International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-05, Issue-04, July 2019

A Novel Approach for Improving Security and Efficiency in VANET by Anonymous Identity Traceability

Dr.Dayanand J, Professor, GNDEC, Bidar, Karnataka, INDIA, jdayanand1@gmail.com

Jeevitha, Student, GNDEC, Bidar, Karnataka, INDIA, josephjeevitha1@gmail.com

Abstract – Vehicular ad hoc network (VANET) provides communication between vehicles and between vehicles and road side unit (RSU) with an aim of providing efficient and safe transportation. Vehicles have to be prevented from some attacks on their privacy and misuse of their private data. For this reason security and privacy are important issues in VANET. The Identity-based batch verification (IBV) scheme was proposed to make VANET more reliable and efficient for practical use. The existing IBV has some security risks. This work introduces an improved scheme that can satisfy the security and privacy desired by vehicles. Additionally batch verification of proposed scheme needs only a small constant number of pairing and point multiplication computations, independent of the number of messages. The efficiency merits of the modified scheme are shown through performance evaluation in terms of delivery delay, packet delivery and delivery rate. Moreover, extensive simulation is conducted to verify the efficiency and applicability of the improved scheme,,

***Keywords* — *VANET, Efficiency, Traceability, V2V, RSU, Trusted Authority, Dedicated Short Range Communications (DSRC*).**

I. Introduction

Vehicle populace has been expanding every day, this leads towards expanded number of mishaps. To beat this issue, Vehicular Ad Hoc Network (VANET) has thought of parcel of clever thoughts, for example, vehicular correspondence considering security and protection as major concern.VANET gives a system where vehicles among the street impart for driving securely. Vehicles are outfitted with onboard unit (OBU), which speaks with different vehicles just as roadside units (RSUs) situated at road to build the driving wellbeing. So this correspondence alludes Vehicles-to-Infrastructure (V2I) & Vehicle-to-Vehicle (V2V) correspondence. A confided in outsider, known as Trusted Authority (TA), speaks with RSU by wired association. TA is fueled with adequate capacity and computational ability. So this system gives a productive method to detect different physical sign to traffic dispersion and gathers different traffic data with more precision and ease. This correspondence is fundamentally represented by Dedicated Short Range Communications (DSRC) convention. Every vehicle intermittently communicates about its present state to its closest vehicle and RSUs in each 100-300 ms. RSU confirms the messages to check its legitimacy and furthermore here and there deals with the traffic circumstance locally.

II. Literature Survey

Numerous attempts are made in order to improve security

and privacy in VANET. In [1], is an autonomous position verification in which detection component is equipped for perceiving hubs duping about their situation in signals (occasional position spread in most single-way geographic steering conventions, for example GPSR) The simulative assessment demonstrates that our position confirmation framework effectively reveals hubs dispersing false positions and accordingly generally counteracts assaults utilizing position duping. In [2], presents an overview that classifies security issues, difficulties and attack types as indicated by various VANET applications. In [3], Securing vehicular ad hoc networks by providing lot of security conventions, it demonstrates that they ensure protection and examine their vigor and effectiveness. In [4], The Vehicle security Communications – application (VSC-A) plan be a three-year adventure (December (2006) - December (2009)) to make & check correspondences based on vehicle-2-vehicle (V-2-V) security structures in the direction of choose whether Dedicated – Short -Range- connections (DSRC) at 5.9 GHz, in mix among vehicle arranging, preserve upgrade self-directed vehicle - base prosperity system as well as furthermore engage novel exchanges base security application. In [5], The ITS correspondence framework depends on roundabout trust connections fabricated statically utilizing affirmation by confided in outsiders (TTPs), for the most part the enrolment specialist (EA). Enrolment is the principle access control to the ITS and the ownership of a substantial enrolment endorsement stipends consent to the station to be a piece of the ITS and, in this way, to pick up approval for the utilization of further administrations. It should, in this way, be confined to stations that satisfy a lot of security properties that are considered to make the stage trusted.

