KEY GENERATION TECHNIQUE FOR DRIVER AUTHENTICATION SCHEME IN VEHICULAR AD HOC NETWORK

***Sam Mathews M, **Bevish Jinila Y**

**PG Scholar, Dept.of Information Technology*
Sathyabama University, Chennai, India
mathews.sham@gmail.com
***Assistant Professor, Faculty of Computing*
Sathyabama University, Chennai, India
bevish.jinila@gmail.com

ABSTRACT

Vehicular Adhoc Networks(VANET) is an emerging intelligent network that provides safety and comfort to the public. The main issues of vanet are maintenance of the system and revocation of malicious vehicles. The secrecy of the vehicle positioning of the vehicle user is the major issue. To provide this privacy, the vehiclecan use different pseudonyms, this secures the privacy only. But authentication of the vehicle is still an imperative issue to cope with. To overcome this issue, we have proposed the solution which states the effective authentication scheme by providing the password to the vehicle user. From that we can achieve the prominentcommunication between the vehicle user and the Trusted authority. Also it has stronger methodology to generate the password. This ensures the passenger safety while driving on the road infrastructure.

Keywords—Authentication, Global Positioning System, OnBoard unit, Road side unit, Trusted Authority,Vanet

INTRODUCTION

The vehicular ad hoc networks (VANETs) have been attracted a lot of attentions due to their interesting and promising functionalities including safety, traffic congestion avoidance, location based services, efficiency of the transportation system and enable new mobile services for the user. The communication are controlled by IEEE 802.11p, i.e., WAVE(Wireless Access in Vehicular Environments). In VANETs each vehicle is equipped with the On board Unit(OBU) communication device, which allow them to communicate not only with each other, i.e., Vehicle-to-Vehicle(V2V) communication and Vehicle-to-Infrastructure(V2I) communication. As the wireless communication channel is a shared medium, exchanging messages without any security over the air can easily leak the information that users may want to keep private. Privacy is an important issue.

To achieve location privacy, a popular strategy[1] proposed that vehicle periodically changing their pseudonyms when they broadcast safety messages, from the Fig 2, we can infer that the safety message is a 3-tuple, including Time, Location and Velocity. Pseudonym based schemes [2]–[4] havebeen proposed to preserve the location privacy of vehicles. However, those schemes require the vehicles to store a large number of pseudonyms and certifications[5], and do not support some important secure functionalities such as authentication and integrity. The safe driving andinfotainment services on the move can be develop by the using the concept of cryptography [6].

Today's vehicle already use information about the close environment, collected by the onboard unit. Nevertheless, this information is often not enough to warn the paper before an accident happens in the road. Exchanging information through inter vehicular communication(IVC) can help to evaluate the road situation far ahead road situation far ahead, and therefore, detect dangerous situations in an adequate amount of time to resolve. Adhoc inter-vehicle networks will soon be a reality as cars become equipped with wireless communication system. Security and Reliability like road travel collision, traffic congestion, fuel consumption are overcome by destination makingsystem which are created by physics, vehicle dynamic and historical data collected from GPS system [7]. So there is a demand to give greater authentication scheme for the vehicle by using the SHA-1X algorithm. It delivers greater efficiency than the key generation scheme need to identify each vehicle.Driver authentication requires effectively identifies each vehicle, broadcasting over the network. So that the vehicle is free from theft and other menaces.

