Enhancing Security and Efficient Authentication Scheme using K-Means Clustering

Dr. G. Revathy, Ms. P. Logeshwari, Mr. D. Vijaybabu, Mr. M. Sivakumar

***Abstract*—Vehicular Ad-hoc Network (VANET) is an budding technology and is an relevance of Mobile Ad-hoc Network (MANET). Intention of VANET is to construct and present infrastructure amid group of vehicles lacking any central base station. In this paper, we proposition a K-means algorithm clusters to made for guide assortment, both personal best ('pbest') and global best ('gbest'),are found to be tremendously successful and complete well evaluate to the already existing methods. Also proposes a pseudonym authentication and Broadcast Methods for V2V Communications (BMVVC) for Vehicle to Vehicle and Vehicle to Infrastructure (Road Side Unit) communications. This paper proposition an resourceful and practical pseudonymous authentication protocol with restricted privacy preservation. The proposed schemes can be applied for vehicle registration and Re-acquiring pseudonyms in VANET. The proper results show the feasibility of our proposed protocol in terms of end-to-end delay and packet delivery ratio.**

Index Terms: VANET (Vehicular ad-hoc network), K-means clustering, BMVVC Routing protocol, PKI, DSRC (Dedicated Short-range Communication), pseudonyms.

1. INTRODUCTION

Vehicles connected to each other's through an ad hoc formation form a wireless network called "Vehicular Ad Hoc Network". VANET has some uniqueness that are similar to the MANET but VANET has unique feature that make it special from MANET. VANET is a form of network that afford communication vehicle to vehicle and vehicle to roadside wireless communication. It ensures that established routing paths do not break before the end of data transmission. This is a difficult problem because the network topology is constantly changing and the wireless communication links are inherently unstable, due to high node mobility. Each vehicle equipped with Wi-Fi/WiMax device acts as a node and Unique ID and IP address are provided for each vehicle. Each node can communicate with any other node; any vehicle can register its identity to a roadway WAP. Information provided by the vehicles directly to the WAP'S and its collective information stored by the WAPs at a dynamic server database [1].

Making inter communication between the node to avoid accident and journey comfort and safely. From out of network by using sensor vehicles can communicate to the destination. It acts as both server and client. A Vehicular Ad-Hoc Network or VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network. VANET turns every participating vehicle approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. A usual VANET environment is composed of vehicles and infrastructure as shown in Fig. 1. The principal goal of VANET is to grant road safety measures where in rank about vehicle's current speed, location coordinates are passed with or without the deployment of transportation. Vehicular ad hoc network (VANET) establishes a wireless arrangement among the vehicles (V2V) and, on the other level, between vehicles and infrastructure (V2I). VANET is a new tools that connects the vehicles on the basis of a short-range wireless communication [2].For instance, preparatory and ending positions of a private vehicle can often be the address of home and office of a customer. Vehicle-to-vehicle (V-2-V) is an automobile technology deliberate to allow automobile to "talk" to each other. V-2-V relations form a wireless ad hoc network on the roads. Such networks are also referred to as vehicular ad hoc network, VANET's. Vehicular ad hoc network (VANET) is a identity organized network also can define as the fleeting network. Vehicle to vehicle (V-2-V) communication is the main goal of the VANET. In the roadside areas the number of the vehicle may differ according to the traffic stipulation of that particular area. But these vehicles need to communicate with each other for the safety purpose. Suppose a swift vehicle is passing across road and a sudden curve or any hurdle arise there is a great chance of come to blows. If we can give the message to the drive on time then he can react according to the position. And the chances of the accident can be play down. The can be of any type like it should be a encouragement or a voice message or a short message. The aim is it should reach to driver on point. There are several methods for the vehicles to get communicate with each other. VANET only just adopts dedicated restricted communication (DSRC) technology, used for the short range communication purpose. There are six tune-up channels and one control channel. PKI (public key infrastructure) is the current security system person used in V2V communications.PKI is a set of standards, measures, software, and people for implement authentication using open key cryptography. PKI is used to request, install, make up, manage and revoke digital certificates. PKI offers validation via digital certificates, and these digital certificates are signed and provided by certificate powers that be. PKI uses public key cryptography and works with x509 standard certificates. It also provides other effects such as authenticating user, producing and distribute certificates, maintain, managing and revoke certificates. PKI is an infrastructure in which many effects happen and is not a route or algorithm itself, so PKI consists of a quantity of aspects to enable the infrastructure to work. As well as authentication, PKI also enables the use of providing reliability, non-repudiation and encryption. PKI combines well with Diffie-Hellman in providing vulnerable key exchanges, as Diffie-Hellman does not provide validation on its own capabilities. PKI is used in various protocols such as PGP and SSL [5].Two main PKI models are: *Central* – Used for petite to medium sized companies or flat network design. A single clout assigns all their certificates. *Hierarchical* –Hierarchical is used in medium to large organizations. You have a derivation CA, such as Microsoft in house result, or it can be a public trust company such as VeriSign. Then you have separate sub ordinate CA's assigning separate defense domains digital certificates. Hierarchical is a multi tiered approach suited for endeavor networks. Subordinate CA's hand out certificates to employees and added people (systems and being users).