DOI : 10.35291/2454-9150.2019.0314

III. System Design

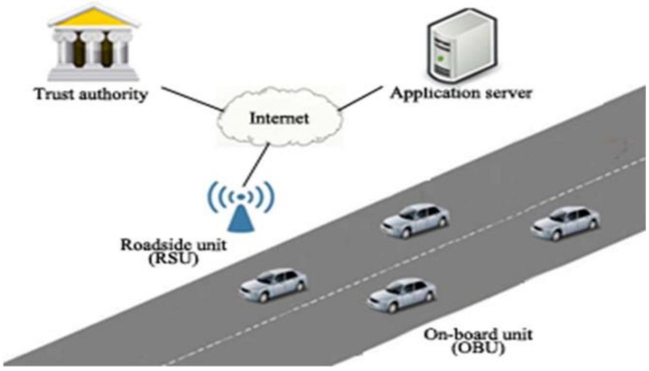


Figure 3.1: System architecture has four entities, i.e., a TA, application server, RSUs by the side of the streets, and OBUs introduced on vehicles.

The Figure 3.1 demonstrates the two-layer vehicular network model whereas the top layer comprises of TA and application servers. The TA and application servers communicate with RSUs through secure channels, such as the transport layer security protocol, by wired connections. The lower layer includes vehicles and RSUs. The communication among them is based on the dedicated short-range communications (DSRC) protocol [6]. As per the VANET safety standard, every vehicle has its individual open/confidential key sets issue via TA. Previous to communication be send, vehicle need to symbol the communication through their confidential keys to ensure the respectability of communication. Getting the wellbeing associated otherwise non traffic associated data, every RSU otherwise vehicle is in charge of confirming their signature of messages.

In the proposed scheme we assume the following:

1. TA is totally trusted by everybody, and it is controlled with adequate calculation and capacity ability. The excess TAs is introduced to abstain from individual a bottleneck or a solitary purpose of disappointment.
2. TA is the solitary in particular to determine the vehicle genuine personality but not by others.
3. TA as well as RSUs convey during a protected fixed network (e.g., Internet).
4. RSUs are not trusted. Because they are placed besides street elevation, they preserve be effectively traded off as well, they be intersected on vehicle security.
5. Tamper-evidence gadgets OBU on vehicles are accepted and its data has never been unveiled [7].

IV. Implementation

The proposed framework gives upgrades to the current framework plan. It attempts to make the current framework increasingly productive, helpful and easy to understand.

The three modules actualized are as per the following:
1. Network Configuration
2. Selection of Registration Node
3. Batch Verification

4.1. Network Configuration

VANET gives a system where vehicles among the street convey for driving securely. Vehicles are furnished with onboard unit (OBU), which speaks with different vehicles just as roadside units (RSUs) situated at road to expand the driving wellbeing. So this correspondence alludes Vehicles-to-Infrastructure (V2I) & Vehicle-to-Vehicle (V2V) correspondence [8]. A confided in outsider, known as Trusted Authority (TA), speaks with RSU by wired association. TA is controlled with adequate capacity and computational ability. So this system gives an effective method to detect different physical sign to traffic appropriation and gathers different traffic data with more precision and ease.

Simulation Parameters for Network Configuration in Rsu

Parameters	Value
Simulation area	2400m*2400m
Simulation time	80 s
Wireless protocol	802.11a
Network simulation tool	Ns-2
Mobility generation tool	TraNS
Pause traffic	0 s
Packet size for the proposed IBVmessage	67 bytes

4.2 Selection of Registration Node

It gives a verified correspondence in VANET by dealing with both "impromptu/messages” just as "bunch messages". At whatever point a vehicle meets another RSU, it validates itself with TA through RSU. At that point TA permits RSU to confirm the vehicle signature with its pseudo personality [9]. TA sends its lord key and shared mystery to the vehicle once in the session of correspondence. So as to send adhoc messages, vehicle needs to sign the messages with its marking key and sends for check. RSU confirms every one of the messages in cluster mode and communicates notice message to the sender vehicles. So as to send gathering messages, a gathering is made with set of wanted vehicles. A mystery key is made for the gathering by TA and is sent to the individuals from the gathering.

4.3 Batch Verification

This improved confirmation scheme is proposed with group check dependent on bilinear matching to make

DOI : 10.35291/2454-9150.2019.0314

VANET progressively secure, effective and increasingly reasonable for down to earth use. In this scheme sealed gadget checks the genuine personality and secret word, creates the Anonymous Identities [10]. With the assistance of this Anonymous Identities and timestamp, it produces the marking key. With the assistance of these keys, messages will be marked by vehicle and sent to RSU. RSU first check the sparkle of the got communication via the timestamp and continues for batch verification. This plan proficiently handles replay attack as it is thinking about the timestamp but it has some extreme security imperfections, for example, hostile to discernibility attacks, falsification assault and character protection infringement.

