should be compared must be in the equivalent classes. After comparison of reports if its true then the component new report will gets inserted or placed in that equivalent class. The decryption will be carried out by the trusted authority [7].

C. Source authentication:

As per the advanced implementation of [12], the complicated cryptography certificates are not used by the Road condition monitoring. Constructing the secret key is received from the sub authority by the vehicle or RU. The received key will be validated using the report trusted sub authority. The report generated from an authorised vehicle will be checked or found by the cloud server. The report generated by the claimed RU must generate by valid token. This process will be carried out by the trusted authority

D. Advantages*:*

- Improve source authentication
- Data integrity.
- Increased privacy protection.

VI. ARCHITECTURE OF PROPOSED SYSTEM

The system architecture in Fig 2 depicts that the vehicles acts as a node in the network which is considered as Ad-hoc domain where the network is scalable and creates a dynamic topology. Whereas, the infrastructure consists of various number of Roadside Units (RSUs), Sub authorities (SAs), one Routing Authority (RA) for a particular city or region which is being monitored by a cloud service provider which can be able to store reports and do computations. The Vehicle to Vehicle (V2V) communication will be established using the strategic algorithms like Dijikstra's shortest path, Ant colony optimization, Bellman ford's algorithm, Floyd War algorithm can be used for finding its neighbor vehicle node and broadcasting routing protocol is used for emergency situations. The Vehicle to Infrastructure (V2I) communication can be established by using either IEEE 802.11a of speed 54 Mbps maximum and at usual speed of between 6 to 24 Mbps at frequency of 5 Ghz (or) using LTE (4G) WiMax 4G stations can be used. No vehicle nodes are given authorized permission to directly communicate with the RA, the vehicle nodes can able to communicate with the RA with the help of only RSUs.

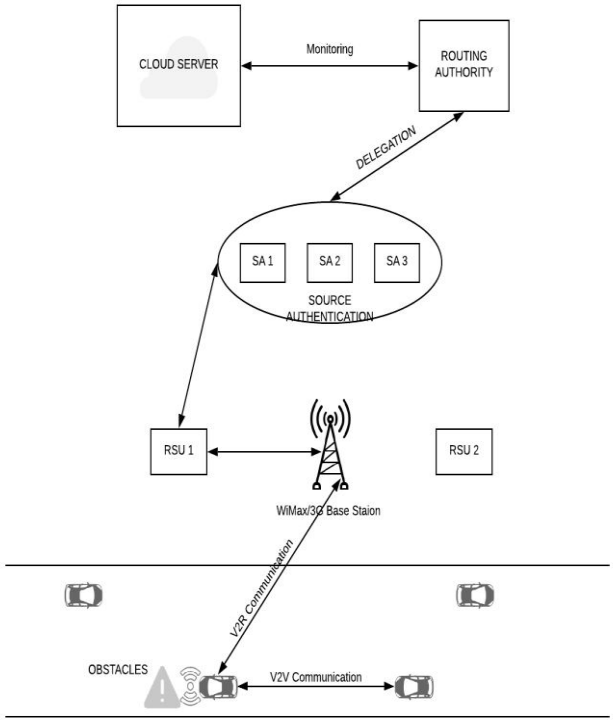

Fig 2. Architecture of Proposed System

VII. IMPLEMENTATION OVERVIEW

A. Node Definition:

In Node Definition, the nodes are defined using the set keyword which is associated with respective simulator name "ns" where its coordinates defined using x, y, z coordinates as necessary. There are about 11 nodes created for road structure starting from node 0 to node 11, 15 nodes for vehicle starting from node 12 to node 27, 7 nodes for creating RSUs from node 28 to node 34 and 1 node for RSU node 35.

B. Road Structure:

In the Road Structure module, the vehicle nodes are allowed to pass through at a speed of 1MB in a timestamp of 10ms interval. The color of vehicle nodes are changed to red color when the node is sending data either to RSU or other vehicle node. The shape of RSU will be changed to Maroon Square when it exchanges data.

C. Node Movement:

In the Node Movement module, since the network is dynamic in nature as vehicle nodes are moving at a particular speed of 10ms constantly from source location to destination location. The source and destination location are defined like "$n(12) setdest 822.0 727.0 $speed".

D. Neighbor Discovery:

In Neighbor discovery module, a FOR loop has been used so that each vehicle node will be kept on loop to identify the neighbor vehicle node which is nearer at a point less than of 500 from its position x and y axis coordinates. And also when a node is discovered it will display a message using the code puts"The neighbor for node $i are:$nb1".

