International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Efficient Authentication in VANET using Clustering and Trust Degree Estimation Process

S.Raja[1], Dr.P.Sachidhanandam[2]
[1]*M.E (Department of Computer Science),* [2]*Associate Professor, M.E, Ph.D., Department of Computer Science, Knowledge Institute of Technology, Kakapalayam, Salem, Tamil Nadu, India*

Abstract: ***Since Vehicular ad hoc networks (VANETs) are defenseless against different kinds of attacks, there is a need to satisfy the security prerequisites like message protection, honesty, and confirmation. The verification strategy is said to be productive efficient if it detects compromised nodes precisely with less complexity, decreased confirmation delay, and keying overhead. In this paper, a trust-based authentication scheme for cluster-based VANETs is proposed. The vehicles are clustered, and the trust degree of every node is assessed. The trust degree is a mix of direct trust degree and it's not direct trust degree. Based on this estimated trust degree, cluster heads are selected. Then, each vehicle is monitored by a set of verifiers, and the messages are digitally signed by the sender and encrypted using a public/ private key as distributed by a trusted authority and decrypted by the destination. In view of this assessed trust degree, cluster heads are chosen. At that point, every vehicle is checked by a lot of verifiers, and the messages are carefully marked by the sender and encoded utilizing a Public / private key as distributed by a trusted authority and decoded by the destination. This confirms the identity of sender just as receiver hence giving confirmation to the scheme. By simulation results, we demonstrate that the proposed procedure gives high security less overhead and delay.***
Keywords: Trust degree estimation, authentication, privacy preserving, vehicular ad-hoc network and clustering.

I. INTRODUCTION

A. VANET

VANETs have been developed because of the advances in remote interchanges and systems administration advances. The VANETs improve traffic well being and efficiency [4]. For correspondences in VANETs, every vehicle has a remote specialized gadget named as an on board unit (OBU), and a remote correspondence convention named as dedicated short range communication (DSRC), which applies the IEEE 802.11p standard for remote correspondence, and is utilized for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) interchanges. Due to the remote correspondence mode, it is simple for an enemy to assume responsibility for correspondence connects and can change, erase and replay messages. Subsequently, the pantomime, modification, replay and man in the center assaults are not kidding dangers for VANETs. These dangers may prompt traffic bedlam or mishap.
Accordingly, security of transmitted messages is one of the fundamental necessities in VANETs. Likewise, protection of the vehicle's character must be accomplished since spillage of their personalities may result in genuine dangers for drivers since pernicious substances can follow their messages and traveling roads for crimes. In any case, unrestricted security saving isn't alluring for VANETs, since noxious vehicles ought to be followed and rebuffed in the event of any bad conduct.Mobile Ad-hoc network (MANET) is developing all around as a correspondence instrument. A MANET is commonly characterized as a system that has many free or self-governing hubs frequently made out of cell phones or other portable pieces that can organize themselves in different ways and work without exacting top-down system organization. Versatile Ad-Hoc Networks is coordinated with remote hubs that can convey anyplace. MANET are sorted into three kinds: VANET, InVANET and iMANET. Vehicular Ad Hoc Networks (VANETs) is innovation that incorporates the capacities of new age remote systems to vehicles. VANET constructs a hearty Ad-Hoc organize between versatile vehicles and roadside units. It is a type of MANET that sets up correspondence among close-by vehicles and contiguous fixed device, generally depicted as roadside mechanical assembly. VANET can accomplish emotional correspondence between moving hub by utilizing diverse specially appointed systems administration instruments, for example, Wife IEEE 802.11 b/g, WiMAX IEEE 802.10, Bluetooth, IRA.
VANET is mainly aimed at providing safety related information and traffic management. Safety and traffic management entails real time information and directly affect lives of people travelling on the road. Simplicity and security of VANET mechanism ensures greater efficiency. Safety is realized as prime attribute of Vehicular Ad Hoc Network (VANET) system. The majority of all nodes in VANET are vehicles that are able to form self organizing networks without prior knowledge of each other. VANET with low

security level are more vulnerable to frequent attacks. There are wide range of applications like commercial establishments, consumers, entertainment where VANET are deployed and it is very necessary to add security to these networks so that damage to life and property could not occur.