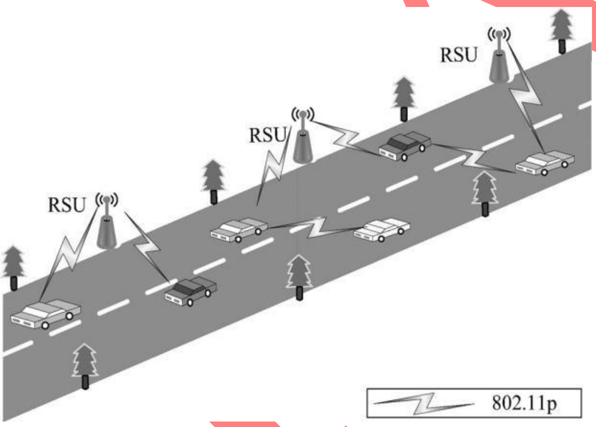

Fig 1 VANET Architecture

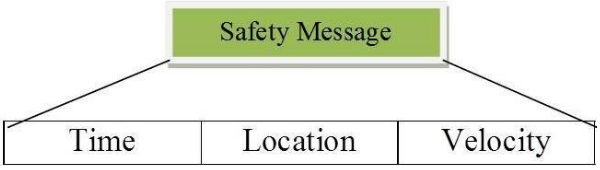

Fig 2 Safety message content

RELATED WORKS

There have been a few prior efforts on key generation for driver authentication scheme s also this section gives the background knowledge about the security in adhoc networking, cryptographic backgrounds and the various methods available. Raya and Hubaux [8] proposed about how to achieve both message authentication and anonymity that each vehicle should be preloaded with a large number of anonymous public and private key pairs together with the corresponding public key certificates. Traffic messages are signed with a public-key-based scheme. To minimized the overhead induced by the group signature-based system, Calandriello et al. [9] developed an alternative scheme in which a vehicle can generate public and private key pairs by itself by using a group key. This scheme can achieve a tradeoff between the group-signature-based scheme and the traditional PKI-based scheme. Sehun Kim et. al in [10] describes about the vehicle collision system that detects the car crush and gives indication about upcoming danger in the road to the drivers in advance.

Collision warning is implemented by using sensors and GPS system. George et al[11] designed and developed an innovative KMS uses a modified hierarchical trust Public Key Infrastructure(PKI) model in which node can dynamically assume management roles. The roles that were undertaken by the nodes in the hierarchical model were: Root Certified Authority(RCA), Delegated Certificate Authority(DCA) and Temporary Certificate Authority(TCA). Yiling et al.,[12] proposed the new scheme for wireless environment called group key management algorithm. The approach is a two- level structure, where the group of users are divided into clusters, this reduces the rekeying cost during key updation. This report also suggests that the method employed here has greater efficiency when compared with the existing logical key hierarchical scheme. To the best of our knowledge, allof the existing group signature schemes in VANETs [13]–[15] are based on centralized key management which preloads keys to vehicles off-line. The centralized key management has some disadvantages. For instance, the system maintenance is not flexible.

PROBLEM DEFINITION

In this scheme, we delineate the problem by deploying the network and the requisites needed for generating the key.

A. *System Model*

We consider a VANET in the urban area which consists of a great number of vehicles which consists of a key distribution center, which is having vehicle registering vehicle site

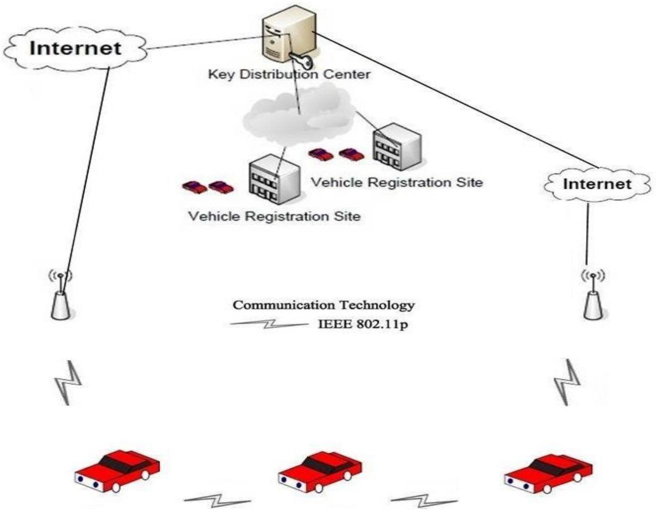

Fig 3 Key Distribution

connected by network. Some stationary RSUs are deployed at the roadsides, and the communication between laid them by IEEE 802.11p, as shown in Fig. 3.

