International Journal of Engineering & Technology, 7 (3.6) (2018) 216-222

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Efficient Multilevel Privacy Preserving Authentication Scheme for Emergency Message Communication in VANE

G. Santhana Devi[1*], M. Germanus Alex[2]

[1]Research Scholar, Research & Development Centre, Bharathiar University, Coimbatore, Tamilnadu.
[2] Kamarajar Government Arts College, Surandai, Tirunelveli (Dist), Tamilnadu.
**Corresponding Author E-Mail:Sandal.Devig@Gmail.Com*

Abstract

Vehicular ad hoc networks (VANETs) provide spontaneous traffic related and emergency rescue messages to its users of the route thereby enable them with the trouble-free driving. VANETs send emergency messages in times of exigencies that save people's lives from disasters. Doing such times it has been a great challenge to ascertain the authentication and privacy of the messages that are broadcasted. Generally when the messages are broadcasted without accommodating privacy the confidential information's like the vehicle's id and location are exposed which adversely affect the users. In this paper to ensure privacy to the users we have recommended TA to provide a verification signature to all the vehicles which is mandatory for a vehicle for all its communication purpose. Normally in the existing schemes, the messages are provided with single level or bi level privacy features but, in the proposed scheme the emergency messages are provided with the multilevel privacy features. In the proposed scheme the TA provides a long term Verification signature which is mandatory to all the vehicles that are registered under VANET and this signature is also necessary in receiving the secondary token and common token from RSU at each interval of time. The authentication of the message is verified with the help of common token and encrypted common token as a RSU Verification signature. Since the emergency messages require secure, timely and factual communication our proposed protocol EMPPA scheme recommend the distribution of multiple verification signatures and tokens at various interval of time, so that the privacy, security and the authentication of messages are ensured to the VANET users.

Keywords: *Authentication, emergency message, multilevel privacy, token, VANET.*

1. Introduction

In our day today life the road traffic has become one of the major distresses. Vehicular ad-hoc network provides an ideal transportation system to the world. It is one of the secondary divisions of mobile ad-hoc network. Generally the VANET architecture shown in Fig: 1 has three key elements, namely the Trust Authority (TA), Road Side Units (RSUs) and Vehicles. The vehicular network has two kind of communications namely vehicle to vehicle communication (V2V) and vehicle to infrastructure communication (V2I). In VANET Intelligent Transportation System (ITS) and the DSRC system provide secure and reliable communication between vehicles and RSUs. [2]. In VANET each vehicle regularly broadcast traffic related messages containing vehicle's id, speed, location and direction etc., to the other vehicles with in the communication range.

The Vehicular ad hoc network provides a numerous applications to users. These applications are generally categorized into two major types namely safety applications and non safety applications. The main aim of the safety applications is to provide early warning to the users to avoid accidents on the road. Such applications issue [3] traffic signal warning, emergency break warning, crash warning, hazard notification and collision warning. In addition there are safety applications that are necessary after the assurance of a disaster or accident to send the emergency message to nearby emergency rescue team. These applications also facilitate the fast and secure message dissemination. The non safety applications provide some useful information to the drivers and the passengers. Such applications inform about the weather condition, traffic and the location of nearest restaurants, gas stations or petrol bulk. Furthermore it presents entertainment applications to the users like media downloading and online games.

Unfortunately if any emergency event occurs, the emergency message is transmitted to the other vehicles and RSU in the vehicular network. In such times various challenges are met like determining authentication and privacy of messages such as privacy for message and location of the vehicle. In the recent years, various authors have proposed privacy preserving authentication schemes for secure message communication. The two most common privacy preserving authentication schemes are the pseudonyms based privacy preserving scheme [4-12, 22, 24], the group signature based privacy preserving scheme [13-17]. Each scheme provides solution to the secure privacy preserving message communication problems in VANET but all of them have some drawbacks.

In the pseudonyms based scheme, the vehicles should contain a large number of pseudonyms in the vehicle's OBU. Hence high memory is required. The malicious vehicles details are put in CRL (Certificate Revocation List). When the counting of malicious vehicles increases, the size of the CRL also increases. This result is CRL overhead problem.

In the group signature based schemes, the vehicles continuously join and leave the group. The group leaders know the entire details of the group members. So group leader's selection is one of the significant challenges. In addition each message is signed with

vehicle's own private key and the message verified with the groups public key. These operations require a lot of pairing calculations.

In the proposed protocol, an efficient and multi level verification signatures and tokens based authentication of vehicle is implemented for secure emergency message communication with other vehicles and RSU in the vehicular network. In this system, registration is mandatory to all the vehicles that all the amenities are provided only to registered vehicles. The registered vehicles update their recent location to trust authority server in a secure manner. During the registration each vehicle receives encrypted primary token as a TA verification signature from trust authority, which is used to gets secondary token and common token from RSU. If the vehicles use their true identity for communication, the adversary vehicles could easily track down the vehicle's location. Therefore the vehicle's location and message privacy is essential during the emergency message communication. Hence this scheme suggests the registered vehicles to use TA verification signature for communication, to protect vehicle identity and vehicle location from an adversary.

