International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Privacy Preserving Message Communication Scheme for VANET

Awanti Sujit Dhekane

New Horizon Institute of Technology, Department of Computer Engineering, Mumbai University, Mumbai, Maharashtra, India
Email: *awantidhekane[at]gmail.com*

Abstract: ***In the today's communication era, the wireless communication is made the drastic changes in the human lifestyle. Hence VANET i.e. Vehicular ad-hock network is the new technology implemented to provide communication between vehicles and also with road side unit like any traffic signal and important place so it provides secure way to travel and improve driving experience. In this VANET there are several methods can be implemented to avoid accidents and vehicle theft. Message communication is the first method. This message communication is implemented basically for providing the traffic details for each driver so that drivers can change the route to avoid congestion. Also, he can find the fastest route. In this method privacy preservation is also important. Each driver's identity must be hidden in the VANET and there must be also a way identified even if someone. In this system we provided 2 factor authentication for privacy preservation and message communication. Here we used certificate authority (CA)and textual driver password to achieve the goals. Here the system requires the several extreme light weight hashing processes and onetime password for message signing and verification between vehicles. Compared with previous schemes because of hashing process computation cost is reduced in multiple times. We use pseudonymous certificate to communicate with each other, so here the vehicle driver's identity is hidden successfully and third party cannot get identity of driver even if the RSU is compromised.***

Keywords: Privacy preservation of driver identity; Vehicular ad hoc network; Certificate authority; TWO-Factor Lightweight Privacy preserving; pseudonymous certificate

1. Introduction

Vehicular ad-hoc network are implemented to improve traffic jam conditions and also drivers' safety while travelling on the road. In this system the vehicle is equipped with on board unit which contains the vehicle details and through which you can communicate with other vehicles and road side units that is RSU. Road side unit also keep the information about the traffic conditions and the systems. VANET is used to transmit the safety information between vehicles to vehicles which helps to avoid the crashes in the system. There 2 types of messages are already available in various system which is helpful in traffic condition and road side safety.

1) Forward collision warning
2) Blind Spot warning

In this project forward collision warning message is used to send the data and between vehicle to avoid the accident by forward collision. Also, by forwarding message to one another it gets information about the accident. Hence the driver takes the action averts impeding the incidents. In vehicular ad hoc network there are 2 different types of security requirements, the first is due to inheritance from the Mobile ad –hoc network (MANET) and second is based on vehicular communication. There are different threats in wireless communication such as forgery attacks and eavesdropping. In vehicular ad-hoc Network due to forgery attack they modifications are done easily then this modification incurs basic security goals.

In the vehicular ad-hoc Network while the vehicles are communicating, they only transmit and receive the anonymous data between them. In the system there is basic data like driver name, identity, vehicle identification number (VIN), speed position, model.

In this paper we proposed the 2-factor authentication technique which include onetime password and certificate authority and it details with OTP and password verification for security purpose in the system.

Advantages of our system:

1) Confidentiality

VANET provides the confidential communication. Third party cannot access the message when it sent from one point to another point. Even if the communication made in group the person outside of group cannot decrypt any message in ad hoc network.

2) High non-repudiation-

In this VANET system the vehicle provides high non-repudiation so that vehicle could not stop itself from sending messages. Even if multiple drivers are already accessing the vehicle, vehicle is with the system that not allow to stop the messages from the system. In VANET driver has to enter his name and password to login in the system. After that user is authenticated, this password is used to start the vehicle. The evidences generated from this password is then transmitted to the certificate Authority and this data is used to trace the driver conditionally. Hence this system provides strong non –repudiation with security.

3) Privacy preservation:

In 2Flip the driver identity is always hidden even if the message is transmitted from one to another. In this case the privacy is always be preserved at the user level. In this system we provide authentication, anonymity and unlikability. In system the RSU having less responsibility that even if the RSU are compromised the third malevolent party cannot identify the identity and thus identity of the driver cannot be revealed.

