Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks

Pandi Vijayakumar, Maria Azees, Arputharaj Kannan, and Lazarus Jegatha Deborah

***Abstract*—Vehicular ad hoc networks (VANETs) are an important communication paradigm in modern-day mobile computing for exchanging live messages regarding traffic congestion, weather conditions, road conditions, and targeted location-based advertisements to improve the driving comfort. In such environments, security and intelligent decision making are two important challenges needed to be addressed. In this paper, a trusted authority (TA) is designed to provide a variety of online premium services to customers through VANETs. Therefore, it is important to maintain the confidentiality and authentication of messages exchanged between the TA and the VANET nodes. Hence, we address the security problem by focusing on the scenario where the TA classifies the users into primary, secondary, and unauthorized users. In this paper, first, we present a dual authentication scheme to provide a high level of security in the vehicle side to effectively prevent the unauthorized vehicles entering into the VANET. Second, we propose a dual group key management scheme to efficiently distribute a group key to a group of users and to update such group keys during the users' join and leave operations. The major advantage of the proposed dual key management is that adding/revoking users in the VANET group can be performed in a computationally efficient manner by updating a small amount of information. The results of the proposed dual authentication and key management scheme are computationally efficient compared with all other existing schemes discussed in literature, and the results are promising.**

***Index Terms*—Authentication, vehicle secret key, Chinese remainder theorem, group key management, VANET.**

I. Introduction

VEHICULAR Ad-hoc Network (VANET) is a distributed, self-organizing communication network, which is built among moving vehicles. Due to the promising features and their security properties, VANETs have extensive attention in the research community in recent years. In general, a VANET consists of three major components, namely the Trusted Authority (TA), Road Side Units (RSUs) and vehicles. The TA provides a variety of online premium services to the VANET users through RSUs. The RSUs are fixed at the road sides which are used to connect the vehicles to the TA. Each vehicle is installed with an On Board Unit (OBU) which is used to perform all computation and communication tasks. Various statistical studies reveal that due to road accidents, many people have either died or injured and the traffic jams generate a tremendous waste of time and fuel. In order to solve these problems and to enhance the driving comfort, appropriate traffic information should be provided to the drivers in a smart and secured way. Therefore, VANETs are developed to provide attractive services such as safety services that include curve speed warnings, emergency vehicle warnings, lane changing assistance, pedestrian crossing warnings, traffic-sign violation warnings, road intersection warnings and road-condition warnings. In addition, it can offer the comfort services such as weather information, traffic information, location of petrol stations or restaurants, and interactive service such as Internet access. Even though, these services make driving comfort, the Intelligent Transport System (ITS) technology heavily depends on the intelligent security and privacy-preserving protocols to enhance the quality of experience for the drivers and passengers without fear for their safety and personal privacy [1], [32].

Two types of communications are performed in VANETs. The first type is the Vehicle to Vehicle (V2V) communication in which the moving vehicles can communicate with each other and the second type is the Vehicle to RSU (V2R) communication in which the moving vehicles can communicate with the RSUs which are located aside the roads. The V2V and V2R communications are carried out using the Dedicated Short Range Communications (DSRC) standard [2], [29] through an open wireless channel. Each RSU and OBU uses a DSRC radio, based on IEEE 802.11p radio technology to access the wireless channel along with a directional or a unidirectional antenna. If an RSU wants to transmit a message to a specific location, a unidirectional antenna is used. Since, V2V and V2R communications are performed through an open wireless channel, these communications are vulnerable to various kinds of attacks such as interference, eavesdropping, jamming, etc. [3].

The primary step to ensure security in VANET is performed by providing an authentication mechanism through which it

Manuscript received September 22, 2014; revised July 17, 2015; accepted October 12, 2015. Date of publication November 11, 2015; date of current version March 25, 2016. This work was supported by the Centre for Technology Development and Transfer (CTDT), Anna University, Chennai, India. The Associate Editor for this paper was X. Cheng.

P. Vijayakumar, M. Azees, and L. Jegatha Deborah are with the Department of Computer Science and Engineering, University College of Engineering Tindivanam, Tindivanam 604001, India (e-mail: vijibond2000@gmail.com; azeesmm@gmail.com; blessedjeny@gmail.com).

A. Kannan is with the Department of Information Science and Technology, Faculty of Information and Communication Engineering, Anna University, Chennai 600025, India (e-mail: kannan@annauniv.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TITS.2015.2492981

is easy to ascertain all the authenticated vehicles [4], [7]. Authentication is the process of verifying a user identity prior to granting access to the network. It can be considered as the first line of protection against intruders. The authentication process ensures that only valid vehicles can be part of the group in VANET. In this paper, a new dual authentication scheme is proposed to provide the security improvement in the vehicle's side to resist malicious users entering into the VANET. After completing the authentication process, the TA can multicast the information to the authenticated vehicles. The authenticated vehicles can broadcast that information to other vehicles in a secure way. To multicast the information from the TA side and to broadcast the information from one vehicle to other vehicles, we have proposed a dual key management technique using Chinese Remainder Theorem (CRT). In this technique, the TA generates two different group keys for two different groups of users, namely primary user group and secondary user group. In the generated group keys, one group key is used for multicasting the information from the TA to primary users (PUs) and the other group key is issued for broadcasting the information from primary users to secondary users (SUs). However, the shared cryptographic group keys should be refreshed through a proper racing operation at the time of group membership changes due to new users joining into the network or old users leaving from the network. Therefore, an old group member has no access to present communications (forward secrecy) and a new member has no access to previous communications (backward secrecy). The proposed dual group key management scheme minimizes the computational cost of the TA and group members in the rekeying operation. To achieve this goal, the TA performs only simple addition and subtraction operations to update the group key. Similarly, each vehicle user of the multicast group performs only one modulo division operation for recovering the updated key when the group membership changes. The major contributions of this paper are summarized as follows.

1) We propose a secure dual authentication technique with the capability of preventing malicious vehicles entering into the VANET system.
2) We introduce a dual key management technique into the VANET to disseminate the information from the TA side to the group of vehicle users in an intelligent and secure way.
3) We get the computational complexity of our proposed dual key management scheme as $O(1)$ in both the TA and vehicle users and hence it is suitable for VANETs.
4) The communication complexity of our proposed dual key management scheme is also $O(1)$ which means that our scheme takes only one broadcast to inform the updated keying information from the TA to vehicle group.

The remainder of this paper is organized as follows. Section II summarizes the previous works in the literature. The system model and attack model are presented in Section III. We describe our proposed dual authentication scheme in Section IV and the dual key management for group communications in Section V. This section also explains secure data transmission scheme that takes place among vehicles. Section VI analyzes the security strength of our proposed scheme. Section VII provides the performance evaluation metrics and results of our proposed algorithm with the other existing key management schemes. Section VIII gives concluding remarks and suggests some future directions.

II. Previous Works

Many existing techniques are available in the literature for providing authentication in the VANET [3]–[6]. Among the various existing techniques, Johnson *et al.* [8] proposed an Elliptic Curve Digital Signature Algorithm (ECDSA), which is mathematically derived from the basic digital signature algorithm. ECDSA uses an asymmetric key pair which consists of a public key and a private key. The public key used in this technique is a random multiple of the base point, where the multiples are generated from the private key. Here, both the public and the private keys are used for user authentication. The two attacking techniques that are performed in this method are the attacks on Elliptic Curve Discrete Logarithmic Problem (ECDLP) and the attacks on the hash function. Wasef *et al.* [9] proposed a technique for the management of digital certificates, namely Efficient Certificate Management Scheme for Vehicular Ad Hoc Networks (ECMV). This method is based on a Public Key Infrastructure (PKI). In this technique, each vehicle has a short lifetime certificate and this certificate can be updated from any RSU. This certificate is frequently updated to provide privacy-preserving authentication, which creates an additional overhead. Shen *et al.* [10] represented Cooperative Message Authentication Protocol (CMAP) to find out the malicious information broadcasted by the malicious vehicles in the road transport system. The cooperative message authentication is a promising technique to alleviate vehicle's computation overhead for message verification. However, the communication overhead increases when the density of vehicles is higher. The main limitation of this method is that if there is no verifier to verify messages, then the malicious messages may be consumed by vehicle users.

Syamsuddin *et al.* [11] presented a comparison of various RFID authentication protocols based on the use of the hash chain method. However, among these existing protocols, most of them have addressed a specific issue called authentication. All these schemes fail to propose an integrated approach to provide the authentication as well as confidentiality services in VANET. Perrig *et al.* [12] represented a Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol, which uses symmetric keys instead of using asymmetric keys. Since the symmetric key systems are significantly faster than signatures, the Denial of Service (DoS) attack is averted in this system. However, it is hard to achieve non-repudiation with symmetric key-based approaches. So the digital signatures provide a best way for providing authentication with non-repudiation. Guo *et al.* [13] proposed a technique based on the group signature, which is a promising security scheme to provide privacy in VANETs. In the group signature, one group public key is connected with multiple groups of private keys. In this group signature scheme, an attacker can easily find a message sent by the group, but it is not possible to track the sender of

the message. Lin *et al.* [33] proposed a time-efficient and secure vehicular communications (TSVC) scheme for sequential message authentication. In this scheme, a vehicle first sends a hash chain to its neighbors and then it generates a MAC based on the elements of the hash chain through which the neighbors can authenticate this vehicle's messages. Due to fast MAC verification, this scheme considerably reduces the message loss ratio. However, in large scale networks, a vehicle is needed to broadcast its hash chain much more frequently to neighbors and hence the message loss ratio could increase.