The TA is responsible for registration of RSUs and vehicles. It is like a centralized server which having all the data around the vehicles. TA offers the key to the vehicle registering to itself. So it is called as Key Distribution center inferred from the fig 3. RSUs act as the infrastructure of the VANET and connect with the TA by wired links in the system. They provide service for information dissemination and certificate updating. In general, the density of RSU varies in different domains. Vehicles equipped with OBUs mainly communicate with each other to share local traffic information and improve the driving experience. A vehicle frequently requests the certificate service from an RSU and obtains enough certificates for the following period until passing by another RSU. Obviously, the number of updated pseudonymous certificates depends on the RSU density.

B. *Existing Methodology*

[16] GSIS is a group-signature-based (GSB) technique that can achieve conditional locationprivacy without PC. However, the pure group signature verification is usually time consuming, whichmay be not suitable for some time-stringent VANET applications. when a legal vehicle passes by an RSU, the RSU will authorize a GSB short-life anonymous certificate to the vehicle. Then, the vehiclecan use it to sign messages with ordinary signature techniques. TA does not directly preload authorized anonymous key to the vehicle; instead, it provides the authorized anonymous key to the user—the owner of the vehicle. Trusted authority has the information about the vehicle as a node participating in the network. It does not possess any unique details about the driver who is authenticated for a vehicle in the VANET environment. As every benign vehicle registers andverifies itself to the TA through RSU takes much time to process their requests has been sacrificed. TA process the request presented by the RSU and it starts providing keys to the vehicle. It takes

much time to finish the verification and issuing key params to the vehicle. Communication overhead occurs due to the delay in processing. This leads to the failure of group based signature.

PROPOSED SECURE TECHNIQUE

In order to decrease the delay in cyclic group based authentication, also to improve the driver authentication, the symmetric key is given to the Trusted authority. Trusted authority chooses the key params as shown in the table 1. From that every vehicle is authenticated and corresponding password has been catered to each vehicle. Using that password its starts the trip and it has been monitored by the centralized authority, so that TA finds out if any attacker attempts to track the vehicle through any false identity, it gives alert to the vehicle. This scheme also provides road information to the driver for safety and comfort. Referable to the inbuilt Global Positioning System (GPS), the driver receives the alarm if any accidents take place or any collision that happens beyond to the driver knowledge . From that the driver authentication can be performed cogently.

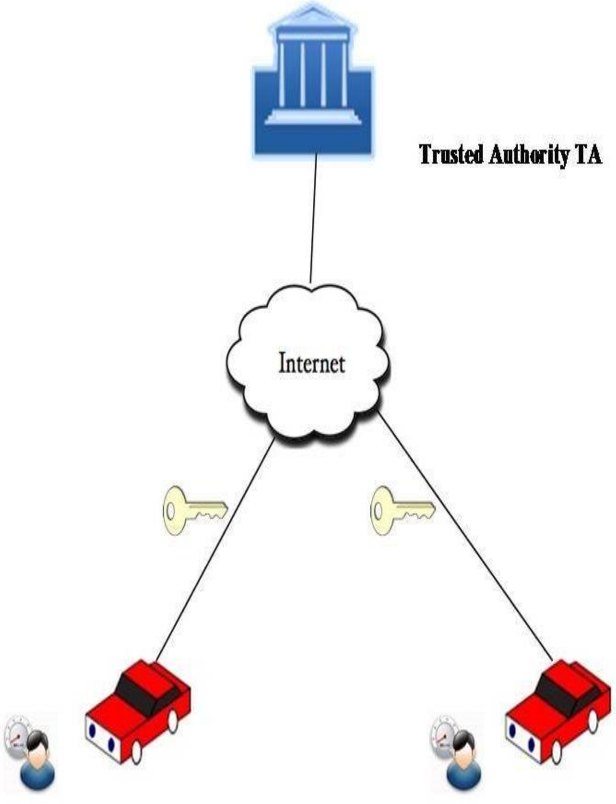

Fig 4 Driver Authentication by TA

ALGORITHM IMPLEMENTATION

Trusted Authority generates the password to the vehicle registering to itself. It uses SHA-1X algorithm for performing the generation process by choosing three components namely R_{id}, T_{pub}, Mk referred in the Table 1

