Survey:- Privacy Preserving Authentication Scheme For VANET

Awanti Sujit Dhekane[1], Prof. Mrs. D. D. Gatade[2]
[1, 2] Department of Computer Engineering
[1, 2] Sinhgad College of Engineering, Pune -41, Savitribai Phule Pune University , Pune, Maharashtra.

Abstract- *In today's era wireless communication technologies reformed human's lifestyles by providing the best convenience and beneficial personal communication applications with the help of internet services. Recently, in vehicle manufacturers and telecommunication companies gear up to equip each car with the facility that allows the vehicle to vehicle communication with each other as well as with the roadside unit, which is located near by the road, such as at every traffic signal or any important location , in order to betterment in driving experience, facilitate secure driving, and enhance people safety.*

In Authentication and Privacy preserving in vehicular ad hoc network (VANET) paper requires secure and efficient authentication and communication with help of privacy preservation of every vehicle and also it requires facility to handle traffic details management. In this project proposed a TWO-Factor Light weight Privacy preserving authentication scheme to enhance the security of Vehicles in Ad-Hock Network communication. It includes the certificate authority (CA) Authentication and the textual Driver password based two factor authentication (2FA) to achieve the goals. System only requires several extreme lightweight hashing processes and a Onetime Password for message signing and verification between vehicles.

Compared with previous schemes, System significantly reduces computation cost by more times. We use pseudonymous certificate to communicate to each other hence proposed scheme provides strong privacy preservation and third party can never access identity of any vehicles even if RSUs compromised.

Keywords- Privacy preservation; Vehicle ad hoc network; Certificate authority; TWO-Factor Lightweight Privacy preserving; pseudonymous certificate

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) are needed to improve road safety and traffic conditions, in which security is essential. VANET every Vehicle is equipped with On Board Unit contain system details and through which you can communicate wirelessly with other vehicle and Road side units. Vehicular ad hoc network is significant to Management of traffic and road Safety. To transmit safety information between vehicles to facilitate warnings to drivers impending Crashes. There are already two different Vehicle to Vehicle warning messages available in many applications.

1. Forward Collision Warning.
2. Blind Spot Warning.

In this project we use forward collision warning message. In vehicle to analyses, send or receive the data at real time and this data also change with each other. To transfer this data one vehicle to another then it helps driver to give accidental information. Hence driver take action averts impending incidents.

In vehicular ad hoc network there are two security requirements. First basic type due to the inheritance from mobile ad hoc network (MANET) and second type based on concerning vehicular communications. There are different threats in wireless communication such as eavesdropping, forgery. In vehicular ad hoc network modification are done easily then this modification incurs the basic security goals.
In VANET system in vehicular communication transmit and collect only "anonymous" data from mobile users for mandatory applications. In VANET systems provide Privacy - preserving by using information related to individual vehicle such as driver's name, speed, position, model and vehicle identification number (VIN) etc.

In this paper, we proposed a Privacy Preserving Authentication Scheme for used in Vehicular ad hoc network which introduces the idea of two-factor authentication technique it derails with OTP and Password verification for security purpose.

Followings are the advantages of our proposed System:

1) Confidentiality

In VANETs, provide confidential communication. When it use in a group, none except group members are able to decrypt the messages that are broadcasted to every member

of group; and none (even other members) except a dedicated receiver member is capable to decrypt the message devoted to it.

2) High Non-repudiation

In this paper 2FLIP provides the vehicle non-repudiation. In that the vehicle could not stop the message from itself.

For example considering multiple drivers of one vehicle could also not stop himself from sending the message. A driver has to first login with his name and password which will be Authentic to the system. Then offers his password to start the vehicle. The evidences generated from the password are transmitted to certificate authority (CA) after some proper time interval, which are used to trace each driver conditionally, hence providing strong non-repudiation.

3) Privacy preservation

In 2FLIP is providing privacy preservation by using authentication, anonymity and unlinkabiliy. The responsibilities of RSUs are purposefully weaken, which leads to strong privacy that even if all RSUs are compromised, malevolent parties still could not pry into real identities of vehicles.

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

II. RELATED WORK

In previous System as they proposed a protocol for effective and secure downloading of the system when the Vehicle is in RSU range. And therefore they are able to share information in between vehicles which is previously downloaded when they outside the range of RSU. In VANET the previous research proposed application layer data sharing protocol, In this system protocol all the vehicles in the network can share information easily. The primary issue is how they share data among each other. An important feature of the this sharing protocol is that it can guarantee the delivery of the requested data file for each vehicle passing through road side unit. Here also addressed security and privacy preserving issues in the process of data sending and sharing, ensuring vehicle applicants' exclusive access to the applied data and privacy preserving of the vehicles involved in the communication. Another Previous Research System proposed the privacy preserving of the vehicle users based on group signature. Group signature is used for anonymous authentication of the vehicle. This scenario provided the advancement in the previous System. Previous system can't meet the requirement of verifying hundreds of messages per second in network. In this proposed scheme, we first divide the area into several domains, in which road- side units (RSUs) are fully responsible for distributing group private keys and managing those keys and vehicles. Finally they works the co-operative message authentication between vehicles, which need to check only few number of messages , so this is short ,effective and time efficient process.