E. Initializing Root Authority (RA):

The Initializing Root Authority (RA) module is the most important module where it contains the most computation process. In this module, ECC.tcl, sha1 (Secure Hashing Function 1), AES (Advanced Encryption System) packages are used. And also the vehicle registration process is done.

F. Mutual Authentication:

In this module, a vehicle node requests for authentication request from neighboring node with the node information like node number, registered are not by returning 0 &1 from RA and Encrypted message.

G. Broadcasting Emergency Message:

The Broadcasting emergency module, is used to send a emergency message to all the nodes immediately and continuously for a particular time and then it stops sending emergency broadcast.

H. Event Recording:

Here, all the events such as packet delivery ratio, packet loss rate, authentication delay, revocation delay are recorded in form of graph using the XGraph plotting.

VIII. RESULT ANALYSIS

The performance analysis is a process of finding out the real time efficiency of a process or a project which can be able to show its maximum or minimum performance level. This analysis is the performance of a simulation which has been recorded while the event program has once started.

The performance analysis of the proposed system has been classified into four categories:

- Packet Delivery rate
- Packet Loss rate
- Authentication Delay
- Revocation Delay

A. Packet Delivery Rate:

The Packet Delivery rate analysis in network simulator is shown in Fig. 3 is used to show how many data packets has been delivered in a particular timestamp has been duly recorded. In the below graph, 20 nodes has been delivered 7 data packets, from 40 to 100 nodes the delivery rate is 14 which is constant and at the 160 nodes the delivery of data packets has been increased to 26 packets of data.

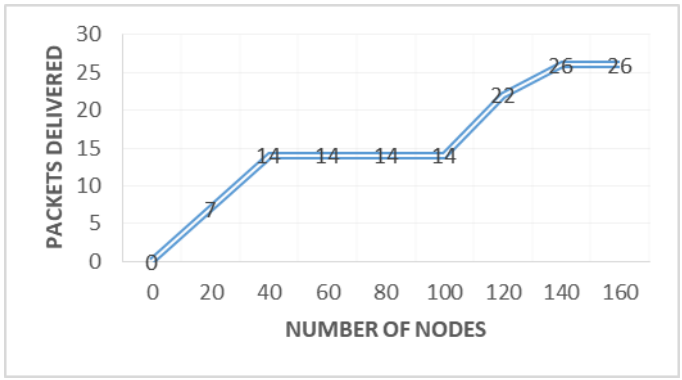

Fig 3. Packet Delivery Rate

B. Packet Loss Rate:

The Packet loss rate analysis in network simulator is shown in Fig.4 is used to show how many data packets has been lost during the data exchange between one node to another while communication. Upto the 62 nodes there has been loss of 5 data packets and rapidly loss of data packets has been increased to 28. The packet loss has been reduced to 3 from 70 to 85 nodes. Again, the loss has raised to 17 at 100th node.

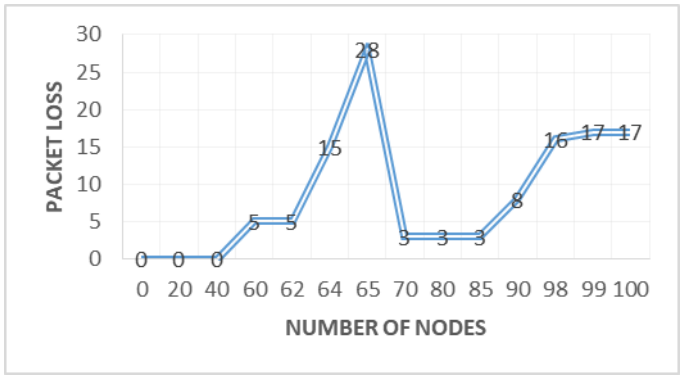

Fig 4. Packet Loss Rate

C. Authentication Delay:

The Authentication delay analysis shown in Fig. 5 means to show how much time a node takes to receive a authentication response from its destination node in order to begin its next process in sending reports thereafter to that node. The authentication delay may rise when the other nodes tries to get a authentication response from the one source node. In fig. 5 the delay has been constantly increasing from 60 ms at 60th node to 94 ms at 100th node. The delay occurred is minimal and hence the efficiency of the system is achieved.

