Securing Vehicular Ad Hoc Data Transmission by Dual Authentication and Group Key Management Techniques

Kanimozhi.R[1], Lakshmi Priya.B[2], Mohanaselvi.K[3],Kavitha Subramani[4]

[1] *Student, Department of Computer science, Panimalar Engineering College, Tamil Nadu, India*
[2] *Student, Department of Computer science, Panimalar Engineering College, Tamil Nadu, India*
[3] *Student, Department of Computer science, Panimalar Engineering College, Tamil Nadu, India*
[4] *Professor, Department of Computer science, Panimalar Engineering College, Tamil Nadu, India*

ABSTRACT

VANET is a self-organizing communication network that is constructed among the moving vehicles. VANET have recently become popular for research, with attention to improve the driving experience and road safety. VANET usually encompass Trusted Authority (TA) that is meant to supply online premium service to nodes in network. It is necessary to keep up the authentication and confidentiality of the messages transmitted between the TA and nodes. Hence we address the security issues and challenges where TA classifies the VANET nodes into primary, secondary and unauthorized users. We propose dual authentication scheme to produce advanced security level to effectively stop the unauthorized vehicle going in VANET environment using smart card. Second, we tend to propose a group key management theme with efficiency distribute a group key to different VANET nodes. From this project, we must send the messages or some safety information from the Trusted authority to the primary user and the primary user to the secondary user with full of secured process.

Keywords: *Authentication, vehicle secret key, Chinese remainder theorem, group key management, VANET*

1. INTRODUCTION

VEHICULAR Ad-hoc Network (VANET) is a disseminated, self-arranging correspondence organize, which is assembled among moving vehicles. Due to the promising features and their security properties, VANETs have a great attention in the research community in recent years. A VANET comprises of three noteworthy parts, specifically the Trusted Authority (TA), Road Side Units (RSUs) and vehicles. The TA gives an assortment of online premium administrations to the VANET clients through RSUs. The RSUs are settled at the street sides which are utilized to interface the vehicles to the TA. Every vehicle is introduced with an On Board Unit (OBU) which is utilized to perform all calculation and correspondence assignments. Different factual contemplates uncover that because of street mischance's, many people have either died or injured and the traffic jams generate a tremendous waste in futility and fuel. So as to take care of these issues and to improve the driving comfort, proper activity data ought to be given to the drivers in a shrewd and secured way. Therefore, VANETs are created to give appealing administrations for example, wellbeing administrations that incorporate bend speed notices, crisis vehicle notices, path evolving help, person on foot crossing notices, movement sign infringement notices, street crossing point notices and street condition warnings. Likewise, it can offer the solace administrations, for example, climate data, activity data, area of petrol stations or eateries, and intelligent administration, for example, Internet get to. Despite the fact that, these services make driving comfort, the Intelligent Transport System (ITS) innovation intensely relies on upon the intelligent security, security safeguarding conventions to upgrade the nature of encounter for the drivers and travelers without dread for their security and individual protection.

Two sorts of interchanges are performed in VANETs. The principal sort is the Vehicle to Vehicle (V2V) correspondence in which the moving vehicles can communicate with each other. The second sort is the Vehicle to RSU (V2R) correspondence in which the moving vehicles can speak with the RSUs which are found aside the streets. The V2V and V2R correspondences are completed utilizing the Dedicated Short Range Communications (DSRC) standard [2] through an open remote channel. Each RSU and OBU utilizes a DSRC radio, in view of IEEE 802.11p radio innovation to get to the remote channel alongside a directional or a unidirectional reception apparatus. In the event that a RSU needs to transmit a message to a particular area, a unidirectional reception apparatus is utilized. Since, V2V and V2R interchanges are performed through an open remote channel, these interchanges are powerless against different sorts of assaults, for example, impedance, listening stealthily, sticking, and so forth.