Vehicle-to-infrastructure (V-2-I or v-2-i) is a phone call model that allows vehicles to share information with the components that sustain a country's highway system. Such components include overhead RFID readers and cameras, traffic illumination, lane markers, streetlights, signage and parking meters. V-2-I communication is usually wireless and bi-directional: data from infrastructure gears can be delivered to the vehicle over an ad hoc network and vice versa. Similar to vehicle-to-vehicle (V-2-V) communication, V-2-I uses committed short collection communication (DSRC) frequencies to transfer data. In an intelligent transportation system (ITS), V-2-I sensors can take into custody infrastructure data and provide travelers with real-time advisories about such things as road surroundings, traffic congestion, accidents, construction zones and parking availability. also, traffic management supervision systems can use infrastructure and vehicle data to set variable speed confines and adjust traffic Signal Phase and Timing (SPaT) to raise fuel economy and traffic flow. The hardware, software and firmware that make communication connecting vehicles and roadway infrastructure is an key part of all driverless car initiative.

A credential Revocation List (CRL) is a list of digital certificates that have been revoked by the issue Certificate Authority (CA) before their programmed expiration date and should no longer be trusted. CRLs are a type of blacklist and are used by various endpoints, plus Web browsers, to verify whether a certificate is valid and constant. Digital certificates are used in the encryption process to make safe communications, most often by using the TLS/SSL protocol. The documentation, which is signed by the issuing Certificate clout, also provides proof of the identity of the documentation owner. When a Web browser makes a connection to a site using TLS, the Web server's digital certificate is checked for anomaly or problems; part of this route involves checking that the record is not listed in a Certificate Revocation List. Certificate authority (CA) uses digital signatures to form digital documentation that we use over the internet to authenticate the identity of the person sending data in an IPSec array, and these digital certificates be provided by CA's such as VeriSign. VeriSign would send a certificate to each someone or entity and digitally sign them with their (Verisign's) private key that certifies the authenticity of the user. Certificates are then weighted down and verified by end user's. CA's are the masterminds behind the public key infrastructure (PKI). The CA's digital documentation is created with the CA's private explanation; it's the one that guarantee the authenticity. Some examples of open CA's are VeriSign, RSA, Entrust, Thwarted, and Baltimore.

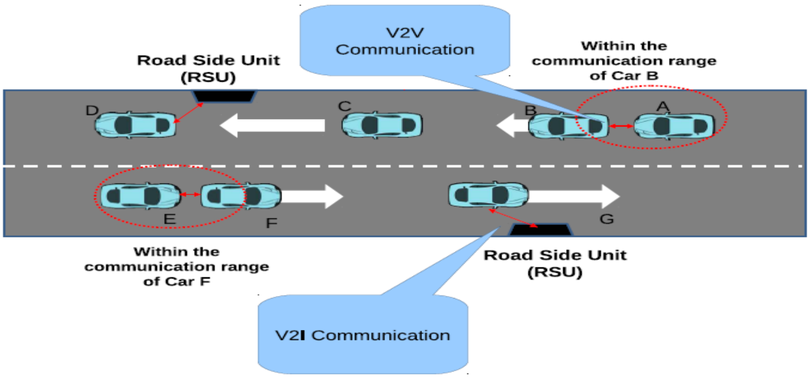

FIGURE 1. Typical VANET constitution.

A typical VANET environment construction is composed of vehicles and infrastructure as shown in Fig. 1. The vehicles communicate both other with the help of vehicle-to-vehicle (V-2-V) communication and with wayside Unit (RSU) with the help of vehicle-to-infrastructure (V-2-I) communication. Each vehicle is set with an On-Board Unit (OBU) that has computational and announcement capabilities.