VANET inculcate sufficient potential in vehicles to transmit warnings about environmental hazards, traffic and road conditions and regional information to other vehicles. The major intend of VANETs is to absolute the user's choice on the road and build their drive safe and snug. Vehicles move at such a high speed that it is harder to maintain a seamless handoff and a steady connectivity to the Internet.

VANETs consist of following entities:

1) Access point: The access points are fixed and normally associated with the web. Vehicle to vehicle correspondence has two kinds of communication single hop and multi hop.

2) Vehicle: vehicle is nodes of vehicular network. VANET addresses the wireless communication between vehicles (V2V) and between vehicles and infrastructure access point (V2I)

B. Characterstics

There are various appealing and attractive features that make a difference from other types of networks.

1) High Mobility: The nodes present in VANETs move at a rapid. These moving hubs can be shielded spared from assaults and other security dangers just if their area is predicable. High portability prompts different issues in VANET

2) Rapidly Changing Network Topology: Vehicles moving at high speed in VANET lead to quick changes in network topology.

3) No Power Constraints: Power imperative dependably exists in different systems however in VANETs vehicles can give capacity to on board unit (OBU) by means of the long life battery. So vitality imperative isn't generally a basic test as in MANETs.

II. LITERATURE SURVEY

S. ZEADALLY, R. HUN (2012) Late advances in equipment, programming, and correspondence advances are empowering the plan and usage of an entire scope of various kinds of systems that are being sent in different situations. One such system that has gotten a great deal of enthusiasm for the most recent few years is the Vehicular Ad-Hoc Network (VANET). VANET has turned into a functioning zone of research, institutionalization, and advancement since it can possibly improve vehicle and street security, traffic effectiveness, and accommodation just as solace to the two drivers and travelers. Ongoing exploration endeavors have set a solid accentuation on novel VANET structure models and executions. A great deal of VANET look into work have concentrated on explicit regions including steering, broadcasting, Quality of Service (QoS), and security. We review a portion of the ongoing exploration results in these regions. We present an audit of remote access measures for VANETs, and portray a portion of the ongoing VANET preliminaries and organizations in the US, Japan, and the European Union. Moreover, we likewise quickly present a portion of the test systems at present accessible to VANET specialists for VANET recreations and we evaluate their advantages and impediments. At long last, we diagram a portion of the VANET investigate moves that still should be routed to empower the omnipresent arrangement and widespead selection of versatile, dependable, powerful, and secure VANET designs, conventions, advances, and administrations.

A. KHERANI, S. N. MUTHAIAH (2010) Misbehavior detection schemes (MDSs) structure a vital piece of getting into mischief hub expulsion in vehicular ad hoc networks (VANETs). An acting up hub can send messages comparing to an occasion that either has not happened (potentially out of noxious goal), or erroneous data relating to a real occasion (for instance, defective sensor perusing), or both, making applications breakdown. While recognizing the nearness of bad conduct, it is likewise basic to extricate the main driver of the watched mischief so as to legitimately evaluate the trouble making's effect, which thusly decides the move to be made. This paper utilizes the Post Crash Notification (PCN) application to delineate the essential contemplations and the key variables influencing the unwavering quality execution of such plans. The fundamental reason tree approach is delineated and utilized adequately to together accomplish misconduct recognition just as recognizable proof of its main driver. The contemplations with respect to parameter tuning and effect of versatility on the execution of the MDS are examined. The execution of the proposed MDS is observed to be not exceptionally touchy to slight blunders in parameter estimation.