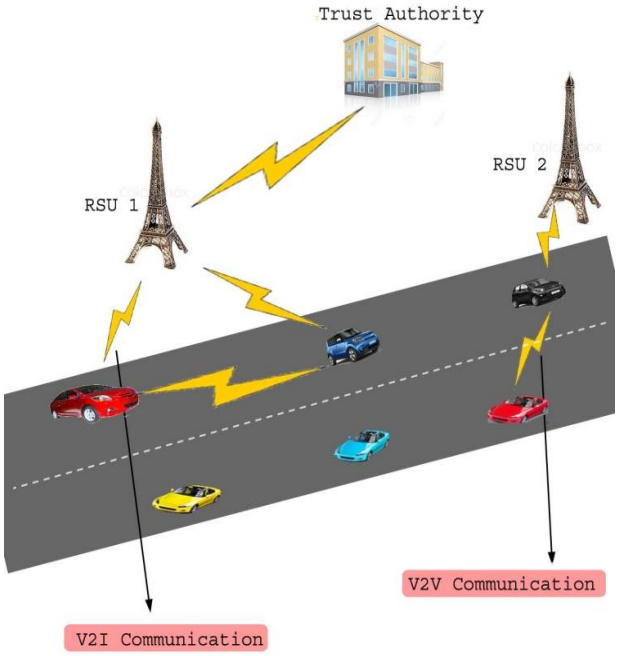

Fig. 1: VANET architecture

If the malicious vehicles broadcasting fake messages in VANET are left undetected it may cause distress to the vehicle and the driver. Hence the message authentication is obligation for a secure emergency communication. By this process only the legitimate vehicles can exists in the network and the malicious vehicles are prevented from entering into the VANET. In the proposed scheme authentication of vehicle is verified based on a multilevel token and signature during the emergency message communication. In this scheme RSU provide two types of tokens namely secondary token and common token which are used for multilevel authentication. The first level authentication is performed at the time of vehicle to vehicle communication and second level authentication is performed during the vehicle to RSU communication. During the first level of authentication, the receiving vehicle legalizes the common token of the sender vehicle by comparing it with that of itself. If the legalization is success, the message is forwarded to next-hop vehicle or else sent the report message about the sender vehicle to RSU. At the second level of authentication, the RSU verify encrypted common token i.e., the RSU verification signature with, with that of secondary token of the regarding vehicle. If the verification is success the message is forwarded to trust authority or else the message gets discarded.

Whenever the malicious vehicle is discovered, immediately the TA informs to the RSU to updates the current session common token and the corresponding vehicle's secondary token. Subsequently if necessary, the trust authority may update the primary token of the corresponding vehicle. In addition to accomplish vehicle location privacy, the common token and secondary token are vary in each RSU session and these tokens are updated regularly.

Message dissemination routing of this paper is based on [19] our previous paper, which provide fast emergency message dissemination. In the proposed scheme, we additionally included security to provide secure location privacy to the vehicles that involve in emergency message communication. The major contributions of this work as follows

- The trust authority TA provides primary token as a TA verification signature to the vehicle at the time of registration. These are essential to obtain secondary token and common token at the all RSU session. The TA is trustworthy. It has all the details of a registered vehicle and the corresponding primary token.
- In each session, RSU provides secondary token and common token to the registered vehicle, which is used for emergency message communication and also is used for authentication. The first level authentication is performed during vehicle to vehicle communication using common token and second level authentication is performed during vehicle to RSU communication using encrypted common token.
- Apart from this the tokens are updated in diverse time such that each RSU's common tokens are updated in a minimum period, secondary tokens updated in a average period and primary token updated in a long period. Furthermore when a malicious vehicle is invented, the corresponding registered vehicle's tokens are updated by TA and RSU.
- For each communication all the registered vehicles use TA verification signature and RSU verification signature along with the current session common token. This provides location privacy and authentication to the communicating vehicles.

2. Related Work

The vehicle location privacy preserving is a most significant concept of emergency message communication in VANET. It is commonly separated into two types: the pseudonyms based privacy preserving scheme and the group signature based privacy preserving scheme. In pseudonyms based scheme, all vehicle broadcasts message with its pseudo ID rather than its real ID; it is used only in certain circumstances generally to hide an individual's original identity. Therefore the malicious vehicle cannot detect the vehicle's location. If the malicious vehicle is traced out, it is inserted to the CRL during communication the vehicles confirm the CRL list for message authentication. Since the CRL List is incredibly bulky, the time delay occurs in this system of message authentication.

In [4] Raya et.al, have proposed of securing vehicular ad-hoc networks based on pseudonymous scheme, in which pseudonyms are used to hide the real identities of the vehicles. The pseudonyms have only a short life, so the vehicles should contain a large number of pseudonyms in the vehicle's OBU. Hence high storage space is required by the vehicle's OBU. This is not possible in a highly dynamic vehicular network. In the pseudonyms based scheme, if the adversary vehicle is detected the details of that vehicle and its certificates are added in CRL (Certificate Revocation List). Each vehicle receive message, after the verification of CRL. However when the number of malicious vehicles increases, the CRL Size also increases. Therefore it takes more time for verification. In [5] provides conditional privacy

preservation. In this scheme the vehicles use pseudonyms to communicate with the RSU, which ensure privacy to the users. In [6] , Zhang et.al., addressed identity based batch signature verification [7] scheme. In this scheme RSU verifies multiple signatures at the same time so that it reduces the verification time. In [8] Pandurang et.al, have presented an identity based security framework for vanets. It provides security and privacy using short lived pseudonyms. In this scheme the authors have addressed the implicit authentication. This eliminates the need of CRL and certificate exchange. The merit of the scheme is that it does not require any special storage space in vehicle or the RSU for each pseudonym. Each message contains source node and the destination node pseudonyms along with signature that is required for any agreement. *In [9]* Rongxing Lu et.al, proposed an efficient conditional privacy preservation (ECPP) protocol in VANET. It creates on-the-fly there by authentication of message and privacy enhancement are short-time anonymous keys between OBU and RSU, accomplished in a rapid process at the same time it reduces the required storage space. The merits of the scheme are reduction of the storage space of anonymous keys in OBU, fast verification of safety messages and efficient privacy preservation. [10] Rajput et.al., presented A Two Level Privacy Preserving Pseudonymous Authentication Protocol for VANET. This protocol uses two types of pseudonyms namely as primary pseudonyms and short time pseudonyms. It provides privacy security only to genuine users. The malicious user's identity is revealed by the law enforcement authority.