In this research work the proposed system concentrate on the communication computation, resource cost overhead and security problems in vehicular ad-hock network. This new protocol is having smart card authentication system which provide strong authentication for driver and uses dynamic login identity device to hide identity of the user. This protocol also resist against attacks like offline password guessing attack, smart card forgery attack, impersonation attack and so on. In this research work the proposed system is to defend against threats due to increase in dependability on communication, computing, and control technologies. There is also privacy preserving challenges posed by VANETs include data integrity (data trust), confidentiality of identity, nonrepudiation, access control of vehicle and privacy protection.

The trust factor is defined by data that is at what extent data in the network can be trusted and node trust is defined at what extent nodes can be trusted in VANETs are. Attack resistant management system is able to detect various attacks and also compute the trustworthiness of both data and mobile node. Data trust is evaluated based on the data accessed and collected from multiple vehicles and node trust is evaluated in two dimensions functional trust and recommendation trust, that is how effectively a node can

complete its functionality and how trustworthy the recommendations from a node for other nodes.

In Privacy Preserving and Authentication in vehicular ad hoc network numerous schemes have been proposed to improve the Security and conditional privacy preservation in VANET.

They are classified into three categories:
1) Pseudonymous certificate
2) Group signature
3) Pseudonymous authentication and group signature.

1. Pseudonymous Certificate Based Schemes-

Pseudonymous certificate authentication based schemes firstly collect and link many pairs of private key in pseudonymous certificate for pseudo identity. Afterwards, a sender vehicle could utilize these pairs of private key to sign messages and generate MAC all receivers could authenticate the messages by the corresponding pseudonymous certificate. Therefore, the real identity of the source vehicle is hidden in V2V communications.

2. Group Signature Based Schemes

The core concept of group based schemes is that group members are hidden in a group with its real identity is covered and privacy protected of each vehicle

3. Hybrid schemes

It includes pseudonymous authentication protocol, digital signature, MAC and other various authentication technologies to make a reduction in between computation efficiency, CRL size, bandwidth consumption, verification delay, and so on. We used the pseudonymous certificate based scheme for hide our vehicle identity

III. SYSTEM MODEL

1. Network Model

CA is centered and trustworthy Authority records all vehicles. It has nearly Unlimited Computation storage re-course for storing massive data.

Model contains following important components:
a. RSU and Vehicle registration
b. Vehicle information and system key management
c. Message Non-Repudiation verification.

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 has high traffic communication abilities, through powerful receivers it can control the whole communication channel, monitor and hack all the on the-fly messages through these channel. An Adversary intends to find the legitimate vehicle to accept wrong or harmful message without being known to main system.

V. SYSTEM FEATURES

The proposed system will implement in three parts
1. Vehicle User
2. Road Side Unit and
3. Certificate Authority

1) System Initialization and entity Information

Driver gives identity and vehicle information like car number, phone number and vehicle owner. CA after that checks and store the information provided by driver and vehicle owner and then it randomly picks vehicle initial pseudo identity and verify driver password.

2) Driver login

Driver needs to firstly pass the login verification by inserting correct username and password, whenever the vehicle generates a new message sign it and broadcast. Without login information correctly inserted user can not access vehicle..

3) Message Signing

Message signing after generating message the login calculate message Authentication value and broad cast it.

4) Message Verification

Receiver vehicle do Message verification when vehicle accepts the message and then it employ the message for application or otherwise rejects the received message.

5) System key updates

System key is important in whole system. CA introduced new method of updating system key when vehicle is stolen CA firstly generates the new system key then sign the Encrypted message, CA broadcast the message to whole network with help of RSU.

IV. FRAMEWORK AND PROBLEM DEFINITION

In Previous system in which driver's identity not that much protected, however protection of driver's identity and message authentication, message encryption these are very important as well as primary things which should be highly protected to communicate within vehicles and network. In privacy preserving system we propose authentication of the message by Encrypting the message when message is send and after that again message is Decrypted and received at the Receiver end.

