Int. J. Advanced Networking and Applications
Volume: 11 Issue: 04 Pages: 4354-4358(2020) ISSN: 0975-0290

New Identity Batch Verification Privacy Scheme in VANET

Shazia Suthana
Assistant Professor, Department of ECE, Global Academy of Technology, Bengaluru
shazia.sulthana@gat.ac.in
Dr. B N Manjunatha Reddy
Professor, Department of ECE, Global Academy of Technology, Bengaluru, Karnataka, India
manjunatha_reddy@gat.ac.in

ABSTRACT

VANET has exposed improvements in solving traffic congestion; the fundamental idea is to use RSU (Road Side Unit) or another vehicle to send traffic related parameters. The broadcast of traffic information used by safety road applications in wireless channel makes secure data hazardous and testing problem in vanet. Mislead of these messages causes accidents and breakdown of human lives at poorer level and thereby, Privacy in vehicular adhoc network has become a great issue, concerning to drivers convenience. Vehicles have to be barred from these attacks and mishandling of privacy information. For this reason, privacy preserving scheme is major requirement for vehicular adhoc network. The identity batch verification privacy scheme is implemented using ECC algorithm which is considered as more secure and practically efficient.

Keywords: **Adhoc Networks, attack, wireless channel**

Date of Submission: Jan 07, 2020 Date of Acceptance: Mar 07, 2020

I INTRODUCTION

Infrastructure-less network is a system which connects between the vehicle Inter-vehicle communication-IVC) and roadside to vehicle (RVC) communication system. The skill in network multiplexes cellular and AdHoc region to attain the nonstop connection of system. The vehicular system is forward with the fresh task of enhancing protection and simplicity in services to vehiclular nodes. Accident caution, jamming in traffic signal, variation in road-line caution, and path obstruction panic is among the main safety associated services addressed by network. The further set of console services which are nearby, vehicular nodes are connected in the network. AdHoc Networks have developed out of the need to carry the growing quantity of wireless products that can now be used in vehicles.

These wireless nodes contain remote entry devices, personal digital assistants, computer and wireless telephones. As cellular networking devices become more and more considerable, the necessity for vehicular architecture makes Communication will continue to grow. VANETs can be used for a wide variety of protective and non-protective Applications like vehicle security, programmed toll expense traffic supervision, superior routing, fixed system based application, discovery the nearby fuel station, café or journey hotel and wireless applications, provided that access to the Internet. Movement leaning form of traffic allows computing traffic flows, journey times and emissions in big highway networks. In making so, these models resolve the lively traffic task trouble iteratively, which tentatively require modernization of the route of each node in each step. A block diagram (Figure 1 shows Block Diagram of VANET Model) shows the traffic model from generation of a medium, towards its path estimate and the modeling vehicles' movement.

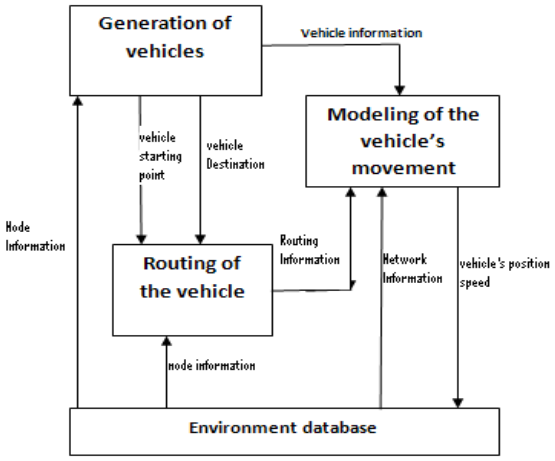

Fig . 1. Vanet Model

The privacy of information swap plays a chief part in today's applications [2]. Assume the communication from on-board is required to identity-verified, checking the honesty previous to it or an enemy can modifies in a row or even take-off other nodes to televise the wrong message [3]. False data perhaps makes most horrible condition. Traffic control centre may provide false traffic data in interpretation an emergency vehicle to necessitate the journey brightness to cooperate with people and break the driving in correct way of other people. To simplify this problem, Identity Batch Verification privacy scheme is demonstrated in this research.