2. Abbreviations and Acronyms

DSRC	Dedicated short-range communications
RSUs	Roadside units
V2V	Vehicle-to-vehicle
V2R	Vehicle-to-roadside unit
OBU	Onboard unit
FCW	Forward Collision Warning
BSW	Blind Spot Warning
MANET	Mobile ad hoc network
VIN	Vehicle identification number
PPA	Privacy preserving authentication
PKI	Public key infrastructure
CA	Certificate authority
2FLIP	TWO-Factor Lightweight Privacy preserving
MAC	Message authentication code
TPD	Tamper-proof device

3. Related Work

In previous research the system is made for effective and secure downloading of the data, when the vehicle is in the RSU range. So, they are able to use and share the data which is previously downloaded when the RSU is not in the range. In VANET previous research paper proposed application layer data sharing, so now we can share the data easily.
The key feature here is how vehicles share data among each other. An important provision of this application layer data sharing is that it guarantees the delivery of information file for each vehicle passing near from each road side unit.

Here is also the security issue is identified regarding privacy preserving in the data i.. e. sharing among the vehicles and road side units and identity of the vehicle drivers that vehicles drivers are using with all vehicle data. here the system is implemented as each sharing message is signed and encrypted with this the data is shared among the vehicles. Another research paper introduces the idea of privacy preserving based on the group signature. Group signature is anonymous authentication for vehicle. In this system the area is divided in the RSU range and the data sharing in that particular area is handled by the particular RSU. Previous system is based on the idea that hundreds of the messages need to be verified per second. But as the area is divided in several domains and road side unit are fully responsible for distributing group private keys and managing those keys and vehicles. Finally, the system works on the co-operative message authentication between vehicles which needed to checked in only few numbers of messages. So, this short and time saving and efficient process.

In this research work proposed we concentrate on the processing cost, resource cost and security problems in vehicular ad-hoc network. This new protocol is having smart card authentication system, in which we provide strong authentication using smart card and, in this system, we use dynamic login identity of the driver for message communication. In this way the system provides the security from password guessing, forgery attacks and impersonation attack and so on. In this research work the proposed system provide security against the threats in occurred in communication, computing and control technologies.

So, in the system we are having various challenges posed by the VANET include data integrity, confidentiality of identity, non-repudiation and access control of vehicle and privacy protection.

In the system the trust factor is defined by data that at what extent the data in the network can be trusted and node trust is defined as at what extent the node in the network is trusted. Attack resistant management system is used to detect the various attack in the system as well as is also compute the trustworthiness of both data and nodes. data trust is evaluated as the verification of data available from the nodes and node trust is evaluated in two-dimensional functional trust and recommendation trust. This is how the data in the system is trusted and functionality of the system is done and the node in the system are trusted.

In privacy preserving and authentication in vehicular ad-hoc network system there are several methods are used which are listed below:
1) Pseudonymous certificate
2) Group signature
3) Pseudonymous authentication and group signature

1) Pseudonymous Certificate Based Scheme
Each vehicle gets the pseudonymous certificate which include the certificate id and various secret keys which are linked together. Each node in the network get one pseudonymous certificate and keys in the certificate are used for message signing and communication. So, the real identity of the vehicle is hidden in this vehicle-to-vehicle communication.

2) Group Signature Based Schemes
In the group signature the message encrypted is distributed among the group. The secret key distribution is only among the group and each node in the group only calculate the private key which is used to decrypt the message in the system.

3) Hybrid schemes
It includes pseudonymous certificate scheme, digital signature-based scheme, MAC and other various message authentication technologies to make a reduction in between computation cost, CRL size, bandwidth of project consumption, verification delay, and so on. We used the pseudonymous certificate-based scheme for secure way for message communication and hide our vehicle identity

4. System Model

1) Network Model
In the Network model Certificate Authority (CA) is main. CA is the trustworthy authority which maintain the record of all the vehicles. CA has unlimited computation storage for computing and storing lots of data of vehicles.

This model contains following important components:
- RSU and Vehicle registration
- Vehicle information and system key management
- Message Non-Repudiation

Road side Unit and CA communication done by different channel as it having powerful communication capability up to 3 km. every vehicle is first registered to certificate authority with the on-board unit which provide pseudonymous certificate for the communication

RSU system on road side is able to make communication with CA directly by weird channel. It has massive storage capacity and powerful communication capability up to 3km. Every vehicle is Equipped with OBU which stores essential login information.

2) Adversary Model

Adversary Model is used in the system for eves drop all the messages. It can control whole communication channel. An adversary model is used to find if any legitimate vehicle is accepting wrong and harmful message without being known to main system.