In [11] Libing et.al, have proposed an efficient location-based conditional privacy-preserving authentication scheme, which use the location information to assign vehicles' partial secret keys. The vehicles sign messages with unrelated pseudonyms to hide its real identity. This scheme functions without using any special device, like ideal TPD. In [12] 2FLIP Authentication Scheme for VANET is addressed which implements two-factors called MAC and hash operation in authentication process within the VANET for improving secure privacy. In this scheme, each vehicle is endorsed with a telematics device which is utilized along with the biometric technology equipped on this vehicle.

In the group based scheme each vehicle anonymously send message with secret member key. The receiving vehicle can verify the message with group public key, however no vehicle can identify the identity of the sender vehicle except the group manager. Chen xi et.al., have presented [13] novel message authentication scheme named RAISE, which creates RSUs in charge of validating the authenticity of messages sent from vehicles and for reporting the result back to vehicles. In addition there is a proposed scheme named COMET, which works in the absence of RSU. In this scheme the vehicles verify the group of message signatures based on their capacity. In [14] authors Lin et.al, Presented protocol named GSIS, which executes privacy preservation based group signature and identity signature. In this scheme the CRL size is reduced. In [15] Zhang et.al., presented a scalable robust authentication protocol for communication. In this scheme each RSU maintains a group within its communication range. Every vehicle entering the group can broadcast message to nearest vehicle which can be immediately verified by the vehicles in the same group or nearest group. In this scheme the RSU must envelope all the roads otherwise it may not be suitable. The authors Lu et al., have proposed an efficient conditional privacy preservation (ECPP) protocol in vehicular ad hoc networks (VANETs). This scheme accomplishes fast authentication and efficient privacy with the short time anonymous keys. This keys are used between vehicle's OBU and RSU. In [16] Zheng et al., proposed two centralized group key management protocols based on the Chinese Remainder Theorem (CRT). The merit of these protocols is that the re-keying computation is done easily. As a user-join or leave from the group, the key server provides a very short key. In [17] author vijayakumar et al., introduced Centralized key distribution protocol using the greatest common divisor method. The protocol focuses on two dimensions. First one generates secured dynamic keys generation and performs updating process with some simple multiplication process and another one dimension is reducing the amount of storage space.

All the above schemes have their own advantages but with some limitations. None of them provide a secure location preserving emergency message communication for highly dynamic vehicular ad-hoc network. In this paper, we propose the efficient location preserving multilevel authentication scheme for emergency message communication in VANET.

3. Preliminaries

The following subdivisions give details of the system model used in the proposed protocol EMPPAS.

System Model

In the beginning, each vehicle is individually identified by its vehicle register Number [The Number obtained by the vehicle by registration under RTO]. In our proposed protocol the vehicle sends their vehicle register Number to the TA and receives the primary token and the TA verification signature from the TA. This TA verification signature and primary token are installed in vehicle OBU. The contributors to the proposed protocol EMPPAS are:

TA

The Trust authority acts a extremely essential role in authentic communication in VANETs. The TA allocate Primary token with the expiry time $V_i(P_{tk\_exp})$ to all the vehicles at the time of registration under VANETs. The TA also provides the TA verification signature $V_i(TA_{Sign})$ to the registered vehicles and keeps the Vehicle Number under privacy. The vehicle details are obtained by the TA is stored in the TADB. Once the Primary token gets expired or the vehicle owner changes, the vehicle requests for new primary token from the TA.

RSU

The TA substitutes several RSUs that are placed along the road side and these RSUs are directly monitored and managed by the TA via secure wired or wireless link. Each RSU has a distinctive identification. These identification details like its id, location are stored in the TA's database. The RSU's calculation and storage power is superior than the vehicle's OBU. The RSU provides the current session Common token and Secondary Token to the vehicles in its communication range.

Sender vehicle

The sender vehicle denoted as V_i. It sends the emergency message along with the TA verification signature and RSU verification signature.

Receiver vehicle

The receiver vehicle is denoted as V_j. It confirms the message with the current session common token. If in case the message sender is found to be fake then the receiver vehicle send a complaint message regarding this to the RSU, with annexing the corresponding vehicles' TA verification signature.

4. Proposed Model

This part provides the detail on the proposed EMPPA Scheme, which is efficient for the secure emergency message communication in VANET. In this scheme all vehicle are

mandatory register their details at the time of joining in the vehicular ad-hoc network. After the registration, the registered vehicles get the primary token and the TA verification signature from the trust authority. The register vehicles exploit the TA verification signature for message communication with the RSU. In addition each vehicle's primary token and TA verification signature are used to obtain the secondary and common tokens from the RSU. Both secondary and common tokens are employed for message communication.