Many existing schemes available in the literature are used to provide authentication only. Therefore, we have discussed some of the existing group key management methods used in the wired and wireless networks [14]–[17]. Among these schemes, Wong *et al.* [14] presented a novel solution to the scalability problem of group or multicast key management. They introduced the concept of key graphs for specifying secure groups. In addition, they presented three strategies for securely distributing rekeying messages after a join and leave operation in the secure group. In the rekeying strategies, join and leave protocols have been implemented in a prototype key server that they have built. The main limitation of this approach is the increased computational complexity. Zheng *et al.* [15] proposed two centralized group key management protocols based on the CRT. The main advantage of their approach is that the number of broadcast messages to distribute the group key to user side is minimized. Moreover, the user side key computation is also minimized. However, the main limitation of their approach is that computation complexity of the key server is very high.

Zhou and Yong [16] proposed a CRT based static key structure for distributing the group key to the members of the group when group membership changes. The main contribution of this work is that it minimizes broadcast messages and also minimizes user side key computation. However, it also increases the workload of key server by allowing the key server to find a common group key by using CRT for 'n' number of congruential equations. Naranjo *et al.* [17] presented a new algorithm for key management to provide security and privacy. Vijayakumar *et al.* [18] proposed a Greatest Common Divisor (GCD) based key distribution protocol that focuses on two dimensions. The first dimension deals with the reduction of computational complexity and second dimension aims at reducing the amount of information stored in the Group Center and group members while performing the update operation in the key content. The main limitation of these existing works is that the computation complexity involved in rekeying operations leading to the decrease in performance. In addition, the memory requirements are high in most existing schemes.

Comparing with most of the existing authentication and group key management schemes existing in the literature, the authentication scheme proposed in this paper is a dual authentication scheme with intelligent decision making for vehicle movement. The main objective of developing a dual authentication scheme is to improve the security in the vehicle side. The dual authentication scheme in our system depends on the vehicle secret key (VSK) which is given to the user during the time of registration by the TA and the fingerprint of the individual user. Even if the VSK value of any user is lost,

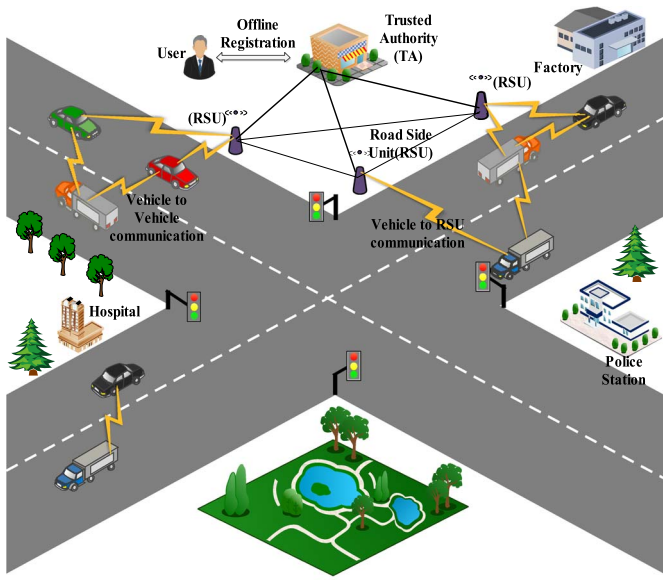


Fig. 1. System model.

the intruder cannot use that VSK for getting service from the TA. To prevent the intruder to use other users VSK, we have included fingerprint of each authenticated user in the smart card issued by the TA. Moreover, the proposed dual authentication technique is a computationally efficient authentication technique. To provide secure and reliable data transmission facility based on group communication in VANETs, we have developed a dual key management scheme in this paper. The dual key management scheme proposed in this paper is superior to others in many ways. First, the computation complexity of the TA and VANET user is reduced substantially by minimizing the number of arithmetic operations taken by the TA and VANET user. In order to minimize the computation time in both the TA and vehicle side, we use the CRT based key management scheme. In addition, we reduce the number of computations by validating the credentials using intelligent agents in the OBU. Hence, the overall computing power is enhanced in each vehicle. Second, comparing with all the existing group key management algorithms, the number of key values stored by VANET users is also minimized in this work. Finally, the proposed algorithm reduces the amount of information needed to be communicated for updating the group key values when there is a change in the group membership.

III. System Overview

In this section, we demonstrate the system model, the attack model and system assumptions used in our proposed method.

A. System Model

The system model of our proposed scheme is shown in Fig. 1. It consists of a TA, RSUs and vehicles.

Trusted Authority (TA): The TA is responsible for the registration of RSUs, vehicle OBUs and the vehicle users and it is also responsible for key generation and distribution to support secure premium services in the VANET system. In our scheme,

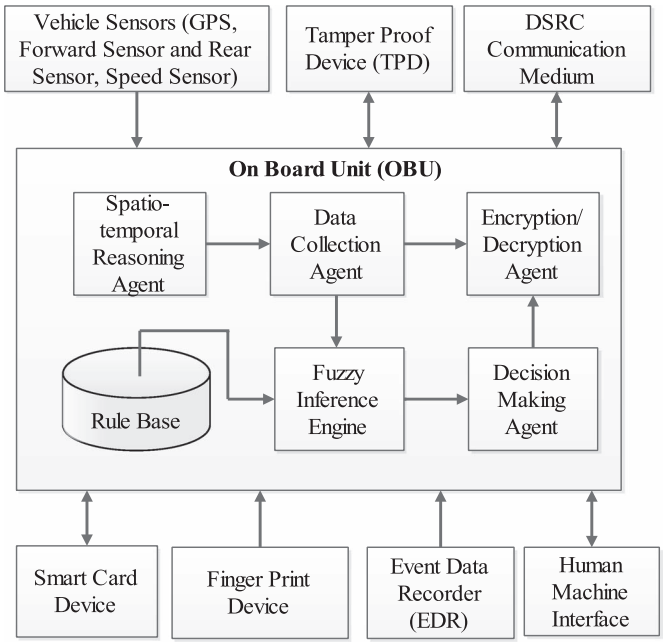


Fig. 2. Components of a vehicle for intelligent transportation.

every state in the country has a TA. When a vehicle moves from one state to another state, the vehicle's credentials will be verified using the TA of the registered state, which is initiated by the TA of the state where the vehicle is roaming currently. In Fig. 1, we have illustrated a single TA for our convenience. In addition to this, each TA authenticates the identity vehicle OBU's or the identity of users to avoid malicious vehicles entering into the VANET system.

Road Side Unit (RSU): RSUs are deployed at the roadsides and they are regularly monitored and managed by the TA [28]. These units act like bridges between the TA and the vehicles. The RSUs connect with the TA by a secure wired network and OBUs by an open wireless channel.

Vehicles: Each vehicle is embedded with an OBU in the VANET system. The vehicles can communicate with other vehicles and RSUs through this OBUs. The vehicles can communicate with the TA through the RSUs. The OBU consists of six major components, namely an encryption/decryption agent, data collection agent, spatio-temporal reasoning agent, Fuzzy inference engine, rule base and decision making agent as shown in Fig. 2.

Moreover, the OBU interacts with vehicle sensors, Tamper Proof Device (TPD), DSRC communication medium, smart card device, fingerprint device, Event Data Recorder (EDR) and human machine interface to perform effective decision making on vehicle movement. The Data collection agent collects the necessary data from the intelligent transportation components like the Global Positioning System (GPS), forward and rear sensors, speed sensor, TPD, DSRC communication medium, smart card device, finger print device and EDR for giving input to the Fuzzy inference engine. Among these devices, the GPS receiver is used to acquire the vehicle's real-time geographical position and to perform fairly accurate time synchronization among the vehicles [31]. The TPD is used to store sensitive data such as a secret key, group key and the identity of the vehicle. The EDR is used to record information related to accidents or vehicle crashes. The speed sensor is used to collect the vehicle information such as velocity and breaking information. The forward and rear sensors are used to monitor the activities happening on the front and rear side of the vehicle. The communication system uses a communication device such a DSRC radio to communicate with other vehicles and RSUs. The data collection agent also collects the fingerprint from the individual user through the fingerprint device and compares this with the fingerprint in the smart card for dual key authentication purpose. The smart card is given by the TA during the time of registration, which contains the fingerprint and VSK. The smart card is used through a smart card device which is also controlled by the OBU. The spatio-temporal reasoning agent is not only responsible for checking spatial and temporal constraints on road conditions, but also to perform predictions on the safest place with respect to space and time for further vehicle movement and to plan in prior the suitable moving arrangements.