P. MUHLETHALER, AND A. LAOUITI, (2008) This article presents a comprehensive survey of the state-of-the-art for vehicle ad hoc networks. We start by reviewing the possible applications that can be used in VANETs, namely, safety and user applications,

and by identifying their requirements. Then, we classify the solutions proposed in the literature according to their location in the open system interconnection reference model and their relationship to safety or user applications. We analyze their advantages and shortcomings and provide our suggestions for a better approach. We also describe the different methods used to simulate and evaluate the proposed solutions. Finally, we conclude with suggestions for a general architecture that can form the basis for a practical VANET. VANETs have several properties that distinguish them from other MANETs. Nodes (vehicles) in VANETs are highly mobile; the probability of network partitions is higher, and end-to-end connectivity is not guaranteed but rather is a luxury. However, although VANETs do have dynamic topologies, they are not completely random. The movement of nodes in a VANET is relatively predictable because it is restricted to the roads on which the vehicles travel. This has several advantages and disadvantages for applications and routing protocols. The predictability of the position of a vehicle allows an improvement in link selection, but the linear topology of VANETs reduces the possible path redundancy. The bandwidth issue also is exacerbated due to intersections, traffic jams, and the presence of buildings beside the roads, especially in an urban environment. VANETs also have the potential to grow to a very large scale. For example, consider a section of a road with three lanes.

2.4 S. Zeadally, and J. S. Camara(2010) Vehicular Ad hoc Networks (VANETs) have developed as of late as a standout amongst the most alluring subjects for specialists and car ventures because of their huge potential to improve traffic security, effectiveness and other included administrations. In any case, VANETs are themselves powerless against assaults that can straightforwardly prompt the debasement of systems and afterward perhaps incite enormous misfortunes of time, cash, and even lives. This paper displays a study of VANETs assaults and arrangements in cautiously thinking about other comparable fills in just as refreshing new assaults and classifying them into various classes.

Be that as it may, numerous types of assaults against VANETs have developed as of late and frightened the agitating circumstance of these systems' security. Being a usage of Mobile Ad hoc NETworks (MANETs), VANETs acquire all the found and unfamiliar security and protection vulnerabilities identified with MANETs. Besides, VANETs have various particular properties [5] that could be additionally vulnerabilities for assailants to abuse. Those properties incorporate the specific idea of correspondence in VANETs. Associations in a VANET specifically and in any Wireless Ad hoc Network when all is said in done depend on hub to-hub correspondences: each hub can go about as either a host asking information or a switch sending information. There are two kinds of hubs: (I) RoadSide Units (RSUs) representing fixed hubs provisioned along the course and (ii) OnBoard Unit (OBU) alluding to versatile hubs (i.e., vehicles) furnished with a type of radio interface that empowers associating with different hubs in remote way. Fig. 2 delineates a general perspective on VANETs structure. It merits referencing that the speed of portable hubs vehicles in VANETs might be a lot higher than in MANETs. This reason makes VANETs exceptionally powerful in nature. Various hubs can convey once as a gathering yet can then quickly change their very own structure brought about by leaving of a part or joining of another hub. Along these lines, it is normal that hubs are constantly "staying in contact" with different hubs in the gathering to keep up the survival of the system. This part of VANETs is by all accounts entirely helpless and assaults can be unwittingly or purposefully performed to harm a piece of or the absolute system. As referenced above, VANETs give many included applications that are security, stimulation, or infotainment arranged. Assaults to VANETs may prompt cataclysmic outcomes, for example, the misfortunes of lives on account of car crash, misfortunes of time (e.g., altering road turned parking lot made by assaults) or budgetary misfortunes (i.e., in installment administrations).

J. P. Hubaux et.al (2007) A significant development for the car business is the one toward setting mindfulness, implying that a vehicle knows about its neighborhood (counting the nearness and area of different vehicles). Present day vehicles currently have a system of processors associated with a focal registering stage that gives Ethernet, USB, Bluetooth, and IEEE 802.11 interfaces. More up to date autos likewise have such highlights as • an occasion information recorder (EDR), roused by the "secret elements" found on planes (EDRs record every single significant datum from the vehicle for accident remaking); • a GPS beneficiary, the precision of which can be improved by learning of street topology (GPS is as of now utilized in numerous route frameworks); and • front-end radar for identifying hindrances at separations to the extent 200 meters (such radar is regularly utilized for versatile journey control)2 and short-remove radar or a ultrasound framework, normally utilized for leaving.