Algorithm steps for IBV

Step 1: TA selects a main q, two groups G with G_T of sort q, an originator P in G, with a bilinear map eˆ: G × G → G_T

Step 2: TA choose two haphazard statistics

Step 3: TA pick three hash function H: {0, 1} ∗ → G, h: {0, 1} ∗ → Z_{q*} and h2: {0, 1} ∗ → Z_{q*}

Step 4: The parameter $\{G, G_T , q, e, P, P\ \hat{}\ P_{Pub1} , P_{Pub2}, H (\cdot), h(\cdot), h2 (\cdot)\}$ are openly accessible via each RSU as well as vehicle.

Step 5: every vehicle is assign through an actual uniqueness RID are kept in its OBU.

Where, TA-A Trust Authority

G-A cyclic preservative cluster

G_T-A cyclic multiplicative cluster

P-The generator of the recurring set G

q-The order of G with G_T

$e^{\wedge}$-The bilinear map $e^{\wedge}$: G × G → G_T

P_{Pub}, P_{Pub1}, P_{Pub2}-The public keys of TA

H (·)-A chart to tip hash utility such as H: {0, 1} ∗ → G

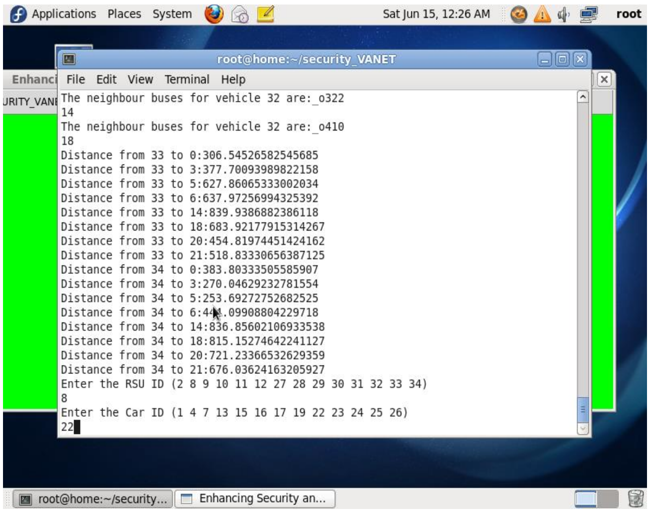
H (·), h2 (·)-Hash utility such as SHA-224 or SHA- 256

RSU-Road Side Unit

OBU-On Board Units

V. EXPERIMENTAL RESULTS

5.1 Number of nodes for RSU and Car

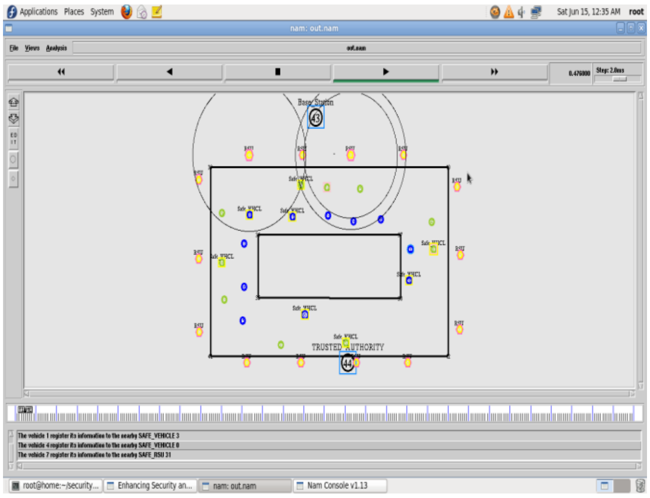


```
The neighbour buses for vehicle 32 are:_o322
14
The neighbour buses for vehicle 32 are:_o410
18
Distance from 33 to 0:306.54526582545685
Distance from 33 to 3:377.70093989822158
Distance from 33 to 5:627.86065333002034
Distance from 33 to 6:637.97256994325392
Distance from 33 to 14:839.9386882386118
Distance from 33 to 18:683.92177915314267
Distance from 33 to 20:454.81974451424162
Distance from 33 to 21:518.83330656387125
Distance from 34 to 0:383.80333505585907
Distance from 34 to 3:270.04629232781554
Distance from 34 to 5:253.69272752682525
Distance from 34 to 6:44[illegible].09908804229718
Distance from 34 to 14:836.85602106933538
Distance from 34 to 18:815.15274642241127
Distance from 34 to 20:721.23366532629359
Distance from 34 to 21:676.03624163205927
Enter the RSU ID (2 8 9 10 11 12 27 28 29 30 31 32 33 34)
8
Enter the Car ID (1 4 7 13 15 16 17 19 22 23 24 25 26)
22
```

Figure: 5.1Number of node for RSU and Car

Screen appearing shows up Rsu contains 14 nodes and Car contains 13 nodes with different ID’s.