The primary step to ensure security in VANET is performed by providing an authentication mechanism through which it is easy to ascertain all the authenticated vehicles. Authentication is the way toward checking a client personality preceding allowing access to the system. It can be considered as the first line of insurance against gatecrashers. The validation procedure guarantees that lone substantial vehicles can be a piece of the gathering in VANET. In this paper, a new dual authentication scheme is proposed to give the security change in the vehicle's side to oppose noxious clients going into the VANET. After finishing the validation procedure, the TA can multicast the data to the validated vehicles. The verified vehicles can communicate that data to different vehicles in a secure way. To multicast the data from the TA side and to communicate the data from one vehicle to different vehicles, we have proposed a dual group key management technique utilizing Chinese Remainder Theorem (CRT)[1]. In this strategy, the TA generates two different group keys for two different groups of users, namely primary user group and secondary user group. In the group keys generated, 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 mutual cryptographic gathering keys ought to be invigorated through an appropriate dashing operation at the season of gathering enrolment changes due to new clients joining into the system or old clients taking off from the system. In this way, an old gathering part has no access to present interchanges (forward secrecy) and another part has no entrance to past interchanges (in reverse secrecy). The proposed dual group key management scheme conspire limits the computational cost of the TA and gathering individuals in the rekeying operation. To accomplish this objective, the TA performs just straightforward expansion and subtraction operations to upgrade the group key. Correspondingly, every vehicle client of the multicast gather performs just a single modulo division operation for recovering the upgraded key when the gathering participation changes. The major commitments of this paper are compressed as takes after.

1) We propose a protected dual authentication scheme with the ability of forestalling malignant vehicles entering into the VANET framework.

2) We present a group key management technique into the VANET to disperse the data from the TA side to the group of vehicle user's in an astute and secure way.

3) We get the computational multifaceted nature of our proposed double key administration conspire as O (1) in both the TA and vehicle clients and henceforth it is reasonable for VANETs.

4) The correspondence many-sided quality of our proposed double key administration plan is likewise O (1) which implies that our conspire takes just a single communicate to educate the redesigned keying data from the TA to vehicle aggregate.

2. RELATED WORK

Jiun-Long Huang [3] proposed an ABAKA (An Anonymous Batch Authenticated and Key Agreement Scheme) which is to tackle the problems, including security, efficiency, and scalability problem. ABAKA scheme is to build a secure environment for value-added services in VANETs. The concept of batch verification to authenticate multiple requests sent from different vehicles using elliptic curve cryptography (ECC). ABAKA scheme to authenticate multiple requests sent from different vehicles and establish different ensure the confidentiality session keys. ABAKA is a suitable scheme for value-added services in VANETs. Stefano Busanelli, Gianluigi Ferrari, and Luca Veltri propsed a Short-lived Key Management scheme[6] which is used to tackle the problems such as connectivity is limited and communication with a central certification authority might be problematic. The group-keys are derived from a couple of independent hash chains for generating onetime

passwords.MD-5, SHA-1.Symmetric cryptographic algorithm to offer group-level confidentiality and group-level integrity services. No per-user authentication and non-repudiation is provided.

Yong Hao[4] proposed A Distributed Key Management Framework With Co-operative Message Authentication in VANET which is to tackle the large computation overhead due to the group signature implementation . A cooperative message authentication protocol [9] is proposed to alleviate the verification burden. Malicious vehicle cannot enter into VANET and privacy is preserved. Security attacks are possible. Anup Dhamgaye and Nekita Chavhan[10] proposed a scheme which routes the data efficiently from source to destination. Many protocols such as Proactive and Reactive routing Protocols, Source routing or hop by hop routing is used. It selects the best path with least time and least expensive route. The best route from source to destination is found. Different types of attack on routing protocols in VANET. Irfan Syamsuddina, Tharam Dillonb, Elizabeth Changc, and Song Hand [2] which is used to tackle the security and the privacy problems in RFID communications. There are several protocols have been proposed to overcome those problems. Hash chain [7] is commonly employed by the protocols to improve security and privacy for RFID authentication. Although the protocols able to provide specific solution for RFID security and privacy problems, they fail to provide integrated solution.

WENLONG SHEN, LU LIU, XIANGHUI CAO (Member, IEEE), YONG HAO AND YU CHENG (Senior Member, IEEE) [9] proposed a scheme which is used to tackle large computation overhead caused by the safety message authentication. A cooperative message authentication protocol (CMAP) is developed to alleviate vehicles' computation burden. All the vehicles share their verification results with each other in a cooperative way, so that the number of safety messages that each vehicle needs to verify reduces significantly. Security is the major issue. Huang,misra,verma,xue [5] proposed a scheme which is used to solve the generation of pseudonyms for anonymous communication. We have proposed a novel PACP (Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs) protocol for the vehicles in VANETs for such that the pseudonyms are only known to the vehicles but have no other entities in the network. Confidential privacy is provided to the vehicles. It is suitable only for small scale VANET test bed.