Inter Vehicle Communication (IVC) underpins numerous significant highlights, especially in the region of accident aversion (for instance, by illuminating vehicles about traffic congestion).3 A lot of imparting vehicles is a case of a versatile specially appointed system. The examination network has dedicated much regard for the security and protection of such systems in the previous few years,4– 6 however none of these commitments thinks about any such system for shrewd vehicles, which is the thing that we'll ponder here. In this article, we call a vehicle smartif it is outfitted with chronicle, handling, situating, and area abilities and on the off chance that it can run remote security conventions. Streets can be made keen, as well. Fixed specialized gadgets introduced

along a street can illuminate passing vehicles about the street's exact topology (see the PATH venture, www.path.berkeley.edu). In any case, this present methodology's disadvantage is that it requires a gigantic budgetary venture, which, at first, would profit a little minority of drivers. The perception of what occurs on streets is called traffic observing, Less "meddlesome" systems incorporate video picture processors, microwave radar, infrared laser radar, and acoustic/ultrasonic gadgets.

C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, (2008) With the appropriation of best in class media transmission advancements for detecting and gathering traffic related data, Vehicular Sensor Networks (VSNs) have risen as another application situation that is imagined to upset the human driving encounters and traffic stream control frameworks. To keep away from any conceivable malignant assault and asset misuse, utilizing a computerized mark conspire is broadly perceived as the best methodology for VSNs to accomplish confirmation, honesty, and legitimacy. Be that as it may, when the quantity of marks gotten by a Roadside Unit (RSU) turns out to be extensive, a versatility issue develops quickly, where the RSU could be hard to successively confirm each gotten mark inside 300 ms interim as indicated by the current Dedicated Short Range Communications (DSRC) communicate convention. In this paper, we present a productive group signature check conspire for interchanges among vehicles and RSUs (or named vehicle to-Infrastructure (V2I) correspondences), in which a RSU can confirm different got marks in the meantime with the end goal that the complete confirmation time can be drastically decreased. We exhibit that the proposed plan can accomplish restrictive protection safeguarding that is fundamental in VSNs, where each message propelled by a vehicle is mapped to an unmistakable pseudo personality, while a trust expert can generally recover the genuine character of a vehicle from any pseudo character. With the proposed plan, since character based cryptography is utilized in creating private keys for pseudo personalities, declarations are not required and in this way transmission overhead can be essentially diminished.

III. PROBLEM IDENTIFICATION

In light of the remote correspondence mode, it is simple for a foe to assume responsibility for correspondence interfaces and can change, erase and replay messages. Henceforth, the pantomime, alteration, replay and man in the center assaults are not kidding dangers for VANETs. These dangers may prompt traffic disorder or mishap. Along these lines, security of transmitted messages is one of the primary necessities in VANETs. Likewise, security of the vehicle's personality must be accomplished since spillage of their characters may result in genuine dangers for drivers since malevolent substances can follow their messages and voyaging streets for wrongdoings. Be that as it may, genuine security saving isn't alluring for VANETs, since vindictive vehicles ought to be followed and rebuffed if there should be an occurrence of any bad conduct.

To fulfill security and protection issues in VANETs, some Public Key Infrastructure-based (PKI-based) confirmation plans have been proposed. These plans are not productive since vehicles need to store countless sets and their comparing declarations, and these authentications are required to be transmitted with messages. To address testament the board in PKI-based verification plans, different security saving character based validation plans have been proposed. These verification plans are planned dependent on bilinear pairings and because of their substantial computational expense.

Actually, they proposed personality based marks without utilizing bilinear pairings to improve execution of these plans. Be that as it may, these plans are not quick enough when there are an expansive number of vehicles in the inclusion zone of a roadside unit (RSU). For instance, think about this situation: since every vehicle communicates its traffic wellbeing message each 100-300 milliseconds as indicated by the determination of DSRC convention, when there are 500 vehicles in the inclusion territory of a RSU, the RSU needs to confirm around 1650-5000 marks in a second. This issue is a major test for the present confirmation plans. To handle the previously mentioned issue, a fascinating validation convention utilizing intermediary vehicles for vehicular systems, and called it as PBAS. In PBAS, intermediary vehicles help RSUs to check countless at the same time utilizing appropriated confirmation.