5.2 Window of Simulation

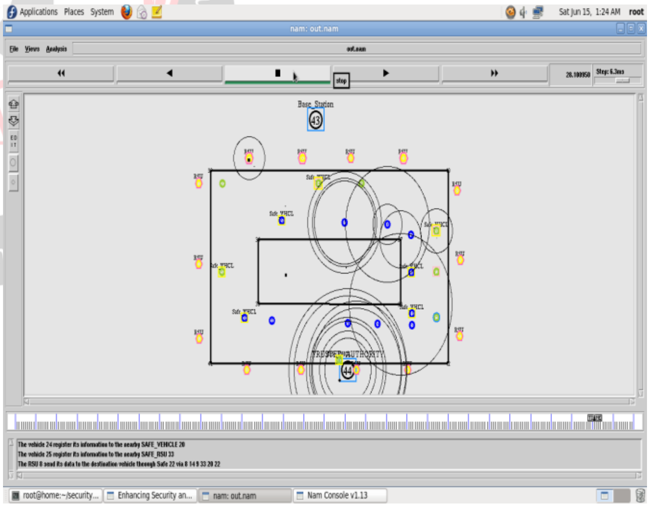


```
The vehicle 1 register its information to the nearby SAFE_VEHICLE 3
The vehicle 4 register its information to the nearby SAFE_VEHICLE 0
The vehicle 7 register its information to the nearby SAFE_RSU 31
```

Figure:5.2 Window of Simulation

Screen appearing shows up demonstrates the yield reenactment though the outside box represents RSU units and inside box are vehicles in moving zone. TA (Trusted Authority) decides vehicles genuine personality of car.RSU speak with TA through Internet.RSU gets traffic subtleties from TA and sends to mentioned vehicle id.

5.3 Packets transmitting and Forwarding from Rsu to required Vehicle



```
The vehicle 24 register its information to the nearby SAFE_VEHICLE 20
The vehicle 25 register its information to the nearby SAFE_RSU 33
The RSU 8 send its data to the destination vehicle theough Safe 22 via 8 14 9 33 20 22
```

Figure: 5.3Packets transmitting and forwarding from RSU to required vehicle

Screen appearing shows up packets are transmitting from RSU to require vehicle through DSRC (Dedicated short range correspondence) which is remote correspondence which is accomplished by means of most secure vehicles.RSU gets traffic subtleties from TA and it sends to chosen CAR ID.

DOI : 10.35291/2454-9150.2019.0314

5.4 Screen appearing for Delivery Delay

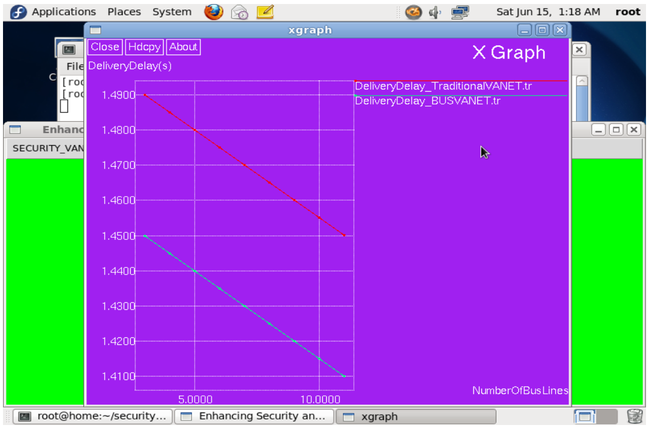


Figure: 5.4 Delivery Delay

Screen appearing shows up conveyance postponement is less contrasted with conventional vanet. Deferral is decreased and there will be quicker correspondence among RSU and Vehicle.