The fuzzy inference engine is the core component of the intelligent transportation system which uses the symmetric fuzzy Gaussian membership function [34] to extract appropriate decisions from the data provided by the data collection agent. The rule base contains IF-THEN fuzzy rules for the classification of the data and the fuzzy rules generated in this research work are given in the Appendix (see Table III). The scheduler in the fuzzy inference subsystem is used to select appropriate rules from the rule base and sends them to the decision making agent. The decision making agent finally selects suitable decisions on the executed rules according to the road conditions in order to reduce the traffic and to minimize the fuel consumption. The encryption/decryption agent is used to encrypt or decrypt the incoming messages that are received from the data collection agent and the decision making agent to achieve data security. The human machine interface component is responsible for the interaction between the vehicle users and OBUs. The goal of this interaction is to allow the vehicle users to view the messages and to generate the messages. Vehicle original equipment manufacturers are required to invest in vehicle components that are designed to interact with the intelligent transportation components via standardized interfaces [30] in order to satisfy the above mentioned objectives.

B. Attack Model

Since the V2V and V2I communications are carried out in an open wireless channel, there are many attacks which threaten these kinds of communications on the road. In this section, we have listed several possible attacks performed in VANETs.

1) **Message replay attack:** As the name implies, this attack is basically happening when the attacker repeats or delays the valid message transmission maliciously to disturb the traffic.
2) **Sybil attack:** The attacker may use multiple identities at the same time. In this attack, an attacker broadcast numerous messages with different identities to other vehicles.

The receiving vehicles think that these messages are broadcasted from different vehicles and hence they feel that there is a traffic jam and they are enforced to change their routes to make the road clear. The Sybil attack is very difficult to identify and it is really dangerous to the VANET environment.

3) **Masquerading:** In this attack, the attacker actively pretends to be another vehicle by using false identities. This attack takes place when one user makes believe to be a different user to gain unauthorized access through legitimate access identification.
4) **Message Tampering/Fabrication/Alteration:** In this attack, the attacker may modify, delete and alter the content of the message or a specific part of the message to be sent. The attacker makes some modifications in the message which helps him to meet his intended purpose of the attack.
5) **Collusion attack:** The collusion attack is the improper secret agreement in which two or more adversaries cooperatively defraud and act as legitimate PUs for their benefit. For example, the vehicles make an improper secret agreement with the current primary users in the group to get the updated group key after leaving from the PUs group.

Hence, our scheme is designed to prevent all the aforementioned security attacks to improve system security during the dual authentication and key management.

C. Assumptions

Some important assumptions are considered in our proposed scheme which are very essential for secure VANET communications. The assumptions are as follows.

1) TA is powerful than vehicle OBUs and RSUs in terms of computation, communication, and storage capability.
2) TA's public key is given to all vehicles and RSUs at the time of registration.
3) TA has powerful firewalls and other protections that prevent them from being compromised [7].
4) Each vehicle keeps its VSK as a secret which is given by the TA to the VANET vehicle users during the time of their registration. Similarly, each RSU keeps its own RSU Secret Key (RSK) as a secret which is given by the TA during the time of its registration.
5) The TA maintains a list of VSKs of all registered vehicles along with its corresponding vehicle ID (ID_V) and RSKs of all RSUs along with its corresponding RSU ID (ID_{RSU}) in a secure manner.

IV. Proposed Dual Authentication Technique

This section explains our proposed dual authentication technique, which is used for secure VANET communication. To provide secure, authenticated communication in VANETs, initially, the TA selects two large prime numbers p and q. The value p helps in defining a multiplicative group z_p^* and q is used to fix a threshold value to select the group key values. Initially, the TA selects the VSK_i $(1 \leq i \leq n)$ from the multiplicative group z_p^* for 'n' number of vehicles which are given to the vehicle users when they complete the registration process. This VSK is used for authenticating the vehicles when they enter into the VANET to start communicating with other vehicles and RSUs. In order to improve the authentication process, we use a dual authentication technique in this paper where the authentication process is performed two times. For the first time, authentication is done on the vehicle side and the second time, authentication is done in the TA side and hence the intruder has no possibility to enter into the VANETs. In the TA, the authentication is performed by verifying the Hash Code (HC) generated by the vehicle using their VSK_i. The authentication was performed on the vehicle side by verifying the fingerprint given by the user at the time of registration. The main objective of introducing dual authentication technique is that anyone who finds the VSK of a vehicle cannot enter into VANET communication as they cannot produce the fingerprint of the corresponding vehicle user. The same is true if the attacker has only the fingerprint of a vehicle user and does not have VSK of that vehicle. Therefore, the dual authentication technique provides more security because these two factors are required in order to authenticate the vehicles.

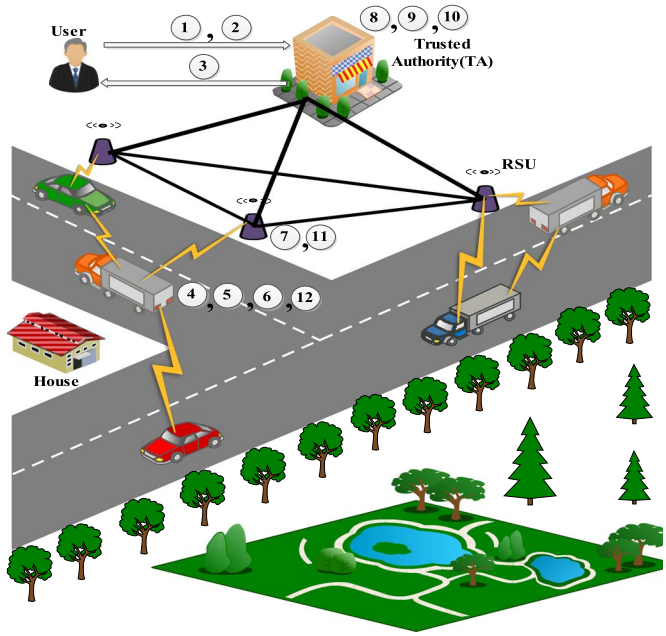


Fig. 3. Authentication in vehicle and the TA.

In VANETs, the registration can be performed in two ways, namely online mode and offline mode. In the online mode, each VANET user performs registration process by submitting his/her details in the TA's website through Internet connection. In contrast to the online mode, the user goes to the TA's office to complete registration in the offline mode. In this approach, the registration is performed in the offline mode. After completing the registration process, each VANET user must complete a dual authentication process to get Authentication Code (AC) in order to send messages in VANETs. After receiving the authentication code, the vehicles are permitted to receive services from the TA and also vehicles can exchange information from one vehicle to other vehicles. This section explains about only dual authentication technique proposed in this paper. Fig. 3 shows

the dual authentication process performed by both the vehicle and the TA. The following steps explain the process of dual authentication in both the vehicle and the TA.

A. Registration Through Offline Mode

1) The VANET user first approaches the TA office directly to make offline registration and provide the essential information like name, address, phone number, email id etc. to the TA.
2) While each user performs registration, the TA gets the fingerprint of the corresponding user.
3) After completing the registration process, the TA provides the VSK_i to the registered user, which is unique for every vehicle and the TA also maintains the list of all the vehicles and their respective VSKs in its storage area. The TA provides the (VSK_i) to the user through a smart card which also contains the user's fingerprint which is given by the TA to the user after completing the registration process.
   - The (VSK_i) is used for creating the Hash Code (HC) and the HC is verified by the TA for authentication and then the TA provides AC to the authenticated VANET users.
   - The fingerprint is also verified in the vehicle side for authentication of the user during the time for making communication with the VANET.
   - If the fingerprint is not matched with the fingerprint which is printed on the smart card, then the user is not permitted to make communications with VANETs.

B. Vehicle's Authentication Process

4) Each user store (VSK_i) in their vehicle in the tamper proof device which is equipped in the car. When a user wants to communicate with the VANETs, then the user first enters his/her fingerprint through a fingerprint device which is equipped inside the car. Then, the OBU of the vehicle compares this fingerprint with the smart card fingerprint that is already stored in the smart card.
   - If they match, the user is allowed to communicate with TA and with the other vehicles.
   - If they do not match, the user is not allowed to communicate with other users of the VANET.