IV. PROPOSED SYSTEM

In order to simplify the public-key authentication, presented the idea identity-based (ID-based) cryptosystem problem, every client needs to enlist at a key generator center (KGC) with personality of himself before joining the system. When a client is acknowledged, the KGC will create a private key for the client and the client's character (e.g., client's name or email address) turns into the relating open key. Along these lines, so as to confirm an advanced mark or send a scrambled message, a client just has to know the "personality" of his correspondence accomplice and the open key of the KGC.

The thought of intermediary signature plot is presented. An intermediary signature plot permits a substance called unique underwriter to designate his marking capacity to another element, called intermediary endorser. Since it is proposed, the intermediary signature plans have been recommended for use in numerous applications, especially in dispersed registering where

assignment of rights is very normal. So as to adjust diverse circumstances, numerous intermediary signature variations are created, for example, once intermediary signature, intermediary dazzle signature, multi-intermediary signature, etc. Since the intermediary signature shows up, it pulls in numerous specialists' extraordinary consideration. Utilizing bilinear pairings, individuals proposed numerous new ID-based signature schemes and ID-based proxy signature(IBPS) plot.

All the above IBPS plans are exceptionally pragmatic, yet they depend on bilinear pairings and the matching is viewed as the most costly cryptography crude. The relative calculation cost of a matching is roughly multiple times higher than that of the scalar duplication over elliptic bend gathering. Along these lines, IBPS plans without bilinear pairings would be all the more engaging as far as proficiency.

To handle the above said issues and have a progressively proficient plan, another personality based validation plot utilizing intermediary vehicles, ID-MAP, without bilinear pairings is proposed.

In ID-MAP scheme, there are three participants.

A. Trusted Authority (TA)

The TA is a confided in outsider which produces framework parameters and ace open key and mystery key, creates individuals' mystery key, preloads them into vehicles, and can follow vehicles from their pseudo personalities if there should be an occurrence of any mischief. TA is the believed administration place for the system. It isolates the area into a few areas. TA is in charge of produce the gathering key and gathering mark material for each area. At that point s closes these materials to the RSU and furthermore gives enrollment and affirmation to RSU and OBU when they join the system.

B. The RSUs

The RSUs are at roadsides, speak with vehicles (intermediary vehicles), can check the legitimacy of got messages from vehicles (intermediary vehicles), and sends them to the traffic control focus. The RSU is a wave gadget generally fixed along the street side or in committed areas, for example, at intersections or close parking spots. The RSU is furnished with one system gadget for a devoted short range correspondence dependent on IEEE 802.11p radio innovation, and can likewise be outfitted with other system gadgets in order to be utilized with the end goal of correspondence inside the infrastructural arrange. RSUs are likewise in charge of issuing the gathering key materials and gathering mark related keys to approve OBUs when OBUs join the area.

