ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website:www.ijircce.com

Vol. 5, Issue 2, February 2017