The Table -I below acquaint you with the most commonly used terms and how they are denoted in this paper.

Table I: Notation

Notation	Description
V_i	Sender Vehicle
V_j	Receiver Vehicle
P_{tk}	Primary Token
S_{tk}	Secondary Token
C_{tk}	Common Token
$V_i(P_{tk\_exp})$	Expiry Time of Primary Token in Vehicle V_i
$V_i(S_{tk\_exp})$	Expiry Time of Secondary Token in Vehicle V_i
$V_i(C_{tk\_exp})$	Expiry Time of Common Token in Vehicle V_i
$M(Tk_{req})$	Token Request Message
$M(R)$	Report message [Vehicle or RSU trace any malicious vehicle inform to RSU or TA through Report message.]
$E( )$	Encryption
$D( )$	Decryption
$M(Sign_{verify})$	Signature verification Message
$V_i(TA_{Sign})$	$E(V_i(ID))_{V_i(P_{tk})}$
$V_i(RSU_{Sign})$	$E(V_i(CT))_{V_i(S_{tk})}$

The proposed scheme is comprised of five phases namely vehicle registration and primary token distribution phase, secondary token distribution phase, vehicle to vehicle message broadcast phase, vehicle to RSU message broadcast phase and token updating phase.

System Parameters

Bilinear pairings

In the ID-based cryptography (IBC), the communal characteristics information such as id, phone number are used as a public key, which overtake the certificate used for the public key verification [20]. The bilinear pairings on elliptic curves utilized to the ID-based encryption scheme [21]. Let *G* be an additive group created by *X*, with order prime n, and G_m be a multiplicative group with the same order of *n*, where *n* is the large prime. The G and G_m are complicated in DLP. The X is the generator of *G* and *e (X, Y)* is the generator of G_m

Let $\hat{}e: G \times G \rightarrow G_m$ is bilinear map between these two groups .The map should assure the following three properties:

i)*Bi-linearity*: $e(aX, bY) = e(X,X)^{a\,b,}$ Such that, $\forall (X,Y) \in G$ and $\forall (a,b) \in Z^*_n$

Such that Z^*_n is a multiplicative group of Z_n, n is the integer modulo. In particular,

$Z^*_n = \{x | 1 \leq x \leq p-1\}$ since p is prime.

ii)Non-degeneracy: $\forall X,Y \in G$, such that $e(X,Y) \neq 1$

iii)Computability : e is efficiently computable. Compute $e(X,Y)$, $\forall X,Y \in G$

Cryptographic hash function

$H\{M,T\} \rightarrow E\{M\}_T$

Let M be a message, the key T is generated by bilinear Pairings and output $E(M)_T$ is the encrypted message.

Parse M as $M_1||M_2||M_3||\ldots\ldots M_n$ *where n is the length of the M*

for i=1 to n

$V = M_i \bmod T$

$E(M_i)_T = (M_i << V) + V) \% 128$

Vehicle Registration and Primary Token Distribution Phase

During the registration vehicle V_i sends its vehicle details [Vehicle Number, chassis no, vehicle model, manufacturer's name, etc.,] and the owner details [owner name, address, email id, phone no, etc.,] to the trust authority TA.

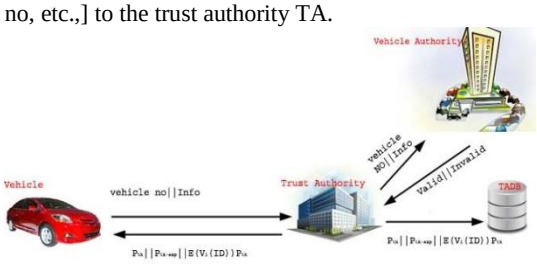

Fig. 2: Vehicle registrations

Step: 1

$V_i \rightarrow TA$: V_i *(Vehicle Number)* || V_i *(Vehicle Info)* || V_i *(Owner Info)*

The trust authority verifies the vehicle V_i details and its owner details with the Vehicle's Manufacturer or RTO. If the details are correct, TA generate primary token $V_i(P_{tk})$ and the expiry time $V_i(P_{tk\_exp})$ to the vehicle V_i.. The primary token generation procedure is explained as follows.

The TA selects an arbitrary $P \in G^*$, and selects a random integer $k \in Z^*_n$.

$H_n = e(P,P)^k$, $V_i(P_{tk}) = H_n$ ___*(1)*

After generating primary token, the TA encrypts the vehicle V_i Number with its primary token $V_i(P_{tk})$

$V_i(TA_{Sign}) = h(V_i$ *(Vehicle Number),* $V_i(P_{tk}))$

Finally, the Trust authority saves the registration details and TA verification signature in the trust authority database [TADB], which is trust worthy. The database TADB entries are shown in Table II.

Step: 2

$TA \rightarrow TADB$: $V_i(TA_{Sign}) || V_i(P_{tk}) || V_i(P_{tk\_exp})$

Table II: Trust Authority Database

User No	Data
u1	$V_i(TA_{Sign}) \| \| V_i(P_{tk}) \| \| V_i(P_{tk\_exp})$
…	…
…	…

Subsequently the TA sends a primary token $V_i(P_{tk})$ with its expiry time $V_i(P_{tk\_exp})$ and TA verification signature $V_i(TA_{Sign})$ to the registered vehicle V_i.