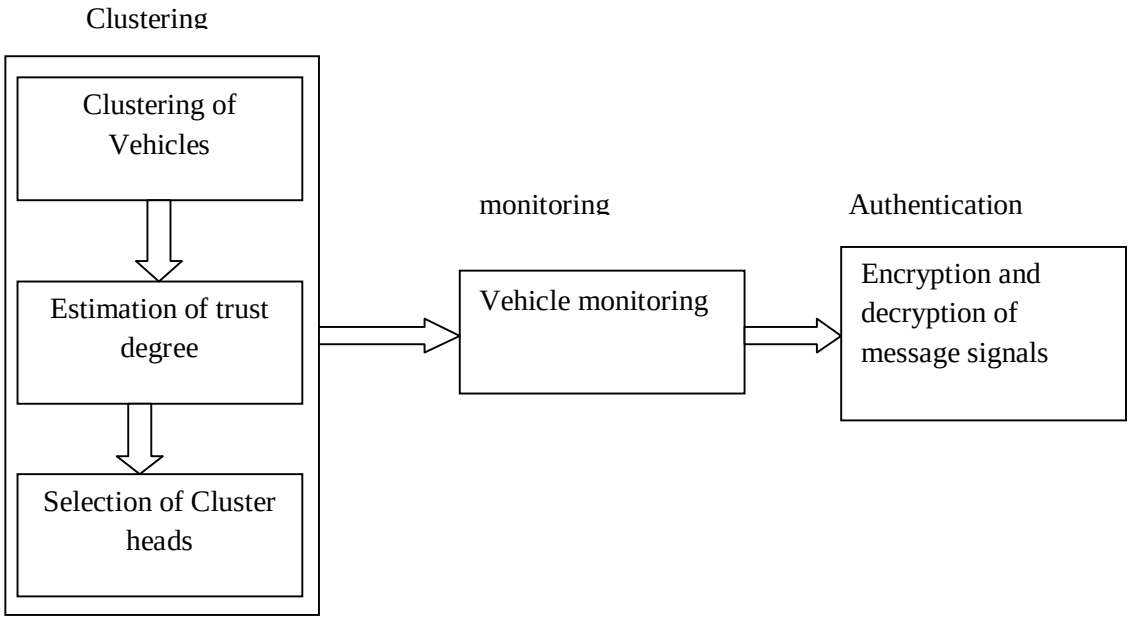

Figure1: System Architecture

C. Vehicles

These are furnished with carefully designed gadgets OBUs, and speak with one another's and RSUs. An OBU is a wave gadget typically mounted on-board a vehicle utilized for trading data with RSUs or with different OBUs. The OBU interfaces with the RSU

or to different OBUs through a remote connection dependent on the IEEE 802.11p radio recurrence channel, and is in charge of the interchanges with different OBUs or with RSUs; it likewise gives a correspondence administrations to the TA and advances information for the benefit of different OBUs on the system.

V. IMPLEMENTATION PROCESS

There are five stages in this plan, Setup, Anonymous personality age, Message age, Verification of messages as a substitute vehicles and Verification of intermediary vehicles' yield by RSUs.

A. Step1: Clustering of Vehicles

In this module, the vehicular network is divided into multiple clusters. Each cluster consists of one cluster head (CH) and one or more members. Vehicles in one cluster are linked directly and vehicles that are located in two different clusters can communicate together via their CHs. Each vehicle can play the role of a CH or gateway or member. If one vehicle is located within two or more clusters, it is called a gateway. Each CH maintains the information about its members and gateways.

B. Step 2: Estimation of Trust Degree

In this module, the trust degree is aggregated for each node. The trust value is calculated based on nodes forwarding behavior. Direct trust and indirect trust are the two parameters calculated for each node. The average trust of a node is calculated based on these two trust values. Trust relationships made from the direct interactions is described as direct trust. The trust relationship built from the trusted node or the chain of trusted node is called as indirect trust node

C. Step 3: Vehicle Monitoring and Authentication

In this module, the vehicular nodes are evaluated and selected as forwarder nodes based on the aggregated trust of each node. In monitoring phase, a set of verifier nodes collect information about the behavior of all vehicles in a cluster. If any abnormal behaviors detected, these nodes verify the trust of the nodes. During the authentication procedure, the node attempting to authenticate presents its identity and certificate to the authenticating node. The authenticating node will first verify the certificate using the public key of CA and then challenge the initiating node by encrypting a nonce with the initiating node's public key, to test whether it has the corresponding private key.

VI. RESULT AND DISCUSSION

The result obtained by our proposed system has been discussed clearly in this section.