C. Trusted Authority's Authentication Process and the Provision of Authentication Code (AC)

5) Each vehicle selects a random number N. After selecting the random number, it successively creates a Hash Code (HC) using N and VSK by SHA_256 [27] algorithm.

$$HC = SHA\_256(\text{VSK} \| N). \tag{1}$$

6) The vehicle encrypts the random number N, the Hash Code (HC) and the Vehicle ID, with its VSK, and broadcasts along with the Vehicle's identity ID_V, TA identity ID_{TA} and the time stamp TS_1 as shown in equation (2). This forms the Authentication Request.

$$\langle E_{\text{VSK}}\left(N \| HC \| ID_V\right) \| ID_V \| ID_{\text{TA}} \| TS_1 \rangle . \tag{2}$$

TABLE I
THE NOTATIONS AND DESCRIPTIONS

Notation	Description
N	Random number
HC	Hash Code
VSK	Vehicle Secret Key
RSK	RSU Secret Key
ID_V	Vehicle Identity
ID_{TA}	TA Identity
ID_{RSU}	RSU Identity
TS	Time Stamp
AC	Authentication Code
$E()$	Encryption
$D()$	Decryption
$PUSK$	Primary Users Secret Key
$SUSK$	Secondary Users Secret Key
k_{pug}	Primary Users Group key
k_{sug}	Secondary Users Group Key
$TA-pvt$	Private key of TA
$TA-pub$	Public key of TA

Here, the identities of vehicle (ID_V), RSU (ID_{RSU}) and the TA (ID_{TA}) are dummy identities which are generated during the time of its registration using the following manner. In order to compute the dummy identities, the TA chooses two random numbers a_1 and b_1 such that $a_1, b_1 \in Z_q^*$ and computes $ID_V = g_1^{a_1} \times g_2^{b_1} \bmod q$. Here, g_1 and g_2 are the generators of Z_q^*. Similarly, the TA generates the dummy identities of RSUs (ID_{RSU}) and its dummy identity (ID_{TA}). The mapping from original identities to dummy identities is done only in the TA. The necessity of attaching the dummy identities in each message is to check the validity of the message source and the identification of the particular vehicle or RSU or TA. Even though these identities are disclosed to all vehicles, they do not reveal the privacy of the vehicle users or RSUs or TA. Because, even if these dummy identities are captured, they provide zero knowledge about the vehicle user or RSU. Table I defines the list of symbols used in this paper.

7) The RSU receives the packet, appends its identity ID_{RSU} and increments the timestamp value TS_1 to get TS_2. Then, the RSU encrypts the entire message using the RSK which is known only to TA and RSU and forwards it to the TA as given in equation (3).

$$\langle E_{\text{RSK}}(E_{\text{VSK}}(N \| HC \| ID_V) \| ID_V \| ID_{\text{TA}} \| TS_2 \| ID_{\text{RSU}}) \rangle . \tag{3}$$

8) The TA decrypts the packet received from RSU using RSK of the RSU and validates the RSU with its identity ID_{RSU} as given in equation (4).

$$\langle D_{\text{RSK}}\left(E_{\text{RSK}}\left(E_{\text{VSK}}\left(N \| HC \| ID_V\right) \right.\right. \left.\left. \| ID_V \| ID_{\text{TA}} \| TS_2 \| ID_{\text{RSU}}\right)\right) \rangle . \tag{4}$$

The TA also verifies its identity ID_{TA} after decrypting it using RSK. After verifying its identity, the TA decrypts

the packet using VSK of the particular vehicle and verifies the ID_V

$$\langle D_{\mathrm{VSK}}\left(E_{\mathrm{VSK}}\left(N \| HC \| ID_V\right)\right)\rangle. \tag{5}$$

Then, the TA generates the HC using the random number N and the VSK by SHA_256 algorithm and then verifies the newly computed HC value with the HC which is sent from the vehicle side.

9) If the two HC values match, then the TA hashes the Hash Code to get the Authentication Code (AC).

$$AC = SHA\_256(HC). \tag{6}$$

10) The TA includes the Vehicle ID, incremented time stamp value and also it includes the lifetime of the AC along with the AC and encrypts this sequence with its private key of TA $(\mathrm{TA} - Pvt)$ to create a digital signature. Therefore, any vehicle user can verify this digital signature using the public key of TA. But, no vehicle user can regenerate this digital signature because it is generated using the private key of the TA.

$$\langle E_{\mathrm{TA}-Pvt}\left(AC \| ID_V \| TS_3 \| \mathrm{Lifetime}\right)\rangle. \tag{7}$$

This forms the authentication response. To securely transfer this AC to the appropriate vehicle user, the TA also encrypts this authentication response using the VSK value of the corresponding user and RSK of RSU.

$$\langle (E_{\mathrm{RSK}}(E_{\mathrm{VSK}}(E_{\mathrm{TA}-Pvt}(AC \| ID_V \| TS_3 \| \mathrm{Lifetime}))) \| ID_{\mathrm{TA}})\rangle. \tag{8}$$

Finally, the TA sends the packet to the RSU.

11) RSU receives the packet from the TA and decrypts the packet using its RSK.

$$\langle D_{\mathrm{RSK}}\left(E_{\mathrm{RSK}}\left(E_{\mathrm{VSK}}\left(E_{\mathrm{TA}-Pvt}\left(AC \| ID_V \| TS_3 \| \mathrm{Lifetime}\right)\right)\right) \| ID_{\mathrm{TA}}\right)\rangle. \tag{9}$$

On receiving this message, the RSU is able to check the identity of TA (ID_{TA}), verifies that whether it is sent by the legitimate TA or malicious node. After verifying the identity of the TA, the RSU sends the packet to the vehicle user.

$$\langle (E_{\mathrm{VSK}}\left(E_{\mathrm{TA}-Pvt}\left(AC \| ID_V \| TS_3 \| \mathrm{Lifetime}\right)\right) \| ID_{\mathrm{TA}})\rangle. \tag{10}$$

12) The vehicle decrypts the packet using its VSK, and then verifies ID_{TA}.

$$\langle D_{\mathrm{VSK}}(E_{\mathrm{VSK}}(E_{\mathrm{TA}-Pvt}(AC \| ID_V \| TS_3 \| \mathrm{Lifetime})) \| ID_{\mathrm{TA}})\rangle. \tag{11}$$

After that, the vehicle verifies the ID_V by decrypting the resultant message using the public key of the TA.

$$\langle D_{\mathrm{TA}-pub}\left(E_{\mathrm{TA}-Pvt}\left(AC \| ID_V \| TS_3 \| \mathrm{Lifetime}\right)\right)\rangle. \tag{12}$$

13) The vehicles then start sending the safety messages to other vehicles with this AC by encrypting the payload (message) using vehicle's group key k_{pug} or k_{sug} as shown in equation (13).

$$\left\langle E_{k_{pug}}(\mathrm{payload}) \| \left(E_{\mathrm{TA}-Pvt}(AC \| ID_V \| TS_3 \| \mathrm{Lifetime})\right)\right\rangle. \tag{13}$$

In many existing approaches, the *payload* is not encrypted [19]–[21] when it is communicated with the other vehicles. In order to protect the *payload* (actual data or information) field against eavesdropping and modification by unauthorized users, we have included a protocol which is explained in Section V. To provide two different secure group communications in VANETs, we have also developed a dual key management scheme in this paper.

V. Dual Key Management for Group Communication

Dual Key Management is a group key management scheme in which the TA computes two different group keys intended for two different groups in VANETs. The group is a very important concept in our scheme. Based on the money paid to the TA, a very simple Service Level Agreement (SLA) is considered between the TA and the vehicle users, which categorize the vehicle users into three groups, namely Primary Users (PUs), Secondary Users (SUs) and Unauthorized Users (UUs) in a predefined manner. The PUs are eligible to get attractive services such as safety, comfort services and interactive services from the TA. The PUs are authorized VANET users who receive these services from the TA side periodically. The SUs are also authorized VANET users who receive the attractive services such as safety services from the PUs without making any requests to them, but they cannot receive the information directly from the TA. The PUs can communicate with each other by means of V2V communications. However, the SUs can also communicate with each other after getting the SUs group key from the TA through PUs. Both the PUs and the SUs will have a valid VSK received from the TA. Finally, UUs are the vehicle users who do not have access to the information exchanged between PUs and SUs and hence a UU is considered as an intruder in this proposed approach.

To disseminate the information from the TA side to PUs side in a secure way, the TA encrypts the information using a common group key which is derived using individual vehicles secret key of PUs as discussed in one of the previous works [22]. Similarly, for broadcasting the information from the PUs to SUs in a secure way, the TA encrypts the group key of SUs using the group key of PUs and multicast it to PUs. All the PUs can get the group key of SUs. This group key is used in the PUs side to encrypt the information and the encrypted message is sent to neighboring SUs. In computing a common group key separately for PUs and SUs vehicles in the TA side, we use CRT based group key management scheme used in many existing schemes [15], [16], [25].

Let $k_1, k_2, k_3, \ldots, k_n$ be pairwise relatively prime positive integers, and let $a_1, a_2, a_3, \ldots, a_n$ be positive integers. Then, CRT states that the pair of congruences, $X \equiv a_1 \mod k_1$, $X \equiv a_2 \bmod k_2, \ldots, X \equiv a_n \bmod k_n$ has a unique solution

mod $\partial_g = \prod_{i=1}^{n}(k_i)$. To compute the unique solution, the TA can compute the value as shown in equation (14).

$$X = \sum_{i=1}^{n} a_i \beta_i \gamma_i (\text{mod } k_i)$$
$$\text{Where,} \quad \beta_i = \frac{\partial_g}{k_i} \text{ and } \beta_i \gamma_i \equiv 1 \bmod k_i. \tag{14}$$

The proposed dual group key management scheme works in four phases. The first phase is the TA Initial set up, where a multiplicative group is created at the TA side from which secret key and group key values are selected. For differentiating the VSK values of PUs and SUs vehicles, we use two types of notations for representing the secret key values used for PUs and SUs in this section. The secret key value of PUs is denoted as $PUSK_i$ $(i = 1, \ldots, n)$ and SUs are denoted as $SUSK_i$ $(i = 1, \ldots, n)$. The second phase is called registration and group key computation phase, where the PUs and SUs complete the registration process and receives $PUSK_i$ and $SUSK_i$ $(i = 1, \ldots, n)$ from the TA side. After that, the TA also generates two group keys separately for two groups of PUs and SUs and it informs this group key to them in a secure way. The third phase is secure data transmission, where the data are disseminated using the group key values in the VANET. The final phase of this algorithm is the key updating phase where a group key is updated when an existing PU leaves the PU's multicast group or a new PU joins the PU's multicast group in order to provide forward and backward secrecy. Similarly, the TA also updates the group key of SUs separately.