In this paper, we put forward a hierarchical pseudonymous-based protocol that authenticates a vehicle for the period of the communication with other vehicles in network and provides conditional anonymity. Therefore, unless a vehicle involve in a malicious commotion, it is hard to trace the vehicle. However, in case a cruel activity is detect, the culprit is tracked and subsequently revoked from the network. Our set of rules also supports the sparse RSU deployment. The expiration point of pseudonyms can be adjusted according to the sparse/dense RSU distribution. This paper is the extended version of our groundwork effort [6] and it covers state of the art regarding pseudonymous authentication issues and more detailed investigation with extensive mock-up results.

2. INTERCONNECTED WORK

A number of researchers have put forward their efforts regarding retreat preserving authentication. We can categorize these examine efforts in the pseudonymous-based authentication. the largest part of the pseudonymous-based schemes are implemented with the help of Public answer Infrastructure (PKI). These schemes use PKI base certificates that are attached with corresponding private keys. A pseudo self is attached with a certificate and the relation between the actual identity and pseudonym is known to the donor of pseudonyms which normally is the Certification Authority (CA). In case of detection of a malicious doings, the real identity is revealed by the CA. Reference [7] proposes the concept to develop the security of the cryptographic material stored in a vehicle's OBU. still, these schemes have obvious drawbacks. First, there is considerable communicational and storage operating cost involved during the distribution and storage of thousands of pseudonyms. Secondly, in crate of a revocation, CA needs to retract all the pseudonymous certificates issued to the vehicle and therefore, CRL grows exponentially. Lu et al. [6] propose another conditional retreat preserving protocol where the short time pseudonym keys are acquired by OBU from RSU but the drawback is the best guess of pervasive deployment of RSUs. Another annoyance is the use of trusted authority that needs to frequently modernize RSUs with the CRL. However, this scheme is computationally infeasible as it requires checking that a meaning is from a revoked vehicle. The scheme presented in [16], introduces an interesting idea of using RSUs as crowd managers to maintain and manage the groups of vehicles. The vehicles entering into the rule of a RSU can send anonymous messages that are verifiable by the crowd members of the same group but also verifiable by the vehicles of the next groups. The scheme assumes a pervasive deployment of RSU that share the system load and therefore, the overall show of the system improves. However, the same assumption can also be regarded as a drawback of this scheme payable to the requirement of pervasive exploitation of RSUs acting as group managers.

Xiong et al. [18] use revocable ring signature scheme, wished-for by Liu et al. [19] in order to achieve conditional privacy. However, the revocation in rank must be distributed through revocation lists to all vehicles. Recently, Rajput et al. [20] proposed a fusion scheme that avoids the disadvantages of pseudonymous-based and provides the conditional inscrutability. The authors proposed the idea of grouping vehicles and assign a common key pair to the grouping members. However, this scheme assumes the pervasive exploitation of RSUs. Upon reviewing the literature, we deduce the following margins. Pseudonymous-based schemes incur significant computational, communicational and storage overhead due to the presence of ever on the increase CRL. As the come to of vehicles grows in the network, the CRL grow exponentially. This paper attempts to cater abovementioned issues by proposing the concept of hierarchical pseudonyms. Our proposed protocol neither involves any group executive overhead nor does it require managing any CRL. Moreover, our wished-for protocol does not require full trust of CA, RA and RSU but expects only an honest-but curious activities from these authorities. The CA issues the primary pseudonym as well as keeps the association between the prime pseudonym and the real identity of a vehicle. nonetheless, the real identities in CA's database are encrypted by another entity knows as Revocation say-so (RA) and therefore, CA is unable to decrypt these real identities. Once a vehicle is involved in a malicious activity, appropriate say-so such as LEA allows RA to provide the decryption key in array to decrypt the real identity of the culprit in CA's database. Secondary pseudonyms are issued by RSU upon successful certification of the primary pen name. A vehicle then broadcasts a message signed by the associated private key of the secondary pseudonym and the getting vehicle verifies the message with associated public key provided in the derived pseudonym.