Step: 3

$TA \rightarrow V_i$: $V_i(TA_{Sign}) || V_i(P_{tk}) || V_i(P_{tk\_exp})$

Secondary Token Distribution

When the Vehicle enters a new RSU coverage, the system automatically sends a secondary and common token request message along with the TA verification signature $V_i(TA_{Sign})$to the RSU. The secondary token and common token have different period for expiry. The common token has the expiry period shorter than the secondary token. When common token expires the RSU automatically updates and distributes the new common token to all vehicles in its communication range. As when the vehicle enters an another new RSU coverage, at this time If the vehicle already has an valid secondary token, it continues with the same secondary token otherwise the system routinely send secondary token requests message to the RSU.

Step: 4

$V_i \rightarrow RSU_j$: $V_i(TA_{Sign}) || M(Tk_{req})$

As the RSU Receives the token request message from the vehicle V_i. It sends TA verification signature $V_i(TA_{Sign})$ of the requesting vehicle to the Trust authority for verification.

Step: 5

RSU → TA: $V_i(TA_{Sign})$ ||M(Sign $_{verify}$)
After receiving the signature verification message [M(Sign$_{verify}$)] from RSU$_j$, TA verifies the vehicle V_i 's, verification signature $V_i(TA_{Sign})$ and current location with TADB database .During the verification, if the vehicle Vi 's verification signature is correct and if its current location is closely associated with the most recently updated TADB location, then the TA sends an approval message to RSU otherwise TA sends a invalid message of its disapproval to RSU.
Step: 6
TA → RSU: Valid/Invalid
If the RSU receives an approval message from the TA, then it generates secondary token $V_i(\mathbf{S_{tk}})$ to the vehicle V_i .After the secondary token is generated the RSU saves a copy of the vehicle V_i 's TA verification signature $V_i(TA_{Sign})$, secondary token $V_i(\mathbf{S_{tk}})$, common token $V_i(\mathbf{C_{tk}})$ and their short expiry periods $V_i(S_{tk\_exp})$, $V_i(C_{tk\_exp})$ in its RSU database and subsequently they are sent to the Vehicle V_i by the RSU.
Step: 7
RSU → DB: $V_i(TA_{Sign})$|| $V_i(S_{tk})$ || $V_i(S_{tk\_exp})$ || $V_i(\mathbf{C_{tk}})$ || $V_i(C_{tk\_exp})$
Step: 8
RSU → V_i: $V_i(TA_{Sign})$|| $V_i(\mathbf{S_{tk}})$ || $V_i(S_{tk\_exp})$ || $V_i(\mathbf{C_{tk}})$ || $V_i(C_{tk\_exp})$
The vehicle use separate tokens for each RSU coverage. Since in the separate token system, the true identity of the vehicle is kept secure and TA verification signature is used for message communication. So the communicated vehicles, with the intermitted location link it is not possible for any adversaries to track down the location of the vehicle. There by the privacy of the registered vehicles are assured by the VANETs. When the vehicle $V_{i's}$ secondary token expires, the RSU automatically removes this vehicle data from its database. If later that, vehicle enters this RSU coverage, it will request for a new secondary token from this RSU.

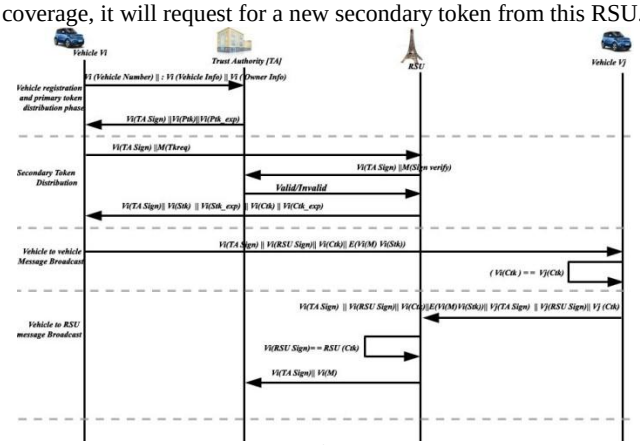

Fig. 3: Working of proposed protocol

Vehicle to Vehicle Message Broadcast

While the RSU is available within the vehicle V_i's communication range, the vehicle directly sends a emergency message to RSU. Otherwise vehicle V_i send a message through intermediate vehicle using vehicle to vehicle communication.
In vehicle to vehicle communication vehicle privacy and message authentication are necessary. The vehicle privacy is assured in this mode of communication. Since the sender vehicle always sends the message with the duplicate Id along with trust authority verification signature $V_i(TA_{Sign})$. The communicating vehicle's authention is ensured by their Common Tokens C_{tk}. The sender vehicle V_i broadcasts the message with the trust authority verification signature $V_i(TA_{Sign})$,Common Token $V_i(\mathbf{C_{tk}})$ and RSU verification signature $V_i(RSU_{Sign})$ to the next-hop vehicle in its communication range.
Step: 9
V_i → V_j : $V_i(TA_{Sign})$ || $V_i(RSU_{Sign})$|| $V_i(\mathbf{C_{tk}})$|| E(V_i(M) $_{V_i(S_{tk})}$)
After receiving the message, the receiver vehicle V_j verifies the common Tokens of the both sender and receiver vehicles.
Step: 10
V_j : If ($V_i(\mathbf{C_{tk}})$ = = $V_j(\mathbf{C_{tk}})$)
During the above verification, if the common tokens are same, the receiver vehicle V_j identify that the message has come from an authenticated vehicle and thereby the receiver vehicle V_j broadcast the message to nearest vehicle until the message reaches RSU and if the common tokens are different the receiver vehicle V_j sends a report message M($V_{i\,Report}$) about the sender vehicle V_i to the RSU.