Edward David Moreno[11] proposed a system in which messages are exchanged in a secure way in VANET by using RSA, ECC and MQQ ALGORITHMS. The main purpose of a VANET is to provide highway passengers with security. Hence one should emphasize the importance of providing security to the data that travels on this type of ad hoc network. Khaleel Mershad and Hassan Artail proposed a framework for A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks [8] which is used to tackle Many forms of attacks against *service-oriented* VANETs that attempt to threaten their security have emerged. It provides Privacy-preserving data acquisition and forwarding scheme by introducing a novel and provable cryptographic algorithm for key generation and powerful encryption. It provides more efficiency and effectiveness compared to previous systems. System is not more scalable in terms of the number of users that can connect to an RSU. Vighnesh N V, N Kavita proposed a system which is a novel sender authentication scheme based on hash chain method [7] for VANET. Authentication is a major security goal to be achieved in VANET. Current scheme focuses only on sender authentication. Xinliang Zheng, Chin-Tser Huang, Manton Matthews proposed a CRT [1] scheme which is used to reduce the computing load onto the key server. We optimize the number of re-key broadcast messages, user-side key computation, and number of key storages. Re-keying computation to be done pre-emptively, which means when a user-join or user-leave event happens the response time for the key server to send out the new group key can be very short. Even though we evaluate our protocol performance using some O-notations, the unit operations of our protocols is different from most other protocols which can cause real performance results to be deviated. Pandi Vijayakumar, Maria Azees[12] proposed a new dual authentication scheme which is used provide the security improvement in the vehicle's side to resist malicious users entering into the VANET. After 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. A key management scheme is computationally efficient compared with all other existing schemes. Security attacks are possible

3. EXISTING METHODOLOGY

Many existing plans accessible in the writing are utilized to give Authentication only. Among the different existing methods, proposed an Elliptic Curve Digital Signature Algorithm (ECDSA), which is

mathematically derived from the basic digital signature algorithm. ECDSA utilizes an asymmetric key pair which comprises of a public key and a private key. The public key used in this technique is a random generation from the private key. Both the public and the private keys are used for user authentication. The two attacking techniques that are performed in this strategy are the attacks on Elliptic Curve Discrete Logarithmic Problem (ECDLP) and the attacks on the hash function. Then they proposed a method for the management of computerized authentications, in particular Efficient Certificate Management Scheme for Vehicular Ad Hoc Networks (ECMV). This strategy depends on a Public Key Infrastructure (PKI). In this procedure, every vehicle has a short lifetime authentication and this endorsement can be refreshed from any RSU. This testament is every now and again refreshed to give security protecting verification, which makes an extra overhead. Agreeable Message Authentication Protocol (CMAP) to discover the data communicated by the malicious vehicles in the road transport framework. The helpful message validation is a promising strategy to mitigate vehicle's calculation overhead for message check. Nonetheless, the correspondence overhead increments when the thickness of vehicles is higher. The primary constraint of this technique is that if there is no verifier to confirm messages, then the malicious messages might be devoured by vehicle clients.

4. PROBLEMS IN THE EXISTING SYSTEM

The existing technique is used To Provide Authentication Only. Public key and Private Key are utilized. Each Vehicle has a Short Time digital Certificate. Vehicle's Certificate Provides Overhead. 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. Information is not confirmed.

5. PROPOSED WORK

The proposed method mainly includes five main phases namely Network Formation, Vehicle User's Authentication, Group Key Allocation and V2R & V2V Communication. In the Network Formation phase involves creating a Trusted Authority (TA) for monitoring the network. Then it involves creating RSU's and OBU's for communicating over the vehicles. The OBU's are devices that are embedded inside the vehicles. The services will be transmitted to the OBU's via RSU's. The OBU's which are in the range of RSU will be the vehicles in the range.