5. System Features

Our proposed system contains the three parts
1) Vehicle Driver
2) Road Side Unit (RSU)
3) Certificate Authority (CA)

1) System Initialization and entity Information

In this system the vehicle user first registers the vehicle at the Certificate authority. It provides the car number, phone number, vehicle identification number, address details car documents. This all information provided by the driver is stored at the CA and the user is registered. After that CA assign the Pseudo identity with pseudonymous certificate and also verify driver's password.

2) Driver login

Driver using the first Correct Username and password to log in to the system. After that system is on and depending on the receiving information the vehicle generates the message sign it and broadcast it. Without username and password user cannot access the vehicle.

3) Message Signing

Message signing is done by the secret key available in the pseudonymous certificate in the vehicle and then message is broadcasted.

4) Message Verification

At the receiver stage the vehicle gets the message decrypt it and if it found useful then is takes otherwise reject the message.

5) System key updates

System key is important in this process CA provides the new method for updating the key.

6. Framework and Problem Definition

In previous research the driver's identity is not protected properly. also, the message signing at the RSU is overhead to the system. In this system we require strong driver identity protection. Message authentication, Message encryption these are very much important things in this proposed system. Privacy preserving of the vehicles is primary concern in this system. In this system the message in send by encrypting the message by the key which is available in the pseudonymous certificate. At the other end the encrypted message is decrypted and the data is gotten by receiver.

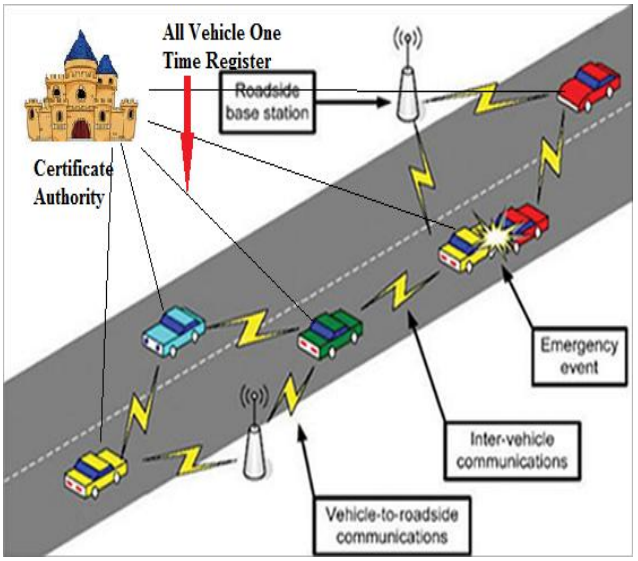

Figure 4.1: Basic Vehicular Ad-Hock Network System [6]

We proposed the privacy preserving authentication in the VANET which hide the driver's real identity while communicating in the network. In the proposed the system user uses the one-time password or user password to log in the on-board unit. The system introduces the fixed-on Board Unit in each vehicle which contains all the driver's data and login information. The system also able to identify the identity of the multiple drivers and allow them use the system.

In This system the 2 FLIP provides the V2V AND V2R private communication through the one-time password, login password and OTP for the system. We provide offline system key update for vehicle which not affect the performance. Up to current research and the new technologies evolving the great authentication system is important in this. This privacy preservation system is providing the strong privacy preservation and avoid the DOS attacks. It is the first and dynamic authentication scheme which authenticate multiple drivers.

Followings are the advantages of our proposed 2FLIP scheme:
1) Here the strong privacy preservation includes the preservation of the identity of Road side unit to vehicles communication and vehicle to vehicle communication. Vehicle can be more secured by the authentication scheme, user login and normal login and One time Password.
2) Secure system key update is important, when the system key is hacked the key is restored by the CA. This is important to maintain the practical system.
3) Offline password update: Driver needs to register the CA and if he wants to update the password in Onboard unit, he can able to do it offline

Pseudonymous certificate management overhead, communication cost and network delay is low in 2FLIP because of a dynamic pseudonymous identity. As compared to other current schemes, our proposed 2FLIP achieves a decrease in communication cost and a considerably lower network delay.

In the current system we use cryptography techniques to communicate between the vehicle to vehicle and vehicle to RSU units.