Table I NOTATIONS USED

R_{id}	Random ID
T_{pub}	Public Key
Mk	Master key
P_{id}	Password

The steps to be followed for generating the password P_{id} is as follows

Step 1: P_{id}, Password generation from Trusted authority

Step2:Choosing three parameters-R_{id}, T_{pub}, M_k

Step 3:Initialize the value for the parameters

R_{id}- any random number in binary(4-digits)

M_k-Master Key in the form of binary value(2-digits)

T_{pub}- Public key, which can be calculated by,

$T_{pub}=M_k * p$

Where M_k is the Master Key taken

P=Prime order, by default it is 11(i.e.,p=11)

Step 4:Using SHA1 Algorithm, perform hashing, i.e., Pid=H(R_{id}, T_{pub}, M_k)

Step 5:Get hold of the answers received

Hashed value is of 160-bits

Take the first five bits from the hashed value, say it as A

Middle five bits from the hashed value is said to be B

C is the last five bits from the hashed function

Step 6:DO XOR of A,B,C i.e., A, B, C

Step 7:Store the resultant value as V

Step 8:Perform XOR operation with the Resultant value V with Master Key M_k taken, store the result results in Vid

Step 9: Convert the binary resultant value of V_{id} into hexadecimal

Step 10: Assign P_{id} to each vehicle, when it registers to the TA initially.

Fig 5 shows the pictorial Implementation of the system that has been developed using SHA-1X algorithm which performs better when compared to the existing method of group signature verification of the vehicle. Every components in the system has its own liabilities to execute the efficient scheme to verify the vehicle identity

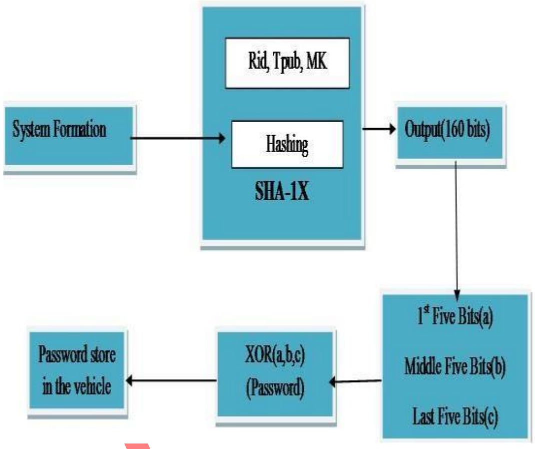

Fig 5 Flow of Algorithm

PERFORMANCE EVALUATION

In this section, we have evaluated the performance by conducting the experiments on the parameters which are used to generate the password. Our developments are based on NetBeans IDE todemonstrate the performance metrics of SHA-1X algorithm when compared with the existing schemeof group signature verification. The values are displayed in the table II below.

Table II Experimental Observations

Random Id Ri_d	Resultant V	V_{id}	Password P_{id}

1011	110101	110110	36h
1001	1010111	1010000	50h
1111	11100001	11101010	EAh
0100	101111100	101110001	171h

The comparison of SHA-1X with the conventional group signature method. From the figure 6, the The functioning of our proposed scheme is higher with respect to the time needed by the TA to provide the password. X-axis is the time taken by the TA to verify the vehicle and Y-axis is the number of vehicles verified by the trusted authority.