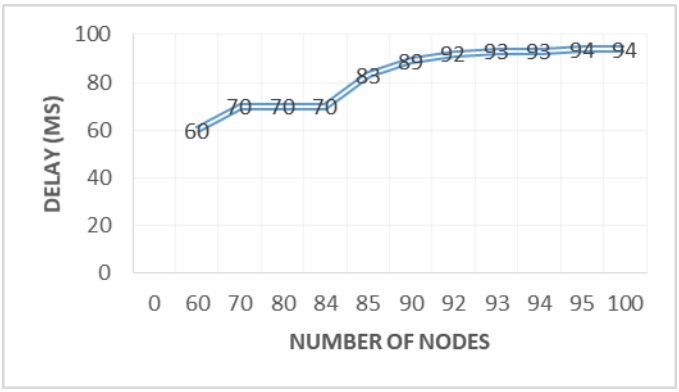

Fig 5. Authentication Delay

D. Revocation Delay:

The Revocation delay analysis in Fig. 6 shows that how much time it takes for a particular node in VANET needs to identify that a node has been registered or not with the Rooting Authority (RA) since the unregistered vehicles are not allowed for participating in the network.

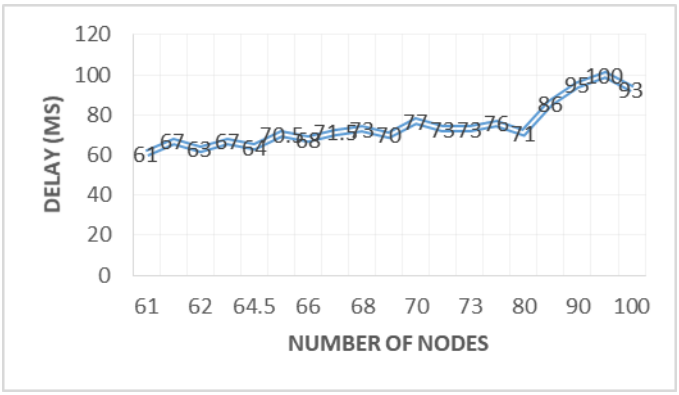

Fig 6. Revocation Delay

IX. NETWORK SIMULATOR

The Network simulator is an application software which is used to simulate the network instead of working it in the real time. The success of simulation is got only after tracing the output value. Usually they are GUI to interact with the user and some simulators require scripts to simulate the network. Some of the Network simulators are as follows:

A. NS-2 :

NS-2 refers to Network Simulator Version 2. A discrete and on open source platform which provides simulation functions for both wired and wireless protocols. The protocols it includes such as TCP, UDP, etc. The properties and characteristics of the simulated network can be analyzed by extracting a text-based data and then it can be presented in any ways. NS was written in both C++ and OTcl1 interpreter as a command and configuration interface [10].With help of Network Simulator 2 (NS2) we can simulate the following:

- Topology: Wired, Wireless.
- Scheduling Algorithms: RED, DropTail.
- Transport Protocols: TCP, UDP.
- Routing: Static and Dynamic routing.

- Application: FTP, HTTP, TelNet, Traffic generators.

Features:

- It supports traffic distribution modelling
- Protocols such as HTTP, TCP, UDP, SRM, RTP can be simulated [10].

X. APPLICATIONS

The main applications of VANET in which our proposed system is mainly focused on traffic service, warning messages which helps in enhancing the transportation management. Some of the applications VANET are:

A. Safety Oriented Applications:

There are many difficulties occurs during driving of the vehicles such as accidents, collisions of the vehicles. To overcome this VANET plays an important role in this by sending warning messages to the neighboring vehicles. Three major applications are explained as:

- **Collision avoidance**: If an accident occur in one place and traffic is generated in that place. Then the other vehicles which are going towards that place can be diverted via multi hop. The vehicle speed and other measures are transferred through this.
- **Cooperative driving**: Speed-hike, sharp turn, speed breakers are the information which are called as the critical information [11]. These critical information are transferred from one vehicle to the another vehicle by the use of the VANET. When the VANET devices failed to transfer these information then vehicle safety is reduced. The drivers cannot be able to drive without a fear.

B. Infotainment applications:

The Infotainment applications like surfing websites, downloading maps, etc. comes under this application [11].

- **Cooperative applications:** Information provided the local nearby nodes such as interest notification, media downloading etc.