Volume: 11 Issue: 04 Pages: 4354-4358(2020) ISSN: 0975-0290

System Model

In figure 2, the scheme planning contains four sub-modules, i.e., a trusted authority, end servers, Road Side Units along the road segment and on unit fabricated on moving nodes. Trusted Authority and end servers are example for control center of traffic. The Trusted Authority which is applied. Communication occurs through the RSUs through guaranteed channels, such as wired connections through stream controlled protocols. The physical layer is connected with nodes and fixed units. connectivity between the entities is depended on Dedicated Short-range Communications Dedicated Short Range rules .As for every moving network security standard, each medium has its hold public key and private key pairs issued by Trusted Authority. Before information is send, moving nodes need to mark information with confidential method to warranty reliability in data. Safety data or added than traffic related information, every part of road-side or node is accountable for verify their signature of message.

Fig . 2. System Architecture

II RELATED WORKS

Shiang-Feng Tzeng., [1] identified an improved method to gratify the privacy and security required by vehicles. This technique simplifies the measurable safety. Cluster based group verification scheme needs low computation in multiplication techniques, not on the number of messages.

Khaled Rabieh et al., [4] have recommended route reporting privacy schemes for managing the traffic for both fixed architecture depended and organizing by self movable networks. Signifying only pseudonyms and unidentified authentication to cover their individuality of the nodes will not fully safeguard the nodes confidentiality because the informed locations to recognize the nodes.

Libing Wuan et al., [5] have proposed simplied privacy-preserving authentication scheme without the use of complex equations and hardware. Other proposed certification schemes, the designed scheme distinctly reduces the estimation costs of information signing and information certification stage, as satisfies every safety needs of vehiclular networks and provides restricted security.

Raya and Hubaux. [6], identified a method to coat the authentic identities of nodes by unidentified identity. Every node is loaded before with a big number of unidentified public and private identities and the corresponding public key identities. The usual infrastructure public key-data is adopted as the secure channel to attain data and validation.

Lin et al., [7] demonstrated a method on a cluster signature. Only a cluster key of private and public are kept in the vehicle. The cluster key is common for all vehicles, and each vehicle key is different. Any recipient only contras the validity of the signature by the cluster key, node has no uniqueness information of the data sender in the sender data.

Zhang et al.,[8] magnified a scheme for communication in Vehicular networks. Adopting single iteration of identified signature, it eliminates checking and broadcasting the data. It reduces the altogether delay of a cluster of data signatures.

Imran Memon et al., [10] have projected a novel process so that node reduces the delay problem. Nodes stirring trend, variation in speed and distance variation are taken into account so as to maintain as many nodes as possible to decrease the cost.

III PROPOSED SCHEME

The proposed scheme is implemented in IBV (Identity Batch Verification) for wireless nodes single time based signature eliminates the authentication and broadcast permit cost for not restricted keys. IBV changes the on the whole certification setback of a bunch of signatures which are communicated and its group verification process for signatures from several nodes is faster speed than that of other Public Key Infrastructure based scheme, In accumulation, the node linked data is confined from attacker access, even the Trusted authority can unveil the sender when clash appears. The Trusted Authority is able to find a sender's real identity from fake character.