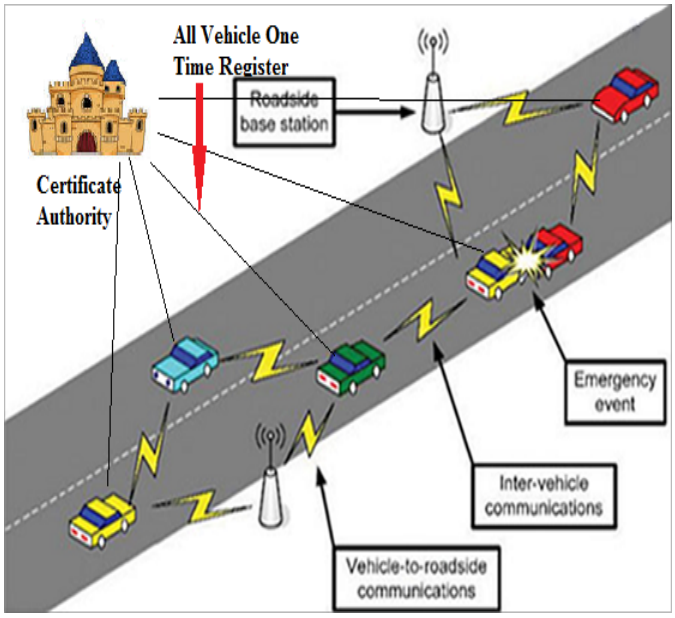

Fig 4.1 Basic Vehicular Ad-Hock Network System[6]

We proposed a Privacy preserving Authentication Scheme for VANET which introduces the idea of authentication technique to VANET mainly by utilizing Onetime password and user password and privacy of VANET. In proposed scheme, each vehicle would be bond to a On Board Unit device which would be utilized along with Password technology equipped on this vehicle to verify the identities of multiple drivers and allow them to access the vehicle. Resilience to biometrics is not considered in this paper. To make communication secure and private in V2V and V2R, 2FLIP only requires OTP and password Secured login or Normal login. We provide offline system key update for vehicle, which would not affect the performance. Up to current and upcoming time system is the great authentication scheme which achieve strong vehicle privacy preservation message authentication and avoid DoS attack, additionally it is also the first and dynamic authentication scheme which authenticate multiple Drivers.

Followings are the advantages of our proposed 2FLIP scheme:

1. Strong privacy preservation is able guarantee 3 levels of privacy: authentication, Certificate Authority and OTP moreover with the vehicles RSU need strong protection about message data. Vehicle can be more secured by authentication schemes like OTP, Secured Login and Normal Login.

2. Secure system key update -once system key is hacked, our scheme provides a mechanism to restore the system by updating the system key at CA. This is essential for maintaining practical system.

3. Offline password update- Driver password and all related information is saved in Database and could be updated without network connection to RSUs or CA, therefore if provides support to flexible use of system.

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 also take care of the message encryption and decryption for the messages. Message cryptography is included in this project for the securing messages from attacks outside the network.

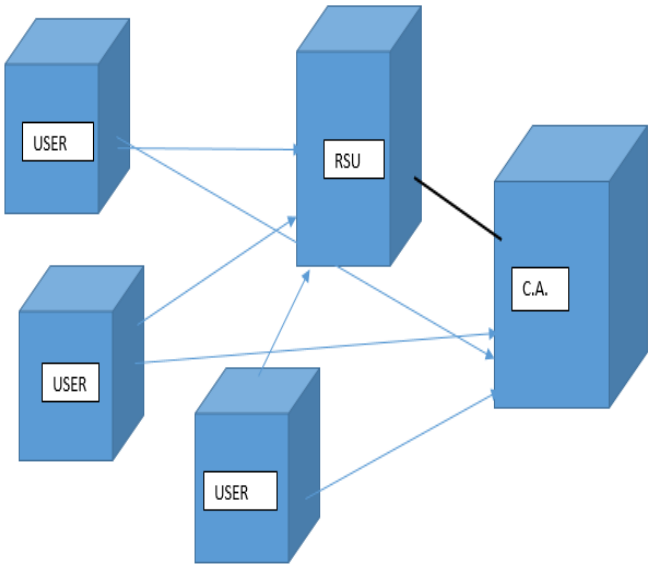

Fig.4.2 Deployment Model of the System

ALGORITHM 1: Proposed for Project:

1. RegistertoCA(vehicleinfo,userinfo)
2. information saved in Databse.
3. CAcheck and register User
4. CAprovide Authentication()
5. user is connected
6. Generate a Secured/Normal Login()
7. Send Message/Encrypted Message
8. Encrypt (Message,Time for message)
9. Broadcastmessage()
10. Reciver recive Encrypeyed/Normal Messge
11. Decrypte the Normal Message/ Secured Message.
12. ReceiveBroadcast()
13. Display Message Time
14. If(received) thenProcess(message)
15. Check user and message Authentication RSUtrack(msg,user)
16. DriverdetailsUpdate
17. STOP

As seen in above algorithm one message broadcasted to several users n; Same each user broadcast several messages m;

Fig.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 an example of a hash-based message authentication code (HMAC). It combines a secret key with the current timestamp using a cryptographic hash function to generate a one-time password. The timestamp typically increases in 30-second intervals, so passwords generated close together in time from the same secret key will be equal.