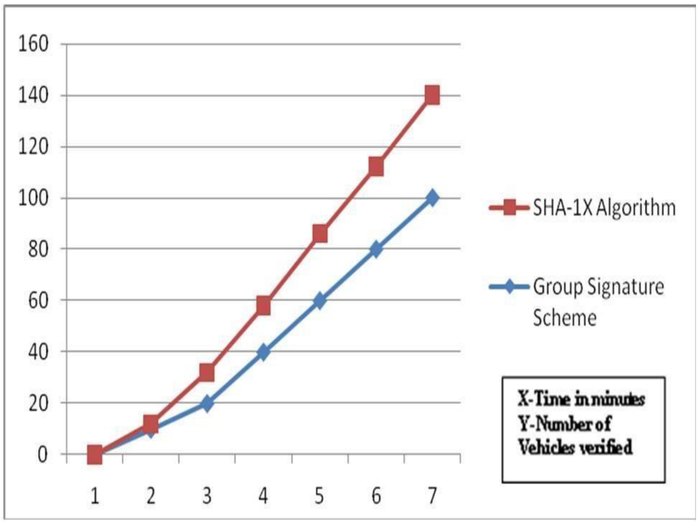

Fig 6 Comparison of SHA-1X with the Group Signature Scheme

CONCLUSION

The deployment of vehicular communication networks is rapidly increasing. In this paper, we have proposed the effective scheme for driver authentication by providing the password to the vehicle for identification. The scheme overcomes the properties of conventional group signature which needs plenty of time to verify the vehicle. Thereby, the vehicle can able to get notification from the centralized authority about emergency reporting, collision warning and secure communication with another. Extended work of this project is providing the authorized access to the RSU’s deployed. So that vehicle need not to wait for validating themselves with the TA, becausenone of the system delivers 100 percent efficiency. Also to achieve location privacy for securing the vehicle's position , incase of any malicious attackers attempts to track the vehicle. We concluded that the vehicle having effective password system provide by the Ta helps to travel with safety and comfort.

REFERENCES

[1] Rongxing Lu, Xiaodong Lin, Tom H. Luan, Xiaohui Liang, and Xuemin (Sherman) Shen, –Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs‖ IEEE Transactions On Vehicular Technology, Vol. 61, No. 1, January 2012

[2] J. Freudiger, M. Raya, M. Feleghhazi,P. Papadimitratos and J.- P.Hubaux., –Mix zones for location privacy in vehicular networks,‖ in Proc. International Workshop on Wireless Networking for Intelligent Transportation Systems, Vancouver, British Columbia, Aug., 2007.

[3] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, –Enhancing wireless location privacy using silent period,‖ in Proc. IEEE WCNC, pp. 1187- 1192, 2005.

[4] K.Sampigethava, L.Huang, M.Li, R.Poovendran, K.Matsuura and K.Sezaki, –AMOEBA: Robust location privacy scheme for VANET,‖ in IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp.1569-1589, 2007.

[5] Sam Mathews M, Bevish Jinila Y, — An Effective Strategy for Pseudonym Generation And Changing Scheme with Privacy Preservation for Vehicular Communication in IEEE Conference on Electronics and Communication System, Coimbatore, India.,2014 ISBN978-1-4799-2320-5/14., In Press

[6] Vighnesh N V,N Kavita, Dr.Shalini R.Urs –A Novel Sender authentication Scheme Based On Hash chain For Vehicular Ad-hoc Networks ‖ IEEE Transaction 2011

[7] Vineetha Paruchuri , –Inter-vehicular communications: Security and reliability issues‖ International conference2011

[8] M. Raya and J.-P. Hubaux, –Securing vehicular ad hoc networks,‖ J. Comput. Secur., vol. 15, no. 1, pp. 39–68, Jan. 2007

[9] Mihail L. Sichitiu, North Carolina State University Maria Kihl, Lund University Inter-Vehicle Communication Systems: A Survey 2nd Quater 2008, Volume 10, NO. 2 IEEE Communication Surveys

[10] Sehun Kim, Sunghyun Lee, Inchan Yoon, Mija Yoon and Do-Hyeun Kim, Department of Computer engineering Jeju National University Jeju, Korea –The Vehicle Collision Warning System based on GPS‖

2011 First ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering

[11] M.Berlach, H-J. hof, d. Kraft,L.Wolf.,(2009)‖ a cluster based security Architecture for AdHoc networks‖,IEEE INFOCOM

[12] Yiling Wang, dhilak Damodran, Phu dung Le.,(2010)‖ Efficient group key management in Wireless Networks‖ Proceedings of the Third International Conference on InformationTechnology:New Generations(ITNG'10)

[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, Alaska, May 2007.

[14] X. Lin, X. Sun, P.-H. Ho and X. Shen, ―GSIS: a secure and privacy preserving protocol for vehicular communications,‖ IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442-3456, 2007.

[15] G. Calandriello, P. Papadimitratos, A. Lloy, and J.-P. Hubaux, ―Efficient and robust pseudonymous authentication in VANET,‖ in Proc. ACM Mobicom, pp. 19-28, QC, Canada, Sept. 2007.