3. K-MEANS CLUSTERING ALGORITHM

K-means clustering aims to division n observations into k clusters in which each observation belongs to the cluster with the nearby mean, serving as a prototype of the cluster. Cluster analysis groups the figures objects based only on information found in data that describes the objects and their affairs. In this paper, we propose K-means clustering [11], mainly aims to show the relationship between the nodes to communicates which is best using both special best ('pbest') and global best ('gbest'),are found to be extremely effective and perform well compared to the already presented methods [12].

Personal best: The personal best position associated with the particle i is the best spot that the particle has visited (a previous value of Xi), yielding the top fitness value for that particle. For a minimization task, a situation yielding the smaller function value is regarded as have fitness. The symbol f(X) will be used to denote the objective utility that is being minimized. The revise equation is

$$\mathrm{p}_{\text{best id}}^{(\mathrm{t+1})} = \{\mathrm{X}_{\text{id}}^{(\mathrm{t})}\ if\ f(\mathrm{X}_{\text{id}}^{(\mathrm{t+1})}) \geq f\left(\mathrm{p}_{\text{best id}}^{(\mathrm{t})}\right)$$

$$\mathrm{p}_{\text{best id}}^{(\mathrm{t+1})} = \{\mathrm{X}_{\text{id}}^{(\mathrm{t+1})}\ if\ f(\mathrm{X}_{\text{id}}^{(\mathrm{t+1})}) < f(\mathrm{p}_{\text{best id}}^{(\mathrm{t})})$$

Global best(g_{best}): The g_{best} offers a faster rate of union at the expense of robustness. This g_{best} maintains only a single best solution called the global best speck, across the entire particle in the swarm. This unit act like an attractor, pulling all the particles towards it. Eventually all particles will converge to this position, so if it is not simplified regularly, the bevy may converge prematurely.

4. ROUTING PROTOCOL

Vehicular Ad hoc Network (VANET), a subclass of cellular phone ad hoc networks (MANETs), is a promising approach for the intelligent transportation coordination (ITS). The design of routing protocols in VANETs is important and necessary issue for sustain the smart ITS. The key difference of VANET and MANET is the special mobility mold and rapidly changeable topology. It is not effectively applied the existing course-plotting protocol of MANETs into VANETs. A routing protocol specifies how routers converse with each other, distributing in rank that enables them to select routes between any two nodes on a computer network. Routing algorithm determine the specific choice of means. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this in turn first among immediate neighbors, and then during the network.To enhances the safety of drivers and provides the comfortable driving environment; communication for different purposes need to be sent to vehicles during the inter-vehicle communications. *Unicast* routing is a deep operation for vehicle to construct a source-to-destination routing in a VANET. *Multicast* is defined by delivering multicast packet from a single font vehicle to all multicast members with multi-hop communication. *Geocast* routing is to deliver a geocast packet to a specific geographic state. Vehicles located in this specific geographic region should receive and forward the geocast packet; if not, the packet is dropped. *Broadcast* protocol is utilized used for a source vehicle sends broadcast meaning to all other vehicles in the network [13].

Broadcast is the last important operation for a vehicle to spread a broadcast significance to all the others in a VANET. For the purpose of comfortable and safe compel for the vehicles, figures can be exchanged among them in the vehicular ad hoc networks. There be bountiful application that have been developed and they depend on the delivery of facts further long distances or in a geographical zone. Routing is about figures packets deliverance starting the starting point to the target over long distance via multihop steps (intermediate nodes). nonetheless, data dissemination refers to data distribution to all of the nodes in a particular zone. The main focus of data dissemination is on the delivery of safety related data to the shelter applications, mainly real-time warning and collision avoidance. One other way of looking at the broadcasting in VANET is to see it as a controlled flooding in the network. Suppose that there is a network with sky-scraping density and in this high density network an event has been detected by the vehicle. Then vehicles try to inform the other vehicles about this event by broad casting the data to them. Now, after there are copious candidates to to the fore and broadcast this data, the overload of the shared wireless channel will occur. as a result there has to be a well-designed forwarding strategy so that the clogging of the wireless conduct will not take place. In addition, the safety letters have the nature of broadcast and the on time availability of them needs to be ensured [14].Hence, in order to pass up the overloading of the channel, the number of unnecessary rebroadcasting desires to be minimized by the adopted techniques of data propagation.