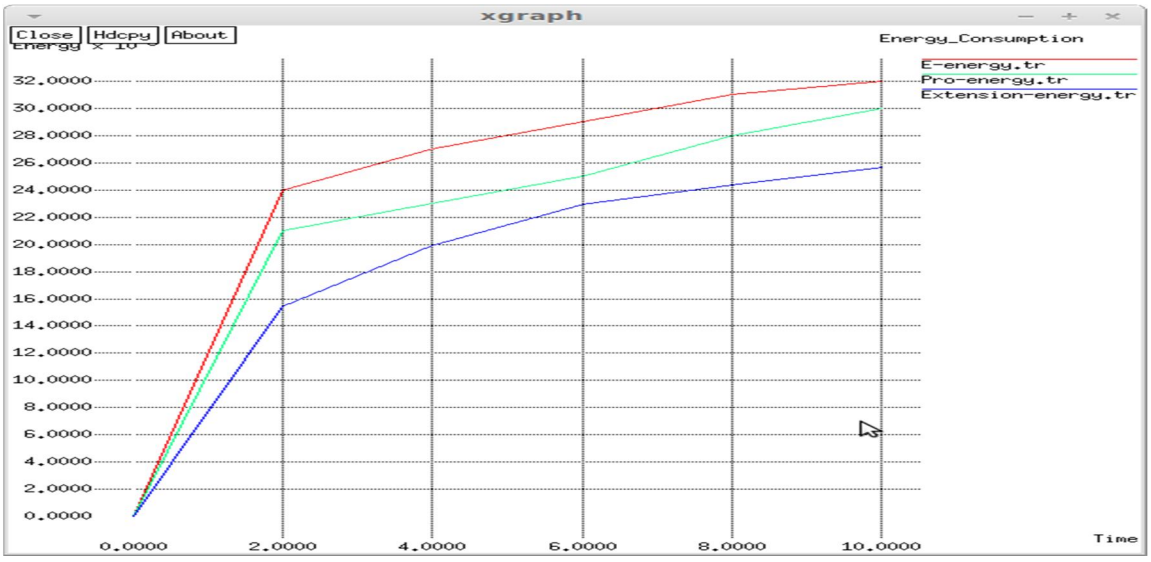

Figure 2: energy consumption comparison graph

The graph shows that our proposed work consumes minimum energy compared to existing systems. The graph generates with respect to two parameters time and number of packets transmitted between source and destination. Initially at starting stage every packets consume same amount of energy and when number of packets increases time consumption reduces compared to existing system. Hence it automatically increases network lifetime.

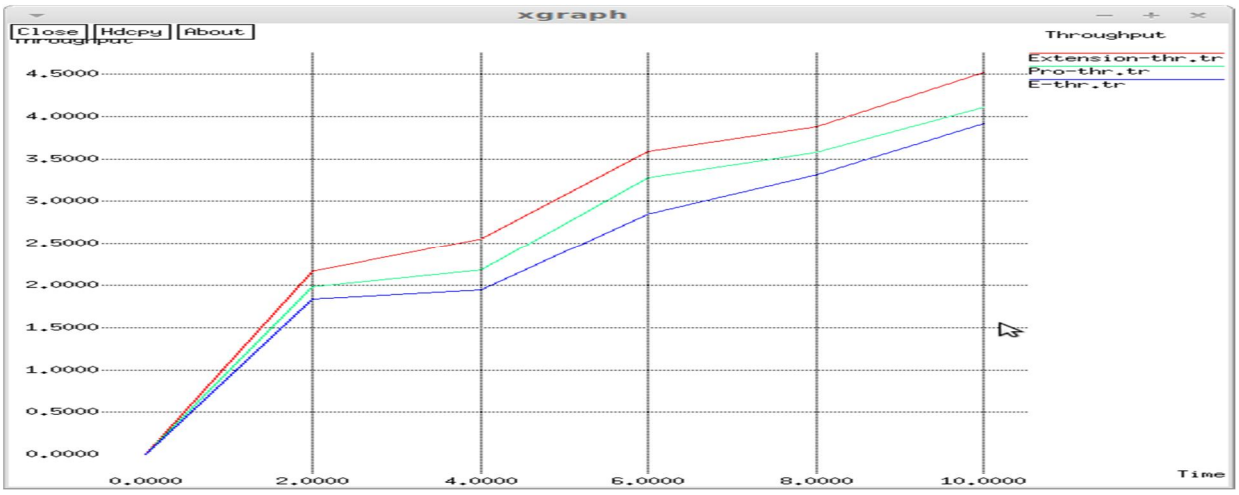

Figure 3: comparison of our proposed and existing system based on throughput parameter

Through put is described as packet delivery between source to destination and the system which achieves high throughput will consider being efficient system. Compared to existing approaches based on time and number of packets parameters it shows that our system achieves high throughput.