Vehicle to RSU Message Broadcast

If the RSU is within vehicle V_j's communication range, the vehicle V_j sends a message directly to the RSU.
The RSU receives two types of messages from the vehicles. First one is the regular emergency message M($V_{i\ emergency}$) and the another one is the Report message M($V_{i\,Report}$).
In case the RSU receives regular emergency Message
Step: 11
V_j → RSU : $V_i(TA_{Sign})$ || $V_i(RSU_{Sign})$|| $V_i(C_{tk})$||E(V_i(M)$_{V_i(S_{tk})}$)|| $V_j(TA_{Sign})$ || $V_j(RSU_{Sign})$|| V_j (C_{tk})
Step: 12
RSU: If ($V_i(RSU_{Sign})$= = RSU (C_{tk}))
In case of receiving the regular emergency message, if the above verification is valid, then the RSU forwards the emergency message to the TA otherwise the RSU sends a report message about the vehicle V_j to the TA.
When the RSU receives report message, then it verifies the verification signature $V_i(RSU_{Sign})$ of both the reporting vehicle and reported vehicle . During the verification, if the vehicle V_j is found to be authentic the RSU sends its report message to TA. Otherwise if the vehicle V_i is found to be authentic the RSU sends the report message about the malicious vehicle V_j to TA.
Step: 13
RSU→TA: $V_i(TA_{Sign})$|| V_i(M)
RSU→TA: $V_i(TA_{Sign})$|| V_i(M)|| $V_j(TA_{Sign})$ V_j(RM)
In case the RSU receives report Message
V_j→ RSU: E $V_i(TA_{Sign})$|| $V_i(RSU_{Sign})$|| $V_i(\mathbf{C_{tk}})$||E(V_i(M)$_{V_i(S_{tk})}$)|| $V_j(TA_{Sign})$|| $V_j(RSU_{Sign})$|| V_j $(\mathbf{C_{tk}})$|| E(V_j(RM)$_{Vj(S_{tk})}$)
When the RSU receives message from the vehicles, it verifies the RSU verification signature $V_i(RSU_{Sign})$ of the vehicle V_j with RSU's current session common token

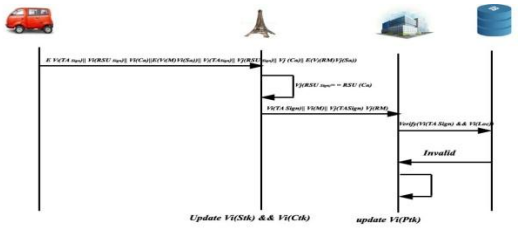

Fig. 4: Token update for malicious vehicle

Token Updating Process

The location privacy is assured to the registered vehicles and users by updating of token regularly. In the proposed system a vehicle uses three types of tokens.
Each token has different validity time. The token updating is the key component of the whole system as it protects the vehicles from the adversaries.
When the TA receives the report message concerning the vehicle V_i, from RSU, the TA verifies the vehicle V_i 's, verification signature $V_i(TA_{Sign})$ and its current location with TADB database. During the verification, if the vehicle V_i 's verification signature is correct but current location not closely associated with the most recently updated TADB location, then TA discovers that the vehicle V_i is a malicious one and it has misused the TA verification signature of another registered vehicle. Therefore the

TA updates the registered vehicles tokens to prevent from further malfunctions.

5. Performance Evaluation

In this section, we compare the functionality features among the proposed scheme EMPPAS and other most relevant schemes EMD [24] and HPPPA [23].

Simulation Settings

To analyze our proposed protocol, we simulated a number of scenarios with varying number of vehicles at average speeds 25 m/s. The number of vehicles is ranging from 20 vehicles up to 150 vehicles and the mean data is collected for every 30 vehicles interval. In our scenarios, 20 vehicles show sparse traffic that gradually becomes dense up to 150 vehicles with an increment of 30 vehicles. The average vehicle speeds were set to 25 m/s. The maximum simulation run time was observed as 3000 simulation seconds. The simulation setup is given in Table III

Table III: Simulation Setup

Parameters	Values
Network Area	3Km X 3 Km
Node Density	20 to 150
No of RSU	3
MAC Protocol	IEEE 802_15.4
Beacon Interval	500 Sec
Packet Size	Dynamic
Simulation Time	3000 Sec
Average Vehicle Speed	25 m/s
Message Size	200 Bytes
Encrypted Message Size	302 bytes

Performance Matrices

End-to-End delay: The end-to-end delay is the average time taken by an emergency message to travel from a source vehicle (V_S) to a destination vehicle (V_D) at the VANET environment.

$$End\ to\ End\ Delay = AVG_t(V_S \sim V_D)$$

AVG_t is the average time, (V_S~V_D) is the difference of time for a packet to reach from source to destination.