5.5 Screen appearing for Packet Delivery

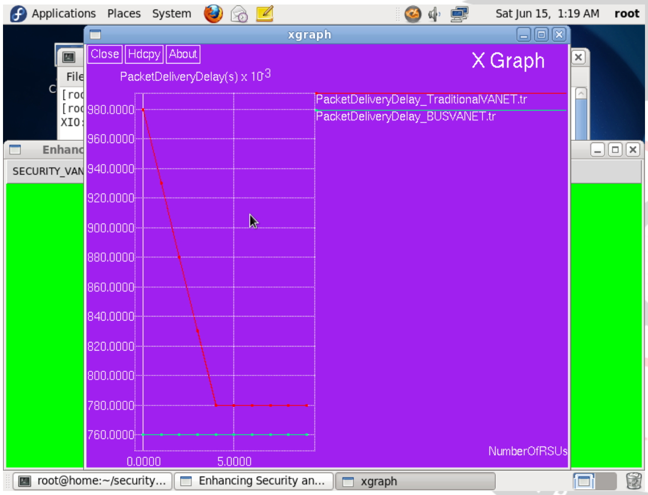


Figure: 5.5 Packet Delivery

Screen appearing shows up bundles are conveyed in less time contrasted with Traditional Vanet.

5.6 Screen appearing for Delivery rate

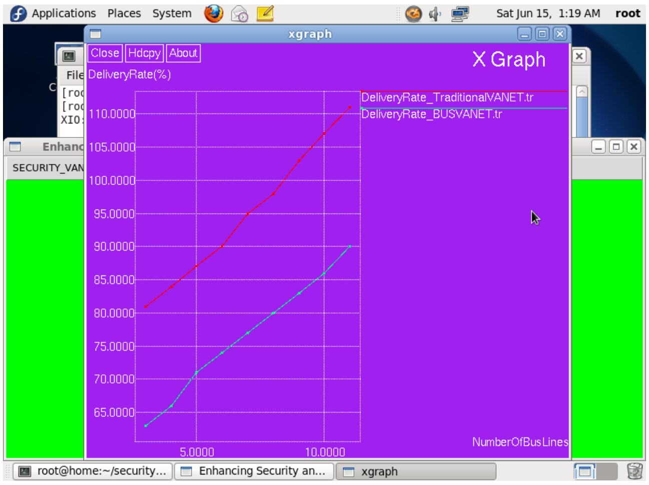


Figure:5.6 Delivery Rate.

Screen appearing shows up conveyance Rate has been diminished contrasted with Traditional Vanet.

VI. CONCLUSION

This work focuses on improvement in IBV to provide secure communication and protect the privacy of data in VANET. The IBV (Identity-based Batch Verification) scheme is proposed for V2I & V2V communication in VANET. The IBV for multiple message signatures is more efficient than one-by-one single verification when the receiver has to confirm large number of messages. In particular IBV needs only constant number of pairing and point multiplication independent of number of message signatures. Consequently the time cost decreases on verifying large number of messages which achieves better scalability. The extensive simulation results shows the existing IBV contains delivery delay 1,4900s, packet delivery 9800000s and delivery rate 1100000% whereas the modified IBV contains delivery delay 1,4500s, packet delivery 7600000s and delivery rate 900000%. IBV not only achieves the privacy preserving desired by vehicles and also the traceability required by trust authority that satisfies security issues such as authentication, integrity and enforceability.

VII. FUTURE SCOPE

This work can be extended with modification of IBV in VANET, for example, perceiving illegal signatures. When attackers propel a few unacceptable communications, the batch verification might lose its efficacy. This issue commonly goes with other batch verification scheme. Thusly, impeding the invalid signature issue is a difficult point to concentrate in our future research.

REFERENCES

[1] T. Leinmüller, C. Maihöfer, E. Schoch, “enhanced safety in geographic ad hoc direction-finding during autonomous spot confirmation.

[2] K. Plossl, T. Nowey, with C. Mletzko, “Toward safety structural plan pro vehicular ad hoc networks

[3] M. Raya with J. P. Hubaux, “secures vehicular ad hoc networks,” J. Comput. Safety — unique concern protection Ad Hoc Sensor.

[4] F. Ahmed-Zaid et al., “Vehicle security interactions – application.

[5] Intellectual Transport Systems (ITS), safety, ITS Communication safety design as well as safety Management.

[6] Y Agarwal, K Jain, S Kumar-“TLST-Time of arrival based localization and smart tunnel concept in VANETs” 2016.

[7] Florian Marcus Schaub-“Conditional Pseudonymity in Vehicular Ad Hoc Networks”November 13, 2008.

[8] BR Maitipe, U Ibrahim, MI Hayee”Vehicle-to-infrastructure and Vehicle-to-Vehicle information system in work zones-Transportation 2012.

[9] Baosheng Wang, Yi Wang, and Rongmao Chen-“A Practical Authentication Framework for VANETs”.

[10] T Praprotnik-“From Anonymity to Self-Disclosure, recontextualization of communication in new media” 2015.