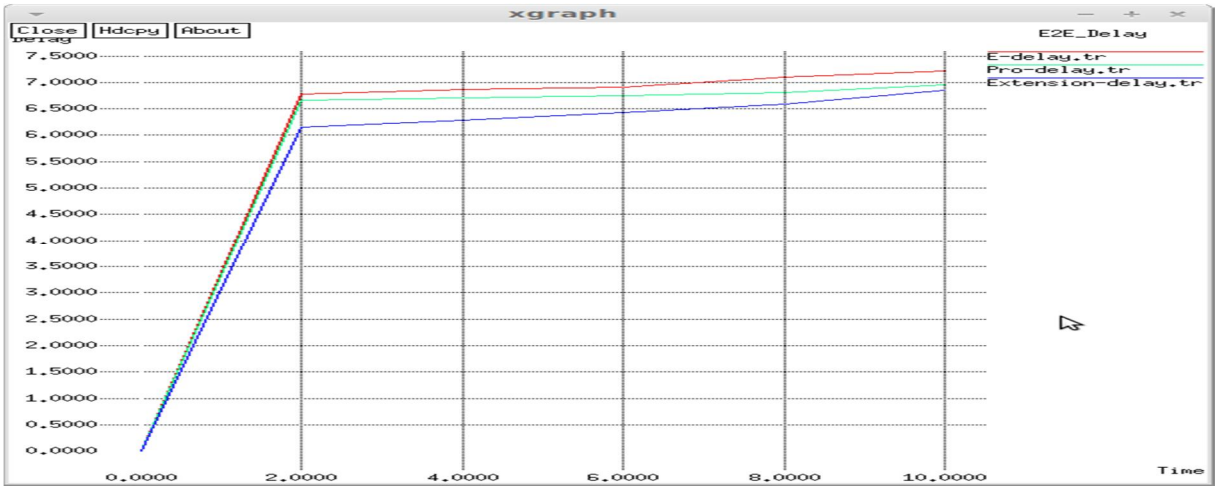

Figure 4: end to end delay comparison

The above graph shows that our proposed system achieves minimum delay in packet delivery ratio. Even though when number of packets transaction increases our proposed system achieves less packet delay in transaction.

VII. CONCLUSION

For VANETs has some security drawbacks: it doesn't fulfill message genuineness, and furthermore it isn't safe against pantomime and alteration assaults and bogus acknowledgment of clustered invalid marks. At that point, to handle the security shortcomings of PBAS, we proposed ID-MAP for vehicular systems. To demonstrate that it is secure against previously mentioned assaults and it has message realness, we demonstrated that the fundamental mark conspire is secure against adaptively picked message and

personality assault under trouble of ECDLP issue in the irregular prophet model. As appeared in the examination, ID-MAP is more effective than PBAS, and furthermore the reenactment results demonstrate that ID-MAP is a proficient contender for VANETs' confirmation in sensible situations.

REFERENCES

[1] S. Zeadally, R. Hun, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): Status, results, and challenges," Telecommunication Systems, vol. 50, no. 4, pp. 217–241, 2012.

[2] M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani, and S. N. Muthaiah, "Detecting misbehaviors in VANET with integrated root-cause analysis,"Ad Hoc Networks, vol. 8, no. 7, pp. 778–790, 2010.

[3] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," IEEE Communications Surveys & Tutorials, vol. 10, no. 3, pp. 74–88, 2008.

[4] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identitybased conditional privacy-preserving authentication scheme for vehicular ad hoc networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2681–2691, 2015.

[5] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," IEEE Wireless Communications, vol. 13, no. 5, pp. 8–15, 2006.

[6] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," IET Communications, vol. 4, no. 7, pp. 894–903, 2010.

[7] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," IEEE Security Privacy, vol. 2, no. 3, pp. 49–55, 2004.

[8] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.

[9] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc. of the 27th Int. Conf. on the Computer Communications- IEEE INFOCOM 2008. Phoenix, AZ, USA: IEEE, 13-18 April 2008, pp. 1903–1911.

[10] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identitybased batch verification scheme for vehicular sensor networks," in Proc. of the 27th Int. Conf. on Computer Communications-IEEE INFOCOM 2008. Phoenix, AZ, USA: IEEE, 13-18 April 2008, pp. 816–824.