The next phase describes about the Vehicle User's Authentication, in this module, we have to authenticate the vehicle users with the Vehicle's Secret Key (VSK). This operation is used to authenticate the authorized users. In the existing system, unauthorized users are allowed to enter into the network. But in this authority will not give permission to the user to entering. This authentication will be performed using the hash code.

The next phase describes about the Group Key Management, in this module, we manage two keys for a RSU for authentication process. The two keys namely primary user key and Secondary User (SU) key. In our project, the Primary User (PU) only links directly with the authority. The secondary user links with the primary user for temperature conditions, road conditions etc. The services which come from authority will be received only by the primary user.

The next phase describes about the V2R & V2V Communication**,** in this, communication process is occurred for transmitting information's and services. First, communication between RSU and primary user will happen. Before receiving information by the primary user, it has to be checked by the authority whether it is an authorized primary user. Then it will transmit the information to the secondary user. It also has been verified by the primary user by the group key. The following diagram depicts the working of all the phases.

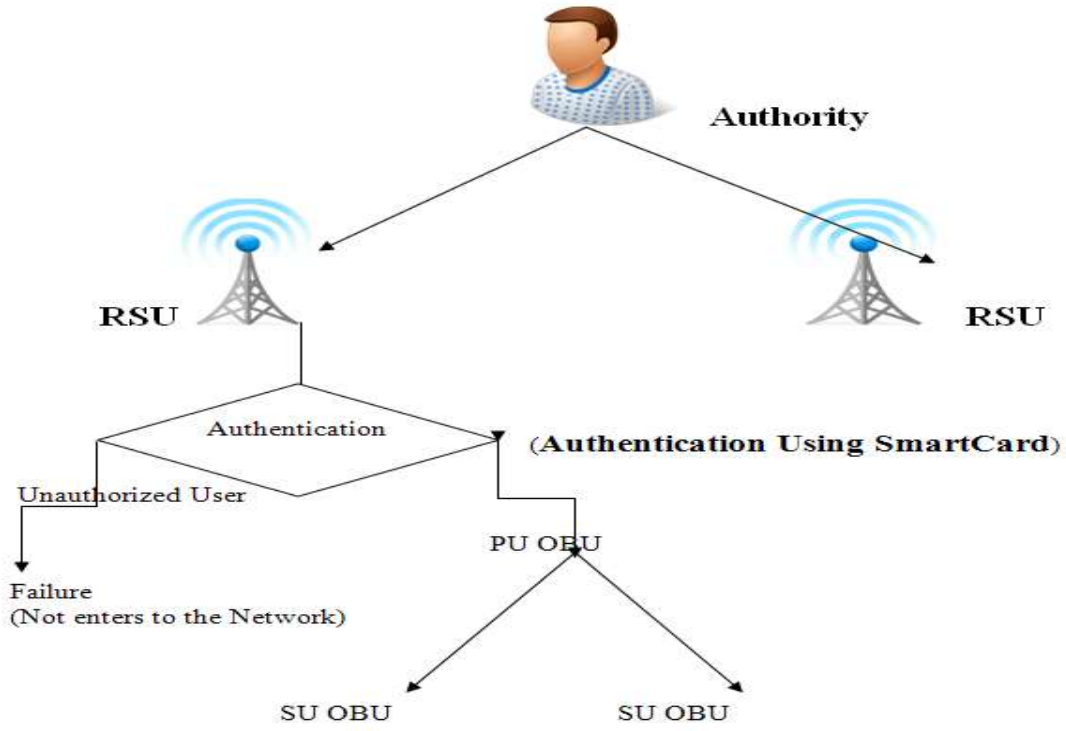

figure.1.SystemModel

6. PERFORMANCE ANALYSIS:

We consider two performance measurements in our proposed plot, namely the computation time and communication time for updating the group key to perform secure group communication in the PUs of VANET. The computation time is characterized as the time taken to figure group key at the TA when aggregate enrollment of group membership changes in the VANET environment. The communication time is characterized as the time taken to communicate the measure of data from TA to make the VANET clients to recoup the gathering key. Table I shows the computation and communication complexities of various key management approaches, namely Chinese Remainder Group Key (CRGK) [1], Fast-Chinese Remainder Group Key (FRGK), Key-tree Chinese Remainder Theorem (KCRT).