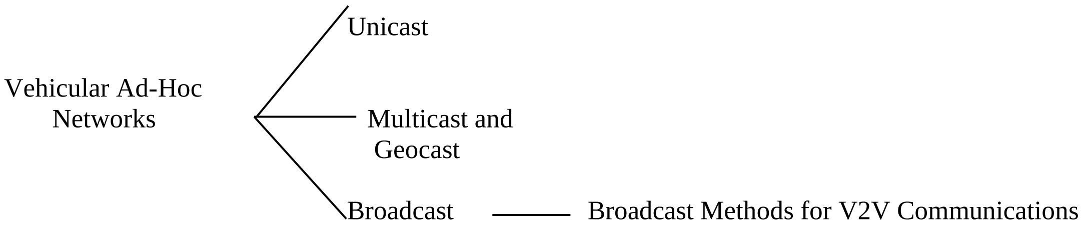
Vehicular Ad-Hoc Networks
Unicast
Multicast and Geocast
Broadcast
Broadcast Methods for V2V Communications

FIGURE 2.The taxonomy of vehicular ad hoc networks

In our proposed method we use the steering protocol is Broadcast Methods for V2V Communications (BMVVC). The primary objective of dissemination in VANETs is to distribute information from a source to many unknown/indefinite destinations. Broadcasting is a necessity for VANETs not only for forwarding but and for delivering information without constructing a data path. The broadcast method for inter-vehicle road and rail network system is to provide emergency information dissemination in VANETs. The purpose of emergency in turn is to announce an urgent event by broadcasting for surrounding vehicle. According to the purposes of emergency information, the proposed broadcast methods in [15]are separated into two categories, *emergency-vehicle-approach* in sequence and *traffic accident* information. Emergency-vehicle-approach information is used to broadcast the urgent event to those vehicles in front of the current vehicle, so the emergency information is only thin ahead. Traffic accident information is used to announce the urgent event to those vehicles following the current vehicle; the emergency information is only disseminated behind. By restraining the broadcast direction, the proposed broadcast methods [16] can provide broadcasts to a finicky area and avoid mistakenly notifying other areas where the in rank is not needed.

5. VEHICLE REGISTRATION AND PRIMARY fictitious name GENERATION

During the registration, sender/initiator vehicle (V_i) generate a random number n (This random value is later encrypted in CA's Paillier public key) and a public/private ECC key twosomePK_i/SK_i. V_i Sends this information along with the VI_i to CA.

Step 1: V_i → CA : n$||PK_i||VI_i$. The V_i sends this in sequence to the CA via some secure channel (for example vehicle visits the CA). Step 1 is required only once.

CA validated theVI_i. Upon proof it encrypts VI_i with one of the public keys generated by RA, encrypts n with its Paillier public keyPK_{CAP}, generated finish time T_{CA} and creates the following database (DB) entries as shown in Table II.

TABLE 2. Example of CA database.

- CA→DB :$(VID_i)_{PK\quad RA}||T_{CA}||PK_i||$n
- CA signs$(T_{CA}||PK_i||(\mathrm{n})PK_{CAP})$, and assigns it to V_i as its first primary pseudonym.

Step 2: $CA \rightarrow\ V_i$: $(T_{CA}||PK_i||(\mathrm{n})PK_{CAP})SK_{CA}$

6. RE-ACQUIRING PRIMARY PSEUDONYM

Once the T_{CA} expires, V_i needs to acquire the chief pseudonymagain. In this regard, V_i randomlyselectsome, n' generates a public/private ECC key pair $PK''_i|SK''_i$, encrypts this data in public enter of CA along with n and sends it to CA using 3G/4G communication.

Step 3: $V_i \rightarrow \text{CA}: (\text{n}||\text{n}'||PK''_i)PK_{CA}$

In case, the vehicle requests the re-acquiring of primary pseudonym to CA via RSU next it sends this message to the nearby RSU that forward this request to the CA. For such a request, some special purpose bits in the message can be used that enable the RSU to identify that a vehicle is requesting for primary pseudonym via RSU or the vehicle is request the RSU for a new secondary pseudonym.

Step 3': $V_i \rightarrow \text{RSU} \rightarrow \text{CA}: (\text{n}||\text{n}'||PK''_i)PK_{CA}$

CA verifies this message with correct n, generates new expiration moment $T_{CA'}$, update its database with new values of n', PK''_i and the $T_{CA'}$. CA repeats step 2, but encrypts the just now generated primary pseudonym in PK''_i and sends back to V_i. In case, the appeal has come from RSU then CA sends this message to V_i through RSU along with the signed n. The signed value of n creates an association with the newvalue of n'. When the RSU televise this message, V_i identifies it with old n, verifies CA's signature, decrypt it and changes its key pseudonym. Due to encryption, RSU is unable to relate the new primary pseudonym to the V_i.