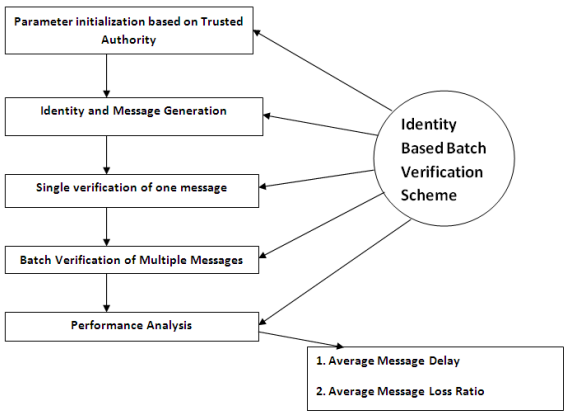

Fig 3: Methodology for proposed work

Volume: 11 Issue: 04 Pages: 4354-4358(2020) ISSN: 0975-0290

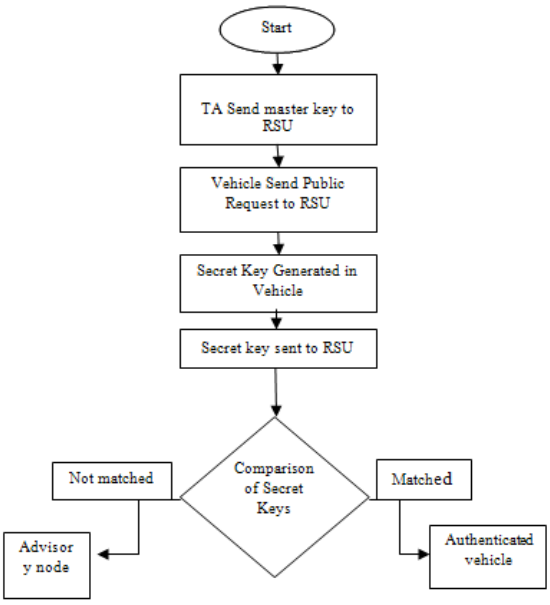

Fig . 4. .Flow diagram for key authentication

Step 1: TA will broadcast the private key to the RSU. (Private Key will be provided to the vehicle at the time of registration).

Step 2: RSU will be having a public key for a group. The vehicle will send a public key request to the nearby RSU.

Step 3: RSU upon request will send the public key to vehicle , vehicle will form a secret key by XOR-ing the public key and private key it has.

Step 4: RSU will also XOR the private and the public key and forms a secret key. The secret key of vehicle is shared between RSU and vehicle.

Step 5: Comparison of secret keys happens. If they are matched, then the vehicle is said to be an Authenticated vehicle else it is considered as malicious vehicle.

IV RESULTS

TA will broadcast the private key to the RSU as shown in Figure 4. Private Key will be provided to the vehicle registration time.

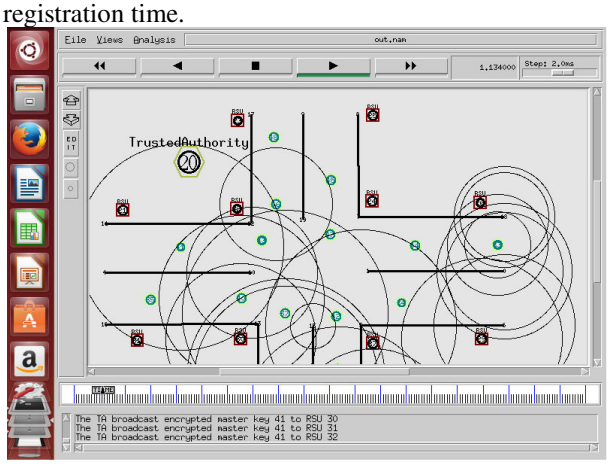

Fig . 5. Trusted authority broadcasting the private key

Secret Key of the vehicle matches with that of Secret Key that is stored in RSU then the Signature is Valid as shown in figure 5.

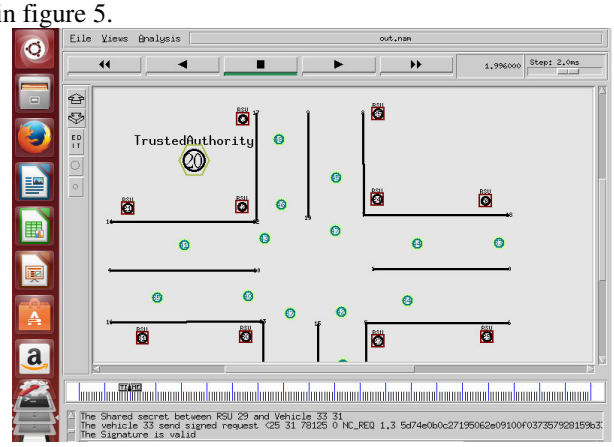

Fig. 6. Verification of secret key

Secret Key of the Vehicle matches with that of Secret Key that is stored in RSU then the Signature is invalid as shown in Figure 6.

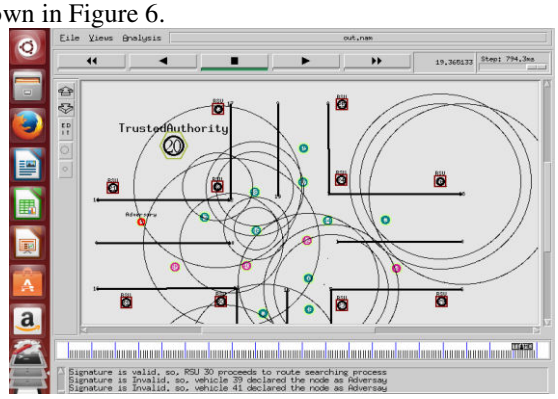

Fig. 7. Matching with secret key

V PERFORMANCE EVALUATION

The proposed IBV evaluation in terms of computation delay, transmission overhead and packet delivery ratio.