A. TA Initial Set Up

Initially, the TA selects large prime numbers p and q, where $p > q$ and $q \leq \lceil p/4 \rceil$ where p value is used for defining a multiplicative group z_p^* and q is used for selecting the group key values. Initially, the TA selects $PUSK_i$ and $SUSK_i$ from the multiplicative group z_p^* for 'n' number of vehicles which will be given to the vehicle users at the time of offline registration. In the proposed group communication scheme, it is required that all the $PUSK_i$ and $SUSK_i$ values are pairwise relatively prime positive integers and are selected from z_p^* as explained in [15], [16]. Moreover, all the secret keys should be much larger than the group key which is selected within the threshold value fixed by q. Next, the TA executes the following steps as we illustrated in our previous approaches [18], [23] for computing the group key used for PUs. Similarly, the TA will also compute a group key for SUs.

1) Compute $\partial_g = \prod_{i=1}^{n}(PUSK_i)$ (15)
2) Compute $x_i = \frac{\partial_g}{PUSK_i}$ where $i = 1, 2, 3, \ldots, n$ (16)
3) Compute y_i such that $x_i \times y_i \equiv 1 \bmod PUSK_i$ (17)
4) Multiply all users x_i and $y_i$values and store them in the variables
$$\text{var}_i = x_i \times y_i \tag{18}$$
5) Compute the value $\mu = \sum_{i}^{n} \text{var}_i$. (19)

B. Group Key Computation

In this phase, the VANET group users complete the registration process and get their corresponding group secret keys from the TA. Whenever the TA wants to send common information to a group of VANET users (PUs) to support the group communication, the TA computes the group key in the following way and multicast it to the PUs group through RSU.

a) Initially, the TA selects a random element k_{pug} as a new group key for PUs within the range q.
b) Multiply the newly generated group key with the value μ which is computed in TA initial setup.
$$\gamma_{pug} = k_{pug} \times \mu. \tag{20}$$
c) The TA broadcast a single message γ_{pug} to the VANET users. Upon receiving γ_{pug} value from the TA side, an authorized vehicle can obtain the new group key k_{pug} by doing only one modulo division operation as shown in equation (21).
$$\gamma_{pug} \bmod PUSK_i = k_{pug}. \tag{21}$$

Since, $k_{pug} < q < PUSK_i < p$ and $\mu \bmod PUSK_i = 1$, the k_{pug} obtained in this way must be equal to the k_{pug} generated in Step a) of group key computation phase. After computing the group key, the TA also computes another group key k_{sug} using the aforementioned procedure for SUs. Then, it encrypts this k_{sug} using k_{pug} and it is sent as a multicast message along with γ_{pug} and γ_{sug} to all the PUs.

$$\left\langle E_{k_{pug}}(k_{sug}) \| \gamma_{pug} \| \gamma_{sug} \right\rangle. \tag{22}$$

After receiving the packet from TA, the PUs compute the value of k_{pug} from γ_{pug}using equation (21) and then decrypt $E_{k_{pug}}(k_{sug})$ to get the group key value of SUs.

$$\left\langle D_{k_{pug}}\left(E_{k_{pug}}(k_{sug})\right) \| \gamma_{sug} \right\rangle. \tag{23}$$

Then the PUs send γ_{sug} as a multicast message to all the SUs in its coverage area. After receiving this message from the PUs, the SUs compute the value of k_{sug} from γ_{sug} as given in equation (24).

$$\gamma_{sug} \bmod SUSK_i = k_{sug}. \tag{24}$$

The PUs utilize the group key value of SUs to broadcast the information to the nearest SUs within their coverage area. Therefore, the TA encrypts the information using this group key (k_{pug}) and multicast it to the PUs. All the PUs can use their group key to decrypt the information received from the TA side. Each PU can in turn broadcast the information received from the TA to SUs by encrypting it using k_{sug}. In this way, the secure group communication is implemented in this proposed work. When 'i' reaches to n, the TA executes TA Initial set up phase to compute ∂_g, var_i and μ for 'm' number of users where $m = n \times \delta$. The value δ is a constant value which may take values less than 5 depending upon the dynamic nature of the multicast group.

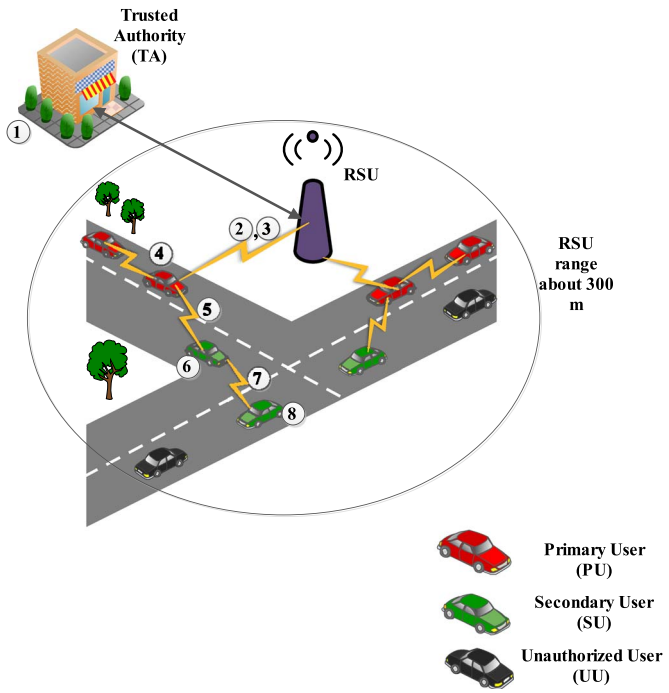


Fig. 4. Secure Data communication in VANET.

C. Secure Data Transmission in VANETs

In this subsection, we have explained the secure transmission of data (information) from TA to vehicles and between vehicles in VANETs. Fig. 4 shows the working of secure data transmission that takes place between the TA and PUs. In addition to this, it also represents the V2V communications that take place between PUs and SUs. The TA has collection of servers for storing the necessary keys and data required for the VANET users. The TA can multicast the information to PUs through a dedicated Internet connection. The PUs in turn can broadcast the information to SUs with the PUs wireless medium. Finally, the UUs have no permission to communicate to the VANETs since they are unauthorized users. In order to improve the confidentiality, the messages should be exchanged in an encrypted form so that the UUs cannot access the messages. The steps involved in the secure data transmission in VANET communication are described as follows:

Step 1. The TA generates a group key (k_{pug}) using the PUSK's of the PUs after collecting the requests of PUs through any RSU. Also, it generates a separate group key (k_{sug}) for SUs.

Step 2. Then, the TA multicasts both the group key values in an encrypted form as explained in equation (20). Both the group users can find their group key using their secret key values as used in equation (21). Also, the TA sends the group key value of SUs through the RSU to the PUs by encrypting it using PUs group key $E_{k_{pug}}(k_{sug})$.

Step 3. The TA sends messages or traffic information to the PUs only by encrypting the messages using PUs group key k_{pug}, and there is no message exchange between the TA and SUs.

$$\left\langle E_{k_{pug}}(ID_{\mathrm{TA}} \| \text{message or information}) \right\rangle. \quad (25)$$

Step 4. After receiving the data packet from the TA, the PUs decrypt the packet using k_{pug} and consumes the information or messages.

$$\left\langle D_{k_{pug}} \left(E_{k_{pug}}(ID_{\mathrm{TA}} \| \text{message or information}) \right) \right\rangle. \quad (26)$$

Step 5. The PUs broadcast the message to the SUs, by encrypting the message or information using the group key of SUs along with the authentication code received from the TA in the dual authentication technique.

$$\left\langle E_{k_{sug}}(ID_V \| \text{message or information}) \| E_{\mathrm{TA}-Pvt} \right. \\ \left. (AC \| ID_V \| TS_3 \| \text{Lifetime}) \right\rangle. \quad (27)$$

Step 6. After receiving the data packet, the nearest SUs can decrypt the data packet using the group key k_{sug} and can also verify the authenticity of the messages by decrypting the authentication part using the public key $(\mathrm{TA} - Pub)$ of TA as shown below:

$$\left\langle D_{\mathrm{TA}-Pub} \left(E_{\mathrm{TA}-Pvt} \left(AC \| ID_V \| TS_3 \| \text{Lifetime} \right) \right) \right\rangle. \quad (28)$$

Step 7. The SUs can in turn forward the received data packet to other SUs by encrypting it using k_{sug} over a long range using multihop communication.