Step4: $\text{CA} \rightarrow: V_i \left(\left(T_{CA'}|PK''_i||(\text{n}')\right)PK_{CAP}\right)SK_{CA}PK''_i||(\text{n})SK_{CA}$

7. SECONDARY PSEUDONYM GENERATION

RSU periodically broadcasts a message announcing its being there. This message also contains the public key of the RSU. Once a vehicle receives this message it apply for for the less important pseudonym. The vehicle generate a new public/private ECC key pair (PK'_{i}, SK'_i). It encrypts this newly generated public key, its primary pseudonym, -n and a nonce in RSU's municipal key and sends it to the RSU.

Step5: $V_i \rightarrow \text{RSU} \; (\left(T_{CA}||PK_i||(\text{n})PK_{CAP}\right)SK_{CA}||PK''_i|| - \text{n}||\text{nonce})PK_{\text{RSU}}.$

RSU verifies CA's signature, encrypts –n with Paillier public key of CA. RSU takes homomorphic sum of both $(n)PK_{\text{CAP}}$ and $(-n)\text{PK}_{\text{CAP}}$, gets $(R)\text{PK}_{CAP}$. Where $(R)\text{PK}_{CAP} = (n)PK_{\text{CAP}} + (-n)\text{PK}_{\text{CAP}}$

RSU sends $(R)\text{PK}_{CAP}$ to CA for verification.

Step6: $\text{RSU} \rightarrow \text{CA}: (R)\text{PK}_{CAP}$

CA decrypts R, finds 0 (n+ (−n) = 0) and sends verified message to RA otherwise sends not verified.

Step7: CA → RSU: verified / not verified.

CA only gets a encrypted value that provides no hint about which vehicle is using this value. The value of –n is used to prevent an impersonation attack.

Upon getting verification that the message came from V_i RSU prepares a inferior pseudonym. It creates the expiration time T_{RSU}, embed it by way of newly generated PK'_i, signs it, encrypts in PK'_i and sends it to V_i. Note that, PK'_i has to be generate by V_i every tine a secondary pseudonym is requested. However, a vehicle can pre-compute a pool of ECC key pairs.

Step8: $\text{RSU} \rightarrow V_i: ((T_{RSU}||PK'_i)SK_{RSU})PK'_i.$

8. PERFORMANCE EVOLUTION

In this case, RSU verifies the primary pseudonym contains in the demand and then generates and sends the secondary pseudonym to the requesting vehicle. Therefore, it is vital to verify that the RSU is able to perform this task on a consistent basis whereas serving a number of vehicles. The simulation results are discuss as under:

(i) PACKET DELIVERY RATIO (PDR)

Packet delivery ratio is defined as the share of packets successfully delivery to the total sent packets.