Table1: Simulation parameters

Specification	Value
model area	1500m*1500m
model time	20
Wireless protocol	802_11
Model tool	NS-2
Routing protocol	AODV
Topology	Flat-grid

Ns-2 simulator is used to calculate approximately the show of the proposed IBV scheme with **Boneh–Lynn–Shacham**.

BLS scheme is for the systems where verification in signature are done by the person transmitted over a low frequency link using minimum size to obtain short signatures.

Volume: 11 Issue: 04 Pages: 4354-4358(2020) ISSN: 0975-0290

$$AMD = \frac{\sum_{i=1}^{N_V} \sum_{j=1}^{Ni_M} \sum_{k=1}^{N_R} \left(T_{Recv}^{V_i \to R_k, M_j} - T_{Send}^{V_i \to R_k, M_j} \right)}{\sum_{i=1}^{N_V} Ni_M} + T_{Veri}^{avg}$$

N_V is the number of vehicles in the simulation area, Ni_M is the number of messages sent by the vehicle Vi, and N_R is the number of RSUs in the simulation area. $T\ Vi \to Rk,mj$ Send is the time

When the vehicle Vi sends the message mj to the RSU Rk, and $T\ Vi \to Rk,mj$ Recv is the time when the RSU Rk receives the message mj from the vehicle Vi. $T_{verif}^{\ avg}$ is the average verification time that the RSUs authenticate vehicles.

A .transmission overhead

transmission overhead introduced by the signature, overhead(μs) in y-axis and number of messages(kbps in x-axis, proposed IBV scheme shows less overhead as shown in Figure 7 than BLS algorithm.

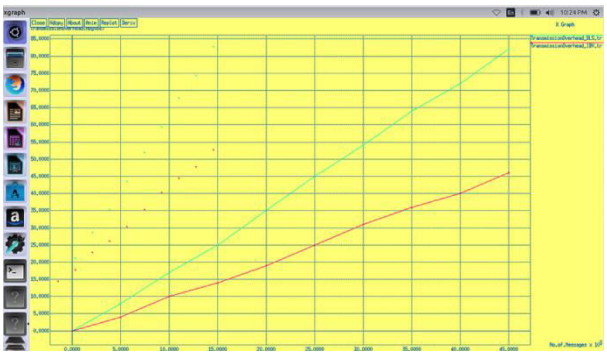

Fig. 8 . Overhead of transmission with the number of messages observed by the receiver.

B .Average message delay

Computation delay is important issue which affects the traffic scenarios. .Delay in y-axis and number of messages in x-axis, proposed scheme shows less delay than BLR algorithm as shown in figure 8.

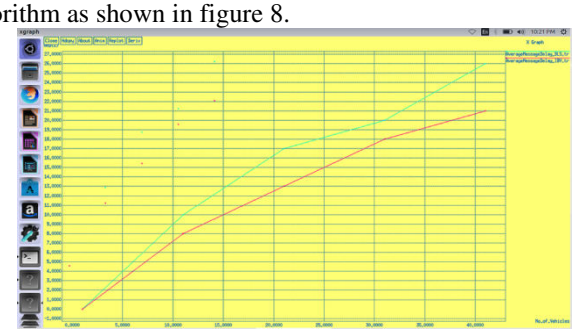

Fig .9. Average message delay versus number of vehicles

C .Average Message Loss

Delay (μsec) towards y-axis and number of vehicles in x-axis, proposed scheme shows less delay than BLR algorithm as shown in figure

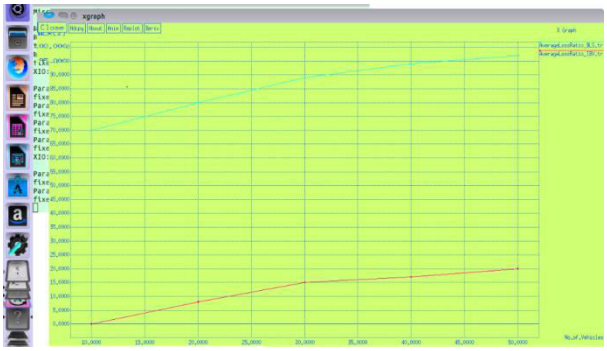

Figure. 10. Average message loss ratio versus moving speed of vehicles

D. Delay in signing messages

Proposed Scheme proved that lowest verification delay when the traffic load increases as shown in figure 10.