Step 8. After receiving the packets, the SUs can decrypt the packet using the k_{sug} and process the messages.

D. Key Updating

Group key updating operation is performed when a PU joins or leaves and usually takes more computational complexity in most of the group key management schemes [20], [22], [26]. When a PU joins the VANET group, it is the responsibility of the TA to communicate the new group key in a secure way to the group members. Therefore, the newly joining user cannot view the previous communications and it provides backward secrecy. Similarly, when a PU leaves from a group, the TA must update the group key in order to avoid the use of a new group key by the old PU to preserve forward secrecy. In our proposed key management scheme, the group key updating process is performed in a simplest way when the group membership changes. For example, when a vehicle v_i of PU leaves the group, the TA has to perform the following steps.

1) Subtract var_i from μ.

$$\mu' = \mu - \mathrm{var}_i. \quad (29)$$

2) Next, the TA must select a new group key k'_{pug} and it should be multiplied by μ' to form the rekeying message as shown below.

$$\gamma'_{pug} = k'_{pug} \times \mu'. \quad (30)$$

3) The updated group key value is sent as a broadcast message to all the existing PUs. The existing users of the PUs group can get the updated group key value k'_{pug} by doing only one mod operation as shown in equation (21). From the received value, the vehicle v_i cannot find

the newly updated group key k'_{pug} since that particular vehicle's secret key is not included in μ'.

Similarly, if a PU wants to join in the multicast group, then the TA has to perform only one addition operation for updating the group key. For example, if v_i wants to join an existing VANET group, then the TA has to perform the following steps for group key updating.

1) Instead of computing x_i and y_i value for the new VANET user, the TA can take the multiplied value of x_i and y_i from the variable var_i which is already computed in the TA initialization phase. The TA can select this value from the TA's storage area to compute $\mu' = \mu + \mathrm{var}_i$.
2) Next, the TA selects a new group key k'_{pug} and multiplies it with updated μ' to form the rekeying message as shown in equation (30).
3) The updated group key value is sent as a multicast message to all the existing and newly joined PUs of the group. From the multicast value γ'_{pug}, the newly joined PUs of the multicast group can find the newly updated group key k'_{pug} since his/her var_i value is included in μ' using var_i.

Therefore, in general, if 'n' PUs want to join in the existing PU's multicast group, the TA has to perform 'n' additions for updating the group key. The key strength of our algorithm is that the computational complexity of the TA is completely reduced in comparison to the other existing approaches [21], [22]. The computation complexity of the TA is $O(1)$ when a single PU joins or leaves from the multicast group. In addition to this, the computational complexity of a multicast PU is also minimized by allowing each PU to perform only one modulo division operation. Moreover, the TA takes only one broadcast message which is same in most of the existing algorithms for informing the updated group key value to PUs of the multicast group.

VI. Security Analysis

In this section, we analyze the security strength of our proposed dual authentication scheme with respect to the attack models presented in Section III. The proposed group key management scheme is analyzed for various attacks to support forward secrecy and backward secrecy as discussed in many existing algorithms [14], [17], [18], [22]. The assumption of the implemented key management scheme is that an adversary might be a PU for some time and the TA keeps all user secret keys secretly.

i) Resistance to replay attack: In a replay attack, the malicious user re-injects the previously received messages or packets back into the VANET. To protect our system from replay attack and provide freshness to messages, our proposed scheme maintains time stamps to keep a cache of recently received messages through which the newly received messages can be compared.

ii) Masquerade and sybil attacks: In this section, we analyze the security properties of our proposed dual authentication scheme and will show how the scheme is effective for resisting masquerade and Sybil attacks. In many existing approaches, TA is unable to distinguish an authentication effort from a malicious attacker. Because, the malicious attacker makes use of real users' authentication efforts with stolen passwords, usernames and secret keys, and the TA still considers the attackers as real users. In this paper, we have used a novel dual authentication scheme, which can effectively oppose the malicious behavior of the attackers that is previously mentioned. In our proposed authentication scheme, even if the attacker knows VSK of any vehicle user, the OBU verifies the fingerprint of the vehicle user. If it doesn't match, the particular vehicle is not allowed to make communication with VANETs. Hence, the masquerade and Sybil attacks are successfully prevented in our dual authentication scheme.

iii) Message tampering/fabrication/alteration attack: In our scheme, the messages are encrypted using the group keys in the group communication before they are sent among the groups. For example, the TA sends messages to the PUs group by encrypting the messages using the PUs group key k_{pug}. Therefore, no one can delete, modify and alter the content of the messages during the transmission between the TA and PUs. Since, the group keys are managed by the TA, an intruder will not be able to find the key in a feasible amount of time to communicate with the group.

iv) Backward secrecy: Backward secrecy is the technique of preventing a new PU from accessing the previous communication before joining the group. In order to access the previous communication, an adversary needs to obtain the previous group key. Moreover, if the adversary becomes a PU in a group, it may try to derive the previous group key which is not permitted. In the proposed group key management scheme, when the newly updated group key is communicated to old group members, an adversary needs to find any one of the PUs secret key. Moreover, all the $PUSK$'s are randomly selected from a large set of positive integers with respect to the multiplicative group. Even if the adversary finds any one of the PUs secret key $PUSK_i$, then the adversary cannot use this $PUSK_i$. Because, we use dual authentication scheme in this proposed approach to participate in VANET communication. When the adversary tries to use any other PUs $PUSK_i$, the TA will also ask the adversary user to complete the authentication process to get authentication code before participating in the VANET's group communication. Moreover, if an adversary sends any information without including the authentication code, then the receiving vehicles will not process the information. This property makes the situation infeasible for the adversary to use any other PUs secret key. Consequently, the adversary cannot access the communication sent before join, which means the proposed approach supports the initial security requirement.

v) Forward secrecy: Forward secrecy is the technique of preventing a PU from accessing current communication after leave operation. When a PU leaves the group, he or she may try to derive the group key by using any attacking methods. In the proposed algorithm, it is infeasible for a PU to compute the current group key after the leave operation from the group that was explained for the backward secrecy technique. Because, when a PU v_i leaves from the group, the TA subtract his or her share value such as multiplication of x_i and y_i which is stored in var_i from μ value to produce μ'. This updated μ'

is multiplied by the newly generated group key value k'_{pug} to form the rekeying message γ'_{pug}. Therefore, a PU who had already left for the service cannot find the new group key in a feasible way since his or her personal keying information is not included. The PU who had left from the group may try to find k'_{pug} from the rekeying value which is sent as a broadcast message from the TA in an infeasible method. In order to do that, the PU has to multiply his or her secret key value with all the numbers starting from 1 to q where q is the maximum limit of group key value. At a certain point, it will give a value $\vartheta = k'_{pug}$ (i.e. $PUSK_i \times \omega = \vartheta$). After finding this ω value, the PU v_i can find a set of numbers S that will divide the number ω. Therefore, the value of S is defined as the set of numbers $\{\omega \bmod 1, \omega \bmod 2, \ldots, \omega \bmod \omega\} = 0$. Among the set of numbers, newly generated group key k'_{pug} is also one of the number (i.e., $k'_{pug} \in S$). In this case, if the size of $PUSK_i$ is w bits, then the attacker has to perform 2^w multiplication. The time taken to derive k'_{pug} can be increased by choosing a large $PUSK_i$ for each VANET user's secret key. In this work, the size of $PUSK_i$ must be 1024 bits and prior experiments were conducted with 128 bits, 256 bits and 512 bits. After finding the set of values S that divides the number ω, the attacker (user left from the group) can find the new group key by selecting the values from the set S by using brute force attack by making 2^{s-1} attempts. Consequently, an adversary cannot find the group key in a feasible method in order to access the current communication, which means the second security requirement is also supported in our proposed algorithm.

vi) Collusion attack: The Collusion attack is the one in which two or more adversaries act as legitimate PUs when they are participating in the group and then cooperatively compute the updated group key after leaving the group. Since, the value of var_i is subtracted from μ after the leaving operation is performed in a multicast group, any number of prior user's collision will not be used to gain information about the congruence system and to derive the updated group key k'_{pug} as long as the pairwise relatively prime numbers are large. The following scenario describes a kind of collusion attack in which two adversaries act as legitimate users. Consider v_1 as an adversary A who knows the key values $PUSK_1$, k_{pug} and v_3 as an adversary B who knows the key values $PUSK_3$ and k_{pug} at time '$t-2$'. In time '$t-1$', the adversary A leaves the group with the key values $PUSK_1$ and k_{pug}. B receives the rekeying message γ'_{pug} from the TA at the time 't' and computes k'_{pug}. In time '$t+1$', B leaves the group with the two key values $PUSK_3$ and k'_{pug}. Both of these adversaries exchanges their known key values $PUSK_1$, k_{pug}, $PUSK_3$ and k'_{pug}. Using these known values, the adversaries A and B cannot cooperatively find the updated group key k'_{pug} which is broadcast at time '$t+2$' in a feasible amount of time since their shares var_1 and var_3 are excluded from μ.