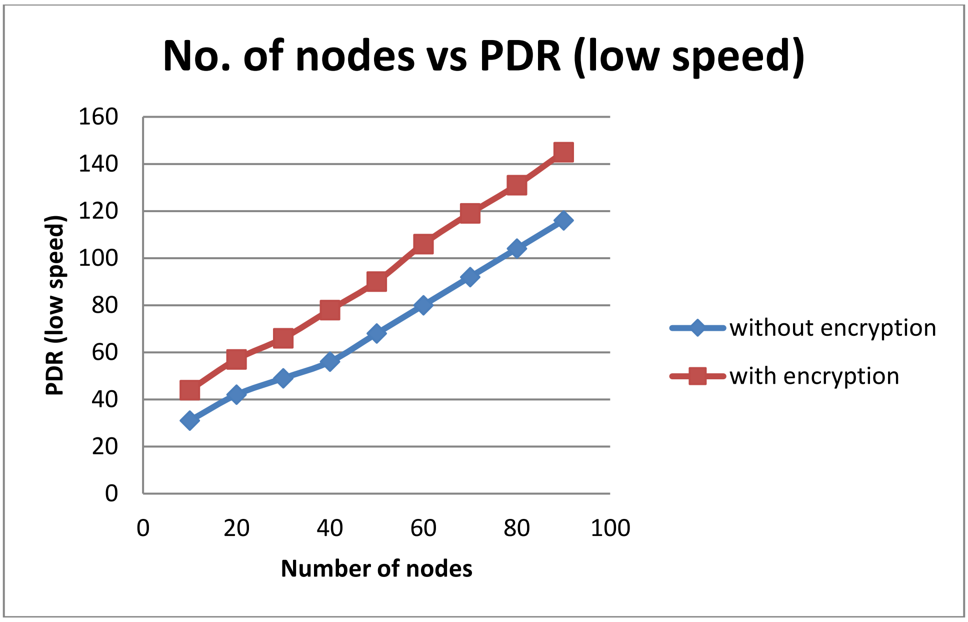

Fig. 4(a)PDR (low speed)

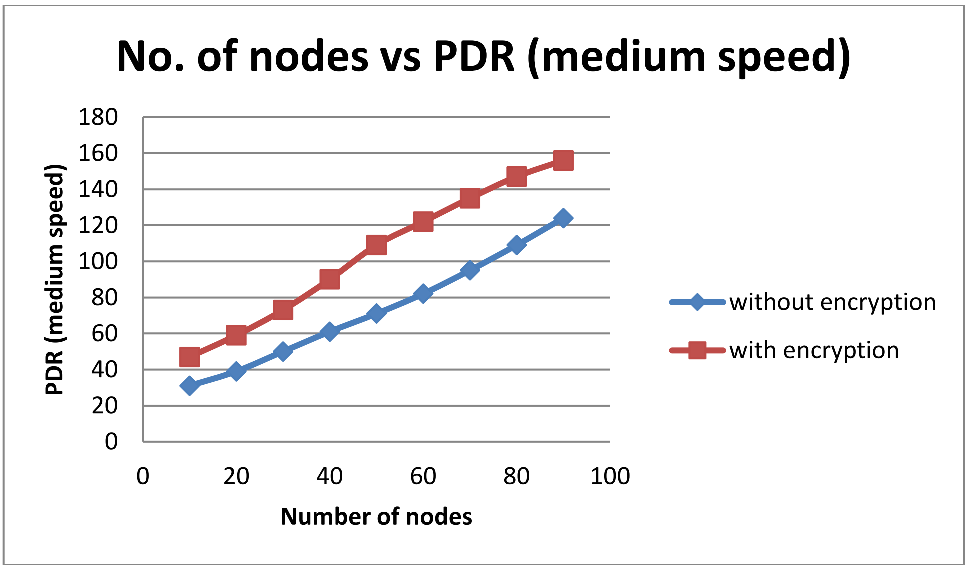

Fig. 4(b)PDR (medium speed)

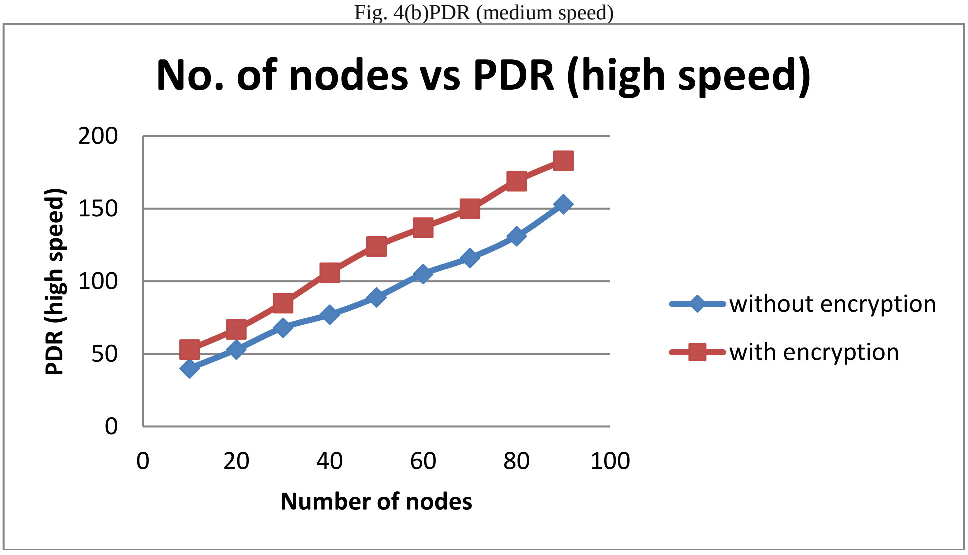

Fig. 4(c)PDR (high speed)

FIGURE 4. PDR w.r.t speed (a) PDR (low speed). (b) PDR (medium speed). (c) PDR (high speed).