Message Delivery ratio: The message delivery ratio is the number of message received [Msg_r] by the destination vehicle and the number of message generated [Msg_g] by the source vehicle.

$$Message\ Delivery\ ratio = \frac{N\ [Msg_r]}{N\ [Msg_g]}$$

Throughput: The message throughput (in bps) is the total number of message received $N[Msg_r]$ divided by the total duration of simulation time T.

$$Throughput\ = \frac{N\ [Msg_r]}{T}$$

Message Overhead: The message overhead is total number of control message N [C Msg_g] generated divided by total number of delivered data message N [Msg_d].

$$Message\ Overhead = \frac{N\ [C\ Msg_g]}{N\ [Msg_d]}$$

Simulation Results Analysis

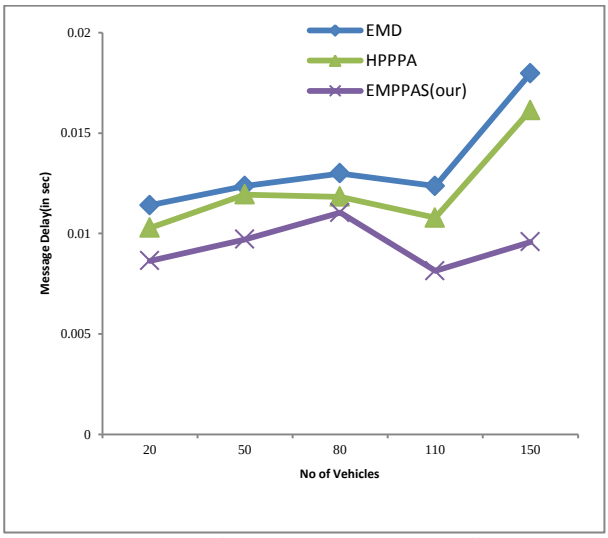

Fig. 5(a): Comparison of end-to-end delays among different schemes

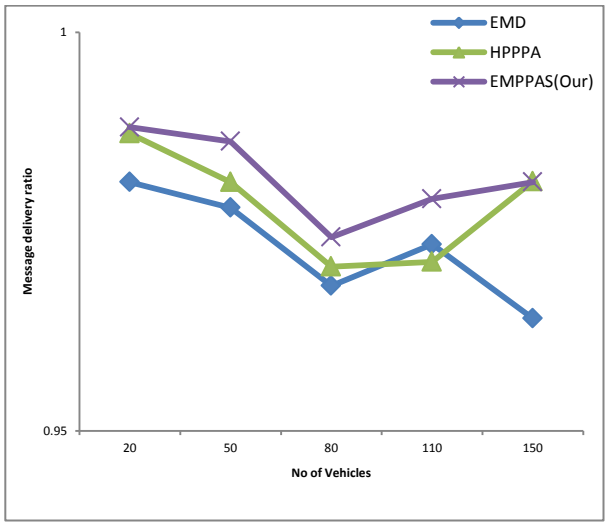

Fig. 5(b): Comparison of message delivery ratio among different schemes

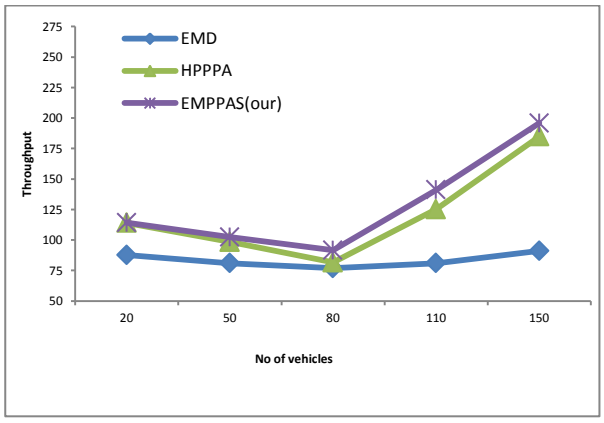

Fig. 5(c): Comparison of throughput among different schemes

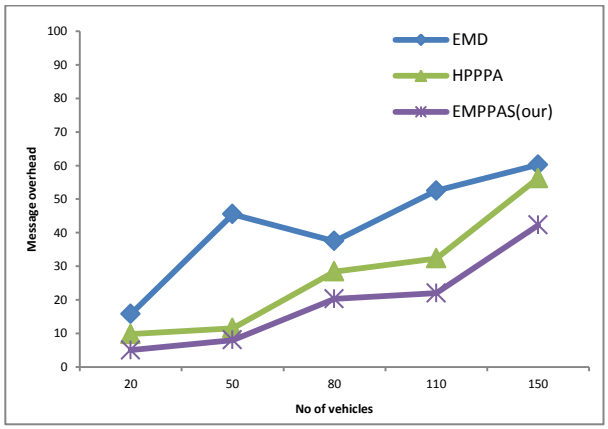

Fig. 5(d): Comparison of overhead among different schemes

End-to-End Message delay: Fig 5(a) shows the end-to-end delay of EMPPAS is compared with the EMD and HPPPA. In EMD select the forwarder node based only on furthest from source node. If the selected forwarder node is move opposite direction of destination or it move slow speed, the result is increase end to end delay. In HPPPA scheme, the message communication is single-hop broadcast. It cause end to end delay acquired by the beacon

increase with the increase in vehicle density. In EMPPAS select the reliable node while issuing acceptance and confirms the best node based on MRT. As the result the delay is reduced in the proposed EMPPAS scheme.

Delivery ratio: Fig 5(b) shows the delivery ratio of all protocols. The proposed scheme EMPPAS the delivery ratio is gained than the existing secure beacon scheme HPPPA. Because the proposed scheme encrypted message size is less than the existing scheme. Additionally in EMPPA scheme use FEMD routing algorithm identifies the global best path dynamically which is also responsible for improved delivery ratio.