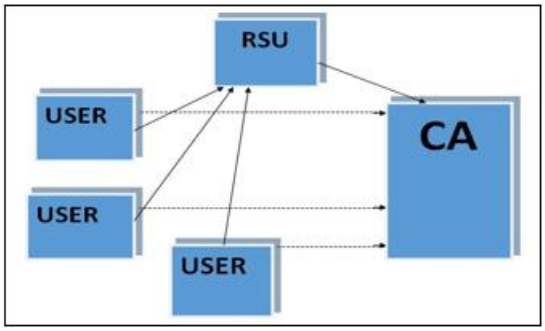

Figure 4.2: Deployment Model of the System

ALGORITHM 1: Proposed for Project:
Let S be the system,
S= {Input, Output, Functions, Success, Failure}

Were,
Input= {I1, I2, I3, I4}
Where, I1=Driver's data for registration
I2= Username and Password for login purpose
I3= Update Username and Password
Output= {O1, O2, O3, O4}

Where, O1=Provide the message of emergency on the road through secret key Cryptography
O2= Provide the traffic messages details thorough secret key cryptography

Functions= {F1, F2, F3, F4}
Were,
F1= The pseudonymous certificate generation on random key generation
F2= One time password for user registration
F3= Offline password updating on the On board unit F4= Pseudonymous certificate updating when request is come

Success= {S1, S2, S3}
Where S1= Message communication done properly
S2= Pseudonymous certificate is updated in regular time interval
S3= Privacy of the driver identity is preserved

Failure= {U1, U2}
Where U1= Pseudonymous certificate forgery not identified.

As seen in the algorithm the one message is broadcasted in several users and one driver can send the multiple messages at the same time.

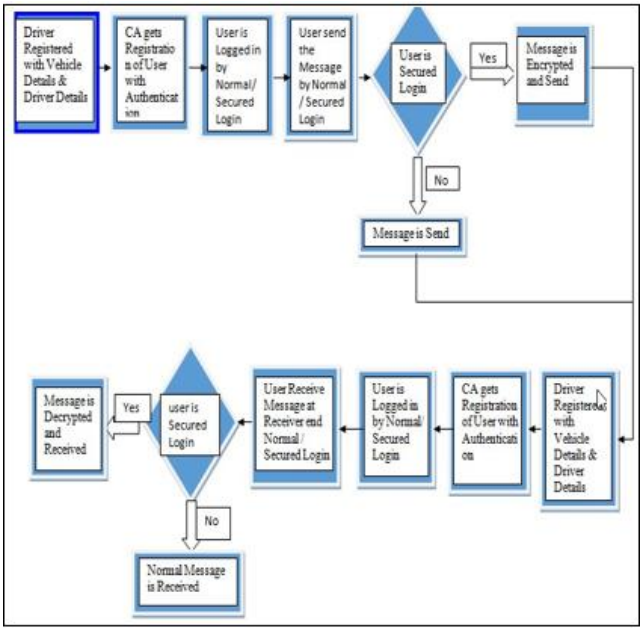

Figure 4.3: System Architecture

ALGORITUM 2: The **Time-based One-time Password Algorithm (TOTP)**

TOTP is an algorithm that computes a one-time password from a shared secret key and the current time. It has been adopted as Internet Engineering Task Force standard RFC 6238,[1] is the cornerstone of Initiative For Open Authentication (OATH), and is used in a number of two-factor authentication systems.

TOTP is based on hash-based message authentication code (HMAC). It computes the password by combining secret key with the current timestamp using cryptographic function which uses hashing.

This typical two factor authentication works as follows. First user enters the username and password for the system then system generates the one-time password for the server using TOTP which run in the on-board system. Once the password is generated user enter the password online system. Server also detect the password and calculate the one-time password using TOTP algorithm. This password generation allows the time delay interval of the 30 seconds in generation of the password. So, the generated password gets closer together and secret key will be equal.

For this work the clock of the user and the server must be roughly synchronized. A single secret key to be used for all the sessions must be shared in all this process of authentication and this must be done by secure channel

ALGORITHM 3: AES Algorithm for Encryption and Decryption of messages:

AES is developed by Rijndael. Rijndael is a cipher operates on blocks i. e. message is broken into blocks of a fixed length, and each block is encrypted separately. Rijndael operates on blocks having length 128-bit. There are 3 variants of messages in Rijndael cipher, each variants uses a different key length. The standard key lengths are 128, 192, and 256 bits.