In a typical two-factor authentication application, user authentication proceeds as follows: a user enters username and password into a website or other server, generates a one-time password for the server using TOTP running locally on a Smartphone or other device, and types that password into the server as well. The server then also runs TOTP to verify the entered one-time password. For this to work, the clocks of the user's device and the server need to be roughly synchronized (the server will typically accept one-time passwords generated from timestamps that differ by ±1 time interval from the client's timestamp). A single secret key, to be used for all subsequent authentication sessions, must have been shared between the server and the user's device over a secure channel ahead of time. If some more steps are carried out, the user can also authenticate the server using TOTP.

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.

V. RESULT ANALYSIS

At first in the system driver send his/her personal details to the CA. CA accept details and save it to the database. After that user is Normal/ Secured Logged in with CA. Then Onetime Password is been send to the user mobile for dual Authentication which will Register user. Message is Encrypted and send by Normal/ Secured logged user. at Receiver end message is again Decrypted by using the Algorithm. At runtime 2 authorities i.e. Certificate Authority and Road Side Units are alive and several vehicles in range. These all system bodies are active at a time and each vehicle send messages to each nearby vehicle and RSU simultaneously.

Registering to C.A. and C.A. saves details and gives Authentication to the Registered user and vehicle. The time and Length to send Normal / Secured Message is been Calculated by the Machine.

CONFIGURATIONS

Parameters	Values
Communication range	100m
Channel bandwidth	4bps
Broadcast Interval	30s
Delay time	((Encrypted msg +Decrypted msg + Time for Psudo Certificate)-(Time interval for original msg))

CERTIFICATE/SYSTEM KEY UPDATION OVERHEAD

In the VANET these are thousands of vehicle active at one time so if the system key leakage and problem related to pseudonymous certificate force to update in system key. As thousands of users in network can generate high message traffic overhead on network rather than other systems, Hence CA as a server should be enough to handle or be distributed.

HANDLING ISSUE OF CERTIFICATE FORGING

To handle this major issue Certificate Authority automatically need to update details of certificate periodically. This is only solution; hence we provide facility that certificate authority automatically sending new certificate to vehicle on daily basis.

VI .CONCLUSION

In this paper, we proposed a privacy preserving authentication scheme based on the decentralization of CA, the proposed scheme requires only several extreme lightweight hashing process and OTP for message signing and authentication, the Message goes by the procedure of Encryption and Decryption along with the verification, which increases efficiency of computation and communication. Extensive simulation reveals that the novel scheme is feasible and has an outstanding performance on message signing and verification, message loss ratio and network delay.

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.

[9] "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," IEEE Std 1609.2-2006 , vol., no., pp.0_1,105, 2006

[10] B. Libert and D. Vergnaud, "Multi-use unidirectional proxy re-signatures," in Proc. 15th ACM conference organized Computer and communications security, Alexandria, USA, 2008, pp. 511-520.

[11] "RFC 6238 - TOTP: Time-Based One-Time Password Algorithm". Retrieved July 13, 2011.

[12] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, ": Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc. INFOCOM 2008, pp.1903-1911.

[13] C. Zhang, R. Lu, X. Lin, P.-H. Ho, X. Shen, " An Efficient Identity Based Batch Verification Scheme for Vehicular Sensor Networks," in Proc. INFOCOM 2008

[14] A. Fiat, "Batch RSA," in Proc. of Crypto, 1989,

[15] J. Camenisch, S. Hohenberger, M. Ø. Pedersen, "Batch verification of short signatures," Advances in Cryptology-EUROCRYPT: Springer, 2007.

[16] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," Vehicular Technology, IEEE Transactions on, vol. 56, no. 6, pp. 3442-3456, 2007.

[17] D. Cham and E. van Heyst, "Group Signatures," in Proc. Advances in Cryptology—EUROCRYPT, 1991, pp. 257-265.

[18] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. CRYPTO, 2004.

Mrs Awanti Sujit Dhekane received her Btech degree in computer science from Dr.Babasaheb Ambedkar Marathwada University of Aurangabad, Maharashtra in 2010. She was an Lecturer in MOZE Institute of Technology and Lecturer from Morden College of Engineering, Pune, from 2012 to 2014. Research interest includes the privacy and security issues in vehicular ad-hoc networks and wireless sensor networks.