Parameter	**CRGK**
Computation cost(TA)	O(n)(xor+A+M+EEA)
Computation cost(User)	1mod+1xor
Communication Complexity	1 broad cast

Table I. Computation and Communication cost

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

We measured the computation time independently for xi which is acquired by partitioning ∂g and yi which is found by finding the multiplicative inverse for xi. All the current calculations appeared in Table I sets aside more computational time for figuring xi and yi values, which would build the processing load of the TA in VANETs. In the proposed approach, computational complexity nature is especially diminished in light of the fact that 1) ascertaining xi and yi esteem is disregarded by putting away them in the TA's server and 2) duplicating xi with yi is likewise lessened, which is done in the TA introduction stage.

Steps for computing the group key for PUs.

1) Compute $\partial g = \prod_{i=1}^{n} (PUSKi)$
2) Compute xi = $\frac{\partial g}{PUSKi}$ where i = 1, 2, 3, . . . , n
3) Compute *yi* such that $xi \times yi \equiv 1 \bmod PUSKi$

4) Multiply all users *xi* and *yi*values and store them in the variables var*i* = *xi* × *yi*
5) Compute the value $\mu = \sum_{i}^{n} vari.$

7. CONCLUSION

In this paper, we proposed a new dual authentication scheme for enhancing the security of vehicles that are communicating with the VANET environment. For giving such authentication in double mode, we utilized two parts such as hash code, Smart card. In this manner, Smart card is coordinated into a hash code creation technique in this paper to stay away malicious users from to utilize the secret key of any VANET users with a specific end goal to take an interest in the VANET correspondence. In addition, to avoid malicious users from stealing the authentication code issued for any VANET users and sending malicious messages to other vehicles we have introduced a new dual key management scheme in this paper. The dual key management technique 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 advancement of this work is to devise new strategies to save the vehicle's area security from the interlopers.

8. REFERENCES

[1]Chinese Remainder Theorem Based Group Key management, Manton Matthews, Xinliang Zheng , MARCH 2007.

[2]A Survey of RFID Authentication Protocols Based on Hash-Chain Method Irfan Syamsuddina, Tharam Dillonb, Elizabeth Changc, and Song Hand *aState Polytechnic of Ujung Pandang, Indonesia b,c,dDEBI Institute, Curtin University of Technology, Australia* , 2008 .

[3] ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks, Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien, JANUARY 2011.

[4] A Distributed Key Management Framework with Cooperative Message Authentication in VANETs , Yong Hao, *Student Member, IEEE*, Yu Cheng, *Senior Member, IEEE*, Chi Zhou, *Senior Member, IEEE*, and Wei Song ,MARCH 2011.

[5] PACP:An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs Dijiang Huang, *Senior Member, IEEE*, Satyajayant Misra, *Member, IEEE*, Mayank Verma, *Member, IEEE*, and Guoliang Xue, *Fellow, IEEE , SEPTEMBER 2011.*

[6]Short-lived Key Management for Secure Communications in VANETs Stefano Busanelli, Gianluigi Ferrari, and Luca Veltri Wireless Ad hoc and Sensor Networks (WASN) Laboratory Department of Information Engineering, University of Parma, Italy, 2011.

[7] A Novel Sender Authentication Scheme Based on Hash Chain for Vehicular Ad-Hoc Networks , Vighnesh N V,N kaviyha ,Dr. Shalini R ,Dr.Srinivas Sampalli , SEPTEMBER 2011..

[8]A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks , Khaleel Mershad and Hassan Artail , FEBRUARY 2013.

[9]Cooperative Message Authentication in Vehicular Cyber-Physical Systems WNLEONG SHEN, LU LIU, XIANGHUI CAO (Member, IEEE), YONG HAO, AND YU CHENG (Senior Member, IEEE) , JULY 2013.

[10]Survey on security challenges in VANET, 1Anup Dhamgaye, 2Nekita Chavhan , 2013.

[11**]**Impact of Asymmetric Encryption Algorithms in a VANET Edward David Moreno, Leila C.M. Buarque, Florêncio Natan, Gustavo Quirino and Ricardo Salgueiro , 2015.

[12] 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, IEEE, APRIL 2016.