Inthe above Fig. 4. Fig. 4(a) shows the PDR for measured moving vehicles. Here we observe near 100% packet delivery ratio for out of bed to 30 vehicles and after that the gap gradually starts to expand. When the number of vehicles increase to 70, the difference in PDR starts to get significantly higher. This is due to the basis that, as the number of vehicles increases, the slow moving vehicles tend to get quicker and the number of vehicles per unit area increases. The encrypted packets that reside in more bandwidth start to drop more than those without encryption. We examine the PDR for medium and high speed vehicles in Fig. 4(b) and 4(c) in that order. When the number of vehicles reaches to 30, the encryption will increase. on the other hand, from 50 vehicles upwards, this difference observed to be remains constant.

9. CONCLUSION

This paper proposes an efficient authentication protocol next to with enhancing security. The main parts of this paper include an indication of VANETs and K-means clustering, Pseudonym authentication. The current research challenge of VANETs broadcasting protocols are focused on issues such as broadcast method for V2V communications. The security analysis of our proposed protocol exhibits the elasticity against various security threats. Furthermore, the performance appraisal of our proposed protocol not only shows the computational and communication overhead. Routing protocol and ECC model implies the security; we minimize the delay and maximize the sanctuary and appropriate performance.

REFERENCES

[1] ‘‘Comprehensive survey on security services in vehicular ad-hoc networks,’’ by M. Azees, P. Vijayakumar, and L. J. Deborah, IET Intell. Transp. Syst., vol. 10, no. 6, pp. 379–388, 2016.

[2] ‘‘Challenges in securing vehicular networks,’’ by B. Parno and A. Perrig, in Proc. 4th Workshop Hot Topics Netw. (HotNets), 2005, pp. 1–6.

[3] ‘‘Securing vehicular ad hoc networks,’’ by M. Raya and J. P. Hubaux, J. Comput. Secur., vol. 15, no. 1, pp. 39–68, 2007.

[4] ‘‘Certificate assignment strategies for a PKI-based security architecture in a vehicular network,’’ by B. Bellur, in Proc. IEEE GLOBECOM, 2008, pp. 1–6.

[5] ‘‘MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular socialnetworks,’’ by R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing,IEEETrans.Depend.Sec.Comput.,vol.13, no. 1, pp. 93–105, Jan./Feb. 2016.

[6] ‘‘A two level privacypreservingpseudonymousauthentication protocol for VANET’’ by U. Rajput,F. Abbas, H. Eun, R. Hussain, and H. Oh, in Proc.IEEE Int.Conf. Wireless Mobile Comput., Netw. Commun. (WiMob), Oct. 2015, pp. 643–650.

[7] “Securing vehicular communications”, by M. Raya and J. Hubaux, IEEE Commun. Lett. Vol. 13, no. 1, pp. 8-15, Oct. 2006.

[8] ‘‘The security of vehicular ad hoc networks’’ by M. Raya and J. Hubaux, in Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw., 2005, pp. 11–21.

[9] ‘‘Securing vehicular communications’’ by M. Raya, P. Papadimitratos, and J. Hubaux, IEEE Wireless Commun. Lett., vol. 13, no. 1, pp. 8–15, Oct. 2006.

[10] ‘‘An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications’’ by Y. Sun, R. Lu, X. Lin, and X. Shen, IEEE Trans. Veh. Technol., vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

AUTHOR PROFILE

Dr.G.Revathy is working as Assistant Professor in Department of Computer Science and Emgineering
At Erode Sengunthar Engineering College,(Autonomous) Erode. Her area of research includes Wireless Networks and Artificial intelligence.

Ms.P.Logeshwari is working as Assistant Professor in Department of Computer Science and Emgineering At JKKM, College of Technology, Gobi. Her area of research includes Wireless Networks and IoT.

Mr.D.Vijaybabu is working as Assistant Professor in Department of Computer Science and Emgineering At Erode Sengunthar Engineering College,(Autonomous) Erode. His area of research includes software engineering and data mining.

Mr.M.Sivakumar is working as Assistant Professor in Department of Computer Science and Emgineering At Erode Sengunthar Engineering College,(Autonomous) Erode. His area of research includes Cloud computing and Big data.