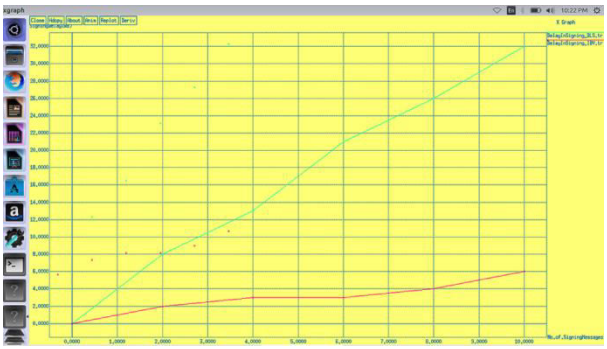

Fig. 11. Delay in signing messages with respect to the number of signing messages

VI. CONCLUSION

The work has proposed a capable idea for vehicular networks. The cluster -based authentication for several data capable than single authentication when the recipient has to verify data. Presentation analysis, the proposed IBV scheme is evaluate with BLR schemes in terms of calculation delay and communication overhead. Tool performance simulate that both the data standard delay and transmission overhead proposed scheme are below BLR scheme.

REFERENCES

[1] Shiang-Feng Tzeng,Shi-Jinn Horng,Tiannui Li,Xian Wang,Po-Hsian Huang and Muhammad Khurram Khan "Enhancing Security and Privacy for Identity-Based Batch Verification Scheme in Vanet"IEEE Transactions on Vehicular scheme in Vanet"IEEE Tranactions on vehicular technology ,VOL.66,NO.4,April 2017.

[2] Jonathan Peti"Analysis of ECDSA Authentication Processing in Vanet"IRIT-Paul Sabatier University Toulouse ,France@ 2009 IEEE.

Volume: 11 Issue: 04 Pages: 4354-4358(2020) ISSN: 0975-0290

[3] C.Zhang,X.Lin,R.Lu,P.H.Ho and X Shen "An efficient message authentication scheme for vehicular communications"IEEETrans,Veh,Technology,vol.57,no,6, pp.33573368,Nov.2008

[4] KhaledRabieh ,Mohamed M.E.A.Mahmoud,Member ,IEEE,and Mohamed Younis "Privacy Preserving Route Reporting Schemes for Traffic Management Systems"IEEE Transactions on Vehicular Technology,VOL 66,NO,3,March-2017.

[5] LibingWu, Jing Fan, YongXie, JingWang, Qin Liu "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc Networks" International Journal of Distributed Sensor Networks, Vol. 13(3), 2017.

[6] M.Raya,P.Papadimitratos and P.Hubaux "Securing Vehiclar Communications" IEEE Wireless Communication ,vol 13,no.5,pp.8-15,oct.2006.

[7] Zhang, X. Lin, R. Lu, P. H. Ho "Security in vehicular adhoc Network," IEEE Commun. Mag.,vol. 6, no. 4, pp. 88–95, Apr. 2008.

[8] C. C. Lee and Y. M. Lai, "Toward a secure batch verification with group testing for Vanet," Wireless Netw., vol. 19, no. 6, pp. 1441–1449, Aug. 2013.

[9] Imran Memon,• Qasim Ali Arain,• Hina Memon Farman Ali Mangi ,Efficient User Based Authentication Protocol for Location Based Services Discovery over Road Networks Springer Science+Business Media New York, pp. 98-110, 2017.

[10] Qasim Ali Arain,• Deng Zhongliang,• Imran Memon Salman Arain,• Faisal Kareem Shaikh,• Asma Zubedi,Mukhtiar Ali Unar, Aisha Ashra, Roshan Shaikh , "Privacy Preserving Dynamic Pseudonym-Based Multiple Mix-Zones Authentication Protocol over Road Networks"23 November 2016 .

[11] Liming Jiang ,yan Wang, Jiajun Tian ,Frank Jiang" An efficient Dynamic Group Based Batch Verification Scheme for Vehicular Sensor Networks" International conference on Future Network Systems and Security, October 2019.

[12] Anitha S Sastry,Shazia Sulthana, Dr. S Vagdevi" Security Threats in Wireless Sensor Networks in Each Layer" Int. J. Advanced Networking and Applications Volume: 04 Issue: 04 Pages:1657-1661 (2013) ISSN : 0975-0290.