Various operations are done and various intermediate results are calculated and saved. Operations which done on intermediate results are known as the state. The state results are 128-bits long. We think that state divided into 16 bytes, a(i,j) where $0 \leq i, j \leq 3$. These 16 bytes are as an array, or matrix, which having 4 rows and 4 columns, like so:

a(0,0) a(0,1) a(0,2) a(0,3)
a(1,0) a(1,1) a(1,2) a(1,3)
a(2,0) a(2,1) a(2,2) a(2,3)
a(3,0) a(3,1) a(3,2) a(3,3)

The state starts as the 128-bit input. We operate on this state by performing various successive rounds. A round is divided three different parts: applications of the S-box, sub key addition, and next is linear diffusion.

7. Result Analysis

At the first the driver has to Register to the CA with all the details of the driver.CA accept the details and save all the details to database. After that user is logged, the one-time password is sent to drivers on board unit for dual authentication which will register the User.

While communicating between V2V and V2R the message is encrypted and send and at the receiver end it get decrypted in the system.

At runtime 2 authorities i.e. Certificate Authority and Road Side Units are operating and several vehicles on road are in range. These all-system users are active at a same time and each vehicle send message o another vehicle as well as road side unit and by using this information the messages are broadcasted by the RSU to vehicle.

Certificate/System Key Updation Overhead
In the VANET these are thousands of vehicle systems active at same time so if the system key leakage problem is happened or problem related to pseudonymous certificate is only corrected by update in system key or certificate. As thousands of the users can request for updating of certificate at one time so the CA server have strong capacity for handling these requests

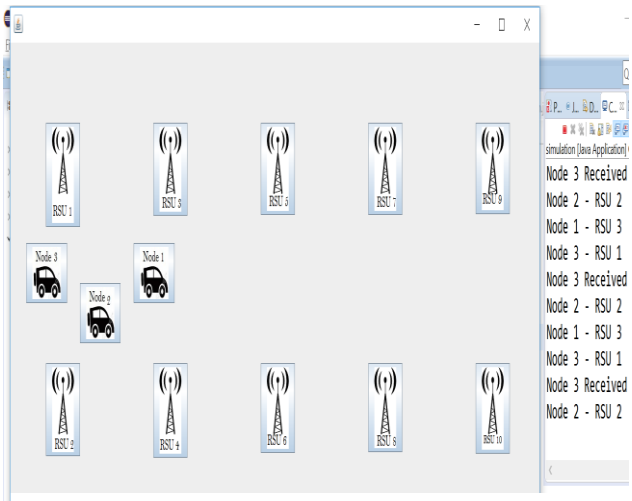

Figure 5.3: Nodes Communication with RSU

Handling Issue of Certificate Forging
To handle the issue of certificate forging we periodically update the certificate through the CA. for that adversary model is used to identify the message key are duplicate after that the certificates are updated.

8. Conclusion

In this paper, we proposed privacy preserving authentication scheme for VANET. so, by using various cryptography techniques we hide the message details. As well as the on-board unit generate the secret identity of the driver which will be shared along with all the messages.

The process of encryption and decryption enhance the message security and efficiency of communication and computation. This system has a outstanding performance on the secret message distribution, message signing, message verification and work good in network delays also.

References

[1] M. Raya, and J.-P. Hubaux, "The security of vehicular ad hoc networks," in Proc. 3rd ACM workshop on Security of ad hoc and sensor networks, Alexandria, VA, USA, 2005, pp. 11-21.
[2] L. Armstrong, "Dedicated short range communications (dsrc) home," 2002.
[3] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons and J. Wang, "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application," NHTSA, Washington, DC, Tech. Rep. DOT-HS-812-014, Aug. 2014.
[4] K. Ren and W. Lou, "Privacy-enhanced, attack-resilient access control in pervasive computing environments with optional context authentication capability," Mobile Networks & Applications, vol. 12, no . 1, pp. 79-92, 2007.
[5] M. Wang, D. Liu, L. Zhu, Y. Xu and F. Wang, "LESPP: Lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication," Computing, pp. 1-24, 2014.
[6] L. Brown and W. Stallings, "User Authentication," in Computer Security Principles and Practice, 2nd ed. New Jersey: Pearson, USA, 2012, pp. 71-105.
[7] M. Raya, and J.-P. Hubaux, "Securing vehicular ad hoc networks," J. Computer. Security., vol. 15, no. 1, pp. 39-68, 2007.
[8] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," Vehicular Technology, IEEE Transactions on, vol. 59, no. 7, pp. 3589-3603, 2010