Message Throughput: In Figure 5(c) shows the throughput of the proposed scheme compared with EMD and HPPPA. Throughput of our proposed scheme is prominent than the EMD and HPPPA. This is because our scheme is efficient and it needs less communication cost due to small sized messages used for authentication as compared to other schemes.

Message Overhead: In Figure 5(d) shows message overhead of EMPPAS is compared with the EMD and HPPPA. In EPPAS, message routing identifies the universal best path dynamically which is also control for unwanted control message broadcast. As the result the proposed scheme engage in low overhead than existing schemes EMD and HPPPA.

6. Conclusion

In this paper, an efficient multilevel privacy preserving authentication scheme named EMPPA is proposed to send a secure message in emergency situation. Our proposed scheme has multiple tokens with diverse life time and it provides multilevel privacy to emergency message. In this scheme, the trust authority updates the tokens, in case of any vehicle involving in malicious activity. Moreover, RSU updates the secondary and common tokens of the involved vehicles. This protocol provides location and message security to vehicles and users. Furthermore, we acquired better results in the performance analysis of our proposed protocol comparison with the existing schemes. In our future works embrace the implementation of the protocol in disaster areas with network connectivity pattern.

References

[1] Toor Y, Muhlethaler P & Laouiti A, "Vehicle Ad hoc networks: applications and related technical issues", *IEEE Communications Surveys & Tutorials*, Vol.10, No.3, (2008), pp.74-88.

[2] Rawashdeh ZY & Mahmud SM, "Communications in Vehicular Ad Hoc Networks, Mobile Ad-Hoc Networks: Applications", (2011).

[3] Kumar V, Mishra S & Chand N, "Applications of VANETs: Present & Future", *Communications and Network*, (2013), pp.12-15.

[4] Raya M & Hubaux JP, "Securing vehicular ad hoc networks", *Journal of Computer Security*, Vol.15, (2007), pp.39–68.

[5] Huang D, Misra S, Verma M & Xue G, "PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs", *IEEE Transactions On Intelligent Transportation Systems*, Vol.12, No.3, (2011), pp.736-746.

[6] Zhang C, Lu R, Lin X, Ho P & Shen XS, "An efficient identity-based batch verification scheme for vehicular sensor networks", *Proceedings of INFOCOM*, (2008), pp.246–250.

[7] Camenisch J, Hohenberger S & Pedersen M, "Batch verification of short signatures", *Proceedings of EUROCRYPT*, (2007), pp.246–263.

[8] Kamat P, Baliga A & Trappe W, "An Identity Based Security Framework For VANETs", *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, (2006), pp.94-95.

[9] Lu R, Lin X, Zhu H, Ho PH & Shen X, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications", *IEEE The 27th Conference on Computer Communications*, (2008), pp.1229-1237.

[10] Rajput U, Abbas F, Eun H, Hussain R & Oh H, "A Two Level Privacy Preserving Pseudonymous Authentication Protocol for VANET", *IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, (2015), pp.643-650.

[11] Wu L, Fan J, Xie Y, Wang J & Liu Q, "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks", *International Journal of Distributed Sensor Networks*, Vol.13, No.3,(2017).

[12] Wang F, Xu Y, Zhang H, Zhang Y & Zhu L, "2FLIP: A Two-Factor Lightweight Privacy Preserving Authentication Scheme for VANET", *IEEE Transactions on Vehicular Technology*,(2015), pp.1-18.

[13] Zhang C, Lin X, Lu R, Ho PH & Shen X, "An efficient message authentication scheme for vehicular communications", *IEEE Transactions on Vehicular Technology*, Vol.57, (2008), pp.3357-3368.

[14] Lin X, Ho PH, Sun X & Shen X, "GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications", *IEEE Transactions on Vehicular Technology*, (2007), pp.1-14.

[15] Zhang L, Wu Q, Solanas A & Domingo FJ, "A scalable robust authentication protocol for secure vehicular communications", *IEEE Trans Veh Technol*, Vol.59, No.1,(2010), pp.1606–1617.

[16] Zheng XL, Huang CT & Matthews M, "Chinese remainder theorem based group key management", *Proc. 45th ACMSE, Winston-Salem, NC, USA*, (2007), pp.266–271.

[17] Vijayakumar P, Bose S & Kannan A, "Centralized key distribution protocol using the greatest common divisor method", *Comput. Math. Appl.*, Vol.65, No.9, (2013), pp.1360–1368.

[18] Santhana Devi G & Germanus Alex M, " Fast Emergency message dissemination routing protocol in VANET", *Journal of Network Communications and Emerging Technologies*, Vol.7, No.2, (2017).

[19] Zhang Y, Liu W, Lou W & Fang Y, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys", *IEEE Trans. Dependable and Secure Computing*, Vol.3, No.4, (2006), pp.386-399.

[20] Boneh D & Franklin M, "Identity-Based Encryption from the Weil Pairings", *Advances in Cryptology-Asiacrypt*, (2001), pp.514-532.

[21] Rajput U, Abbas F & oh H, "a Hierarchical Privacy Preserving Pseudonymous authentication Protocol for VANET", *IEEE Access*, (2016), pp.1-13.

[22] Makwana RJ, "An Algorithm -EMD for Emergency in VANET", *International Journal of Computer Science & Engineering Technology (IJCSET)*, Vol.6, No.06, (2015).

[23] Rajput U, Abbas F & oh H, "A Hybrid Approach for Efficient Privacy-Preserving Authentication in VANET", *IEEE Access*, Vol.5, (2017), pp.12014-12030.