XI. CONCLUSION

Therefore, in this paper that is in road condition monitoring system with source authentication in VANET has been proposed over the existing system which has many security issues over such as privacy of user's information, vehicle information, infringement of malicious data are somehow prevented in this proposed system. And also, in existing system there are no such things of source authentication been there. The Root Authority (RA) performs most of the computations from monitoring the data report to rerouting the traffic in case of any emergency situations. In order to protect data from attacker the road condition report is been encrypted with hash function holding information like vehicle id, encrypted data (Road condition report), and signed certificate provided by the Root Authority (RA). By implementing all the factors mentioned above we can secure and preserve user's privacy in VANET.

REFERENCES

1. B. Ayyappan and P. M. Kumar, "Vehicular Ad Hoc Networks (VANET): Architectures, methodologies and design issues," 2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM), Chennai, 2016, pp. 177-180.
2. Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin and H. Wang, "Privacy-Preserving Cloud-Based Road Condition Monitoring With Source Authentication in VANETs," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 7, pp. 1779-1790, July 2019.
3. H. Noori and B. B. Olyaei, "A novel study on beaconing for VANET-based vehicle to vehicle communication: Probability of beacon delivery in realistic large-scale urban area using 802.11p," 2013 International Conference on Smart Communications in Network Technologies (SaCoNeT), Paris, 2013, pp. 1-6.
4. V. Vijayalakshmi, M. Sathya, S. Saranya and C. Selvaroopini, "Survey on various mechanisms for secure and efficient VANET communication," International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, 2014, pp. 1-5.
5. I. Jawhar, "A flexible object-oriented design of an event-driven wireless network simulator," 2009 Wireless Telecommunications Symposium, Prague, 2009, pp. 1-7.
6. Malhi, A., & Batra, S. (2015). *Privacy-preserving authentication framework using bloom filter for secure vehicular communications. International Journal of Information Security, 15(4), 433–453.* doi:10.1007/s10207-015-0299-4
7. Qianhong Wu, Domingo-Ferrer, J., & Gonzalez-Nicolas, U. (2010). *Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications. IEEE Transactions on Vehicular Technology, 59(2), 559–573.*
8. Sou, S.-I., & Tonguz, O. K. (2011). *Enhancing VANET Connectivity Through Roadside Units on Highways. IEEE Transactions on Vehicular Technology, 60(8), 3586–3602*
9. Zhioua, G. el mouna, Tabbane, N., Labiod, H., & Tabbane, S. (2015). *A Fuzzy Multi-Metric QoS-Balancing Gateway Selection Algorithm in a Clustered VANET to LTE Advanced Hybrid Cellular Network. IEEE Transactions on Vehicular Technology, 64(2), 804–817.*
10. Mohammed Humayun Kabir, Syful Islam, Md. Javed Hossain, Sazzad Hossain" Detail Comparison of Network Simulators", International Journal of Scientific & Engineering Research, Volume 5, Issue 10, October-2014
11. M. Noussaiba and R. Rahal, "State of the art: VANETs applications and their RFID-based systems," 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT), Barcelona, 2017, pp. 0516-0520.
12. M. Li, N. Ruan, H. Zhu, J. Li and X. Li, "A Paralleling Broadcast Authentication Protocol for Sparse RSUs in Internet of Vehicles," 2014 10th International Conference on Mobile Ad-hoc and Sensor Networks", Maui, HI, 2014, pp. 58-65.

AUTHORS PROFILE

Dr.Vijayakumar.V, Assistant Professor at Sri Manakula Vinayagar Engineering College affiliated to Pondicherry University, received both M.Sc. (CS) and M.Tech (CSE) at Pondicherry Central University, Ph.D at Pondicherry Central University. He has 7+ years of teaching experience in Sri Manakula Vinayagar Engineering College.

Praveen Benjamine.S, currently studying final year B.Tech. Computer Science & Engineering in Sri Manakula Vinayagar Engineering College affiliated to Pondicherry University, Puducherry, India.

Karthikeyan.M, currently studying final year B.Tech. Computer Science & Engineering in Sri Manakula Vinayagar Engineering College affiliated to Pondicherry University, Puducherry, India.

Ragul Kumar. M, currently studying final year B.Tech. Computer Science & Engineering in Sri Manakula Vinayagar Engineering College affiliated to Pondicherry University, Puducherry, India.

Ram Kishore. A, currently studying final year B.Tech. Computer Science & Engineering in Sri Manakula Vinayagar Engineering College affiliated to Pondicherry University, Puducherry, India.