VII. Performance Analysis

We consider two performance metrics in our proposed scheme, namely the computation time and communication time for updating the group key in order to perform secure group communication in the PUs of VANET communication. The computation time is defined as the time taken to compute group key at the TA when group membership changes in the VANET group. The communication time is defined as the time taken to broadcast the amount of information from TA in order to make the VANET users to recover the group key. Table II shows the computation and storage complexities of various key management approaches, namely Chinese Remainder Group Key (CRGK) [15], Fast-Chinese Remainder Group Key (FRGK) [11], Key-tree Chinese Remainder Theorem (KCRT) [16], Number Theory Research Unit (NTRU) [24] and Elgamal Group Key Management (EGKM) [24] and our proposed VANET Group Key Management (VGKM) which are based on the CRT. The notations used for comparisons are defined as: n is the number of users, τ is the maximum number of children of each node of the tree, EEA is the time taken to find the inverse element of a multiplicative group using Extended Euclidean Algorithm, exp represents the exponential operation, M represents the multiplication operation, D represents the division operation, A represents the addition operation and S represents the subtraction operation.

TABLE II
Computation, Storage and Communication Complexities

Parameters	CRGK	FRGK	KCRT	NTRU	EGKM	VGKM
Computation Cost (TA)	$O(n)$ $(xor + A + M + EEA)$	$O(n)$ $(xor + A + M)$	$O(log_\tau n)$ $+ A + M + EEA)$	$O(n)(M + A + D + EEA)$	$O(n)(M + A + D + EEA)$	$O(1)$ $(A \text{ or } S)$
Computation Cost(User)	$1mod + 1xor$	$1mod + 1xor$	$1mod + 1xor$	$(2M + 1A + 1mod + 1EEA)$	$(1M + 1exp + 1mod + 1EEA)$	$1mod$
Storage Complexity (user)	2	2	$(log_\tau n)$	4	3	2
Storage Complexity (TA)	$2n+1$	$4n + 1$	$2n-1$	$2n+7$	$2n+5$	$4n+3$
Communication Complexity	1 *broadcast*	1 *broadcast*	1 *broadcast*	n	n	1 *broadcast*

Among these schemes, the Number Theory Research Unit (NTRU) based group key management scheme uses a multiplication ring from which it chooses some polynomial values as private and public keys from which it computes a common group key. Hence, the multiplication operation used in this scheme is performed by using the convolution product method. All the remaining schemes use a multiplicative group for choosing and computing the keys. Moreover, all the existing schemes take $O(n)$ for updating the group key when a single authorized vehicle user joins or leaves from the secure VANET communication. From Table II, it is evident that all the existing approaches take more computation complexity if it is used in the TA side in the VANET for computing the group key for

performing a single user join/leave operation which is very high in comparison with our proposed approach. Therefore, our proposed approach takes less computation complexity when it is compared with all the remaining five approaches since it takes only 1 subtraction operation or (addition) operation to be performed when a single user leave or join operation is performed. Moreover, the proposed approach doesn't perform any cyclic convolution product operation and multiplicative inverse operation on the user side which reduces user's computational complexity. The amount of information bits necessary to be communicated while updating the group key to our proposed approach and existing approaches are calculated and are also shown in Table II. It is very clear that our proposed group key management scheme takes the same communication complexity as that of most of the existing group key management protocol which are based on CRT.

The proposed method has been executed in JAVA (Intel Core i3 processor, 2GB RAM, 500 GB Hard disk, Windows XP Operating System) for a group of 1000 nodes and each node is considered as a VANET user. For implementing this authenticated group key management scheme suitable for VANET, the TA generates $PUSK_i$ values for 1000 nodes randomly. The $PUSK_i$ values used in this approach are 1024 bit positive integers which are relatively prime. For generating large integers in our program, we use BigInteger class that supports various methods for handling large positive integers. The method multiply() supported by BigInteger class is used to multiply all users secret key into a variable which will be used to find x_i and y_i values. The method modInverse() is used to find the multiplicative inverse of a given element with respect to the size of the multiplicative group. Our proposed group key computation scheme takes less computational complexity because it takes only addition or subtraction operation in the key updating process. Moreover, for computing the group key in all the existing approaches present in the literature, we measured the computation time separately for x_i which is obtained by dividing ∂_g and y_i which is obtained by finding the multiplicative inverse for x_i. All the existing algorithms shown in Table II takes more computational time for calculating x_i and y_i values, which would increase the computing load of the TA in VANETs. In the proposed approach, computational complexity is very much reduced because 1) calculating x_i and y_i value is neglected by storing them in the TA's server storage area and 2) multiplying x_i with y_i is also reduced, which is done in the TA initialization phase. Therefore, our proposed VGKM approach reduces the computing load of TA by slightly increasing the storage overhead of the TA.

The graphical results shown in Fig. 5 are used to compare the group key computation time of TA for our proposed method with the existing methods. It compares the results obtained from our proposed VGKM with CRGK, FRGK, KCRT, NTRU and EGKM. From Fig. 5, it is observed that when the key is 512 bits, the group key computation time of TA is found to be 19 ms in our proposed approach, which is better in comparison with the other existing schemes. The results shown in Fig. 6 are used to compare the PUs key recovery time of our proposed method with the existing methods. It compares the results obtained from our proposed scheme with existing approaches

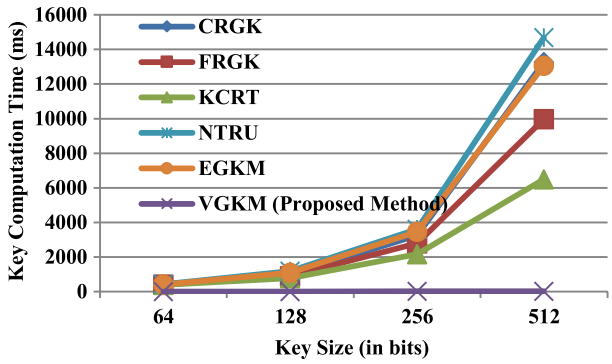


Fig. 5. Group key Computation Time at TA side.

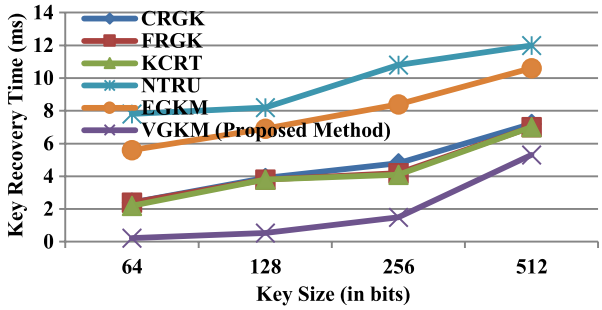


Fig. 6. PUs Key Recovery Time in the VANET.

and it is observed that when the key size is 512 bits, the key recovery time of a user is found to be 5.3 ms in our proposed approach, which is better in comparison with the other existing schemes.

VIII. Conclusion

In this paper, we proposed a new dual authentication scheme for improving the security of vehicles that are communicating with the VANET environment. For providing such authentication in dual mode, we used two components such as hash code and fingerprint of each communicating vehicle user. Therefore, the fingerprint authentication technique is integrated into a hash code creation method in this paper to avoid malicious users to use the secret key of any VANET users in order to participate in the VANET communication. Moreover, to avoid malicious users from spoofing the authentication code issued for any VANET users and sending erroneous messages to other vehicles we have introduced a new dual key management scheme in this research paper. The dual key management scheme implemented in this paper is computationally efficient that supports secure data transmission from TA to PUs and PUs to SUs based on two different group keys, one for PUs and another one for SUs for further improving the security among different classes of vehicles. Moreover, our proposed algorithm also takes single broadcast messages from TA to inform the group members in order to recover the updated group key. The future development of this work is to devise new methods in order to preserve the vehicle's location privacy from the intruders.

APPENDIX

TABLE III
FUZZY RULES SPECIFICATION

Rule No	Fuzzy rules
1	**IF** the front vehicle break change is high and vehicle density is very high and the road width is low **THEN** the traffic is high.
2	**IF** the front vehicle break change is high and vehicle density is very high and the road width is medium **THEN** the traffic is high.
3	**IF** the front vehicle break change is high and vehicle density is very high and the road width is high **THEN** the traffic is high.
4	**IF** the front vehicle break change is medium and vehicle density is high and the road width is low **THEN** the traffic is high.
5	**IF** the front vehicle break change is high and vehicle density is medium and the road width is low **THEN** the traffic is medium.
6	**IF** the front vehicle break change is high and vehicle density is medium and the road width is medium **THEN** the traffic is medium.
7	**IF** the front vehicle break change is high and vehicle density is medium and the road width is high **THEN** the traffic is medium.
8	**IF** the front vehicle break change is medium and vehicle density is high and the road width is high **THEN** the traffic is medium.
9	**IF** the front vehicle break change is medium and vehicle density is medium and the road width is low **THEN** the traffic is medium.
10	**IF** the front vehicle break change is medium and vehicle density is medium and the road width is medium **THEN** the traffic is medium.
11	**IF** the front vehicle break change is medium and vehicle density is medium and the road width is high **THEN** the traffic is medium.
12	**IF** the front vehicle break change is low and vehicle density is medium and the road width is low **THEN** the traffic is low.
13	**IF** the front vehicle break change is low and vehicle density is medium and the road width is medium **THEN** the traffic is low.
14	**IF** the front vehicle break change is low and vehicle density is medium and the road width is high **THEN** the traffic is low.
15	**IF** the front vehicle break change is medium and vehicle density is low and the road width is low **THEN** the traffic is low.
16	**IF** the front vehicle break change is medium and vehicle density is low and the road width is medium **THEN** the traffic is low.
17	**IF** the front vehicle break change is high and vehicle density is low and the road width is high **THEN** the traffic is low.
18	**IF** the front vehicle break change is low and vehicle density is low and the road width is low **THEN** the traffic is very low.
19	**IF** the front vehicle break change is low and vehicle density is low and the road width is medium **THEN** the traffic is very low.
20	**IF** the front vehicle break change is low and vehicle density is low and the road width is high **THEN** the traffic is very low.

REFERENCES

[1] L. Wischhof, A. Ebner, and H. Rohling, "Information dissemination in self-organizing intervehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 6, no. 1, pp. 90–101, Mar. 2005.

[2] X. Sun, *et al.*, "Secure vehicular communications based on group signature and ID-based signature scheme," in *Proc. IEEE ICC*, 2007, pp. 1539–1545.

[3] A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET," *Int. J. Comput. Sci.*, vol. 2, no. 1, pp. 88–96, 2013.

[4] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 248–262, Jan. 2011.

[5] K. Mershad and H. Artail, "A framework for secure and efficient data acquisition in vehicular Ad Hoc networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 2, pp. 536–551, Feb. 2013.

[6] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[7] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 616–629, Mar. 2011.

[8] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Security*, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[9] A. Wasef, Y. Jiang, and X. Shen, "ECMV: Efficient certificate management scheme for vehicular networks," in *Proc. IEEE GLOBECOM*, New Orleans, LA, USA, 2008, pp. 1–5.

[10] W. Shen, L. Liu, and X. Cao, "Cooperative message authentication in vehicular cyber-physical systems," *IEEE Trans. Emerging Topics Comput.*, vol. 1, no. 1, pp. 84–97, Jun. 2013.

[11] I. Syamsuddin, T. Dillon, E. Chang, and S. Han, "A survey of RFID authentication protocols based on hash chain method," in *Proc. 3rd ICCIT*, 2008, vol. 2, pp. 559–564.

[12] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *RSA Crypto.*, vol. 5, no. 2, pp. 2–13, Aug. 2002.

[13] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy preserving vehicular communication framework," in *Proc. IEEE INFOCOM*, Anchorage, AK, USA, May 2007, pp. 103–108.

[14] C. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," *IEEE/ACM Trans. Netw.*, vol. 8, no. 1, pp. 16–30, Feb. 2000.

[15] X. L. Zheng, C. T. Huang, and M. Matthews, "Chinese remainder theorem based group key management," in *Proc. 45th ACMSE*, Winston-Salem, NC, USA, 2007, pp. 266–271.

[16] J. Zhou and Y. H. Ou, "Key tree and Chinese remainder theorem based group key distribution scheme," *J. Chin. Inst. Eng.*, vol. 32, no. 7, pp. 967–974, Oct. 2009.

[17] J. A. M. Naranjo, J. A. L. Ramos, and L. G. Casado, "A suite of algorithms for key distribution and authentication in centralized secure multicast environments," *J. Comput. Appl. Math.*, vol. 236, no. 12, pp. 3042–3051, Jun. 2012.

[18] P. Vijayakumar, S. Bose, and A. Kannan, "Centralized key distribution protocol using the greatest common divisor method," *Comput. Math. Appl.*, vol. 65, no. 9, pp. 1360–1368, May 2013.

[19] N. V. Vighnesh, N. Kavita, R. Shalini, and S. Sampalli, "A novel sender authentication scheme based on hash chain for vehicular ad-hoc networks," in *Proc. IEEE Symp. ISWTA*, Langkawi, Malaysia, 2011, pp. 96–101.

[20] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing vehicular communications-assumptions, requirements, and principles," in *Proc. 4th Workshop ESCAR*, Lausanne, Switzerland, 2006, pp. 5–14.

[21] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. IEEE ICC*, Beijing, China, May 19–23, 2008, pp. 1451–1457.

[22] L. Veltri, S. Cirani, S. Busanelli, and G. Ferrari, "A novel batch based group key management protocol applied to the Internet of things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2724–2737, Nov. 2013.

[23] S. Busanelli, G. Ferrari, and L. Veltri, "Short-lived key management for secure communications in VANETs," in *Proc. IEEE Int. Conf. ITST*, St. Petersburg, Russia, 2011, pp. 613–618.

[24] X. Lv, H. Li, and B. Wang, "Group key agreement for secure group communication in dynamic peer systems," *J. Parallel Distrib. Comput.*, vol. 72, no. 10, pp. 1195–1200, Oct. 2012.

[25] P. Vijayakumar, S. Bose, and A. Kannan, "Chinese remainder theorem based centralized group key management for secure multicast communication," *IET Inf. Security*, vol. 8, no. 3, pp. 179–187, May 2014.

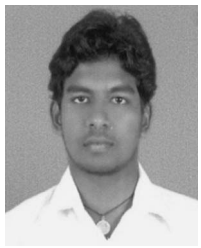
[26] X. Sun, X. Lin, and P.-H. Ho, "Secure vehicular communications based on group signature and id-based signature scheme," in *Proc. IEEE ICC*, Jun. 2007, pp. 1539–1545.

[27] K. Matusiewicz, J. Pieprzyk, N. Pramstaller, C. Rechberger, and V. Rijmen, "Analysis of simplified variants of SHA-256," in *Proc. WEWoRC*, Louvain, Belgium, Jul. 2005, pp. 1–12.

[28] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 736–746, Sep. 2011.

[29] X. Cheng, L. Yang, and X. Shen, "D2D for Intelligent transportation systems: A feasibility study," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 1784–1793, Aug. 2015.
[30] X. Cheng *et al.*, "Electrified vehicles and the smart grid: The ITS perspective," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 4, pp. 1388–1404, Aug. 2014.
[31] R. Zhang, X. Cheng, L. Yang, X. Shen, and B. Jiao, "A novel centralized TDMA-based scheduling protocol for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 1, pp. 411–416, Feb. 2015.
[32] X. Shen, X. Cheng, L. Yang, R. Zhang, and B. Jiao, "Data dissemination in VANETs: A scheduling approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 5, pp. 411–416, Oct. 2014.
[33] X. Lin *et al.*, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 4987–4998, Dec. 2008.
[34] L. J. Deborah, R. Sathiyaseelan, S. Audithan, and P. Vijayakumar, "Fuzzy-logic based learning style prediction in e-learning using web interface information," *Proc. Eng. Sci.*, vol. 40, no. 2, pp. 379–394, Apr. 2015.

Pandi Vijayakumar received the Bachelor of engineering degree from Madurai Kamaraj University, Madurai, India, in 2002; the Master of engineering degree in computer science and engineering from Karunya Institute of Technology, Coimbatore, India, in 2005; and the Ph.D. degree in computer science and engineering from Anna University, Chennai, India, in 2013. He is currently working as a Dean in charge of University College of Engineering Tindivanam, a Constituent College of Anna University Chennai, Tindivanam, India. His main thrust research areas include key management in network security, VANET security, and multicasting in computer networks.



Maria Azees received the B.E. degree in ECE and the M.E. degree in applied electronics from St. Xavier's Catholic College of Engineering, Nagercoil, India, affiliated under Anna University, Chennai, India, in 2011 and 2013, respectively. He is currently working toward the Ph.D. degree with Anna University. His research interests include security and privacy for VANETs.

Arputharaj Kannan received the Master of engineering and Ph.D. degrees in computer science and engineering from Anna University, Chennai, India, in 1991 and 2000, respectively. After completing the master's degree, he worked as an Assistant Professor with Anna University, where he is presently working as a Professor with the Department of Information Science and Technology, Faculty of Information and Communication Engineering. He has successfully produced more than 20 Ph.D. candidates. He is the author or coauthor of more than 100 papers in several reputed journals such as Elsevier, Springer, IET, etc. His main thrust areas of interest include artificial intelligence and database management systems.

Lazarus Jegatha Deborah received the Bachelor of engineering degree from Madurai Kamaraj University, Madurai, India, in 2002; the Master of engineering degree in computer science and engineering from Karunya Institute of Technology, Coimbatore, India, in 2005; and the Ph.D. degree in computer science and engineering from Anna University, Chennai, India, in 2013. She is presently working as an Assistant Professor with and the Head of the Department of Computer Science and Engineering, University College of Engineering Tindivanam, Tindivanam, India (a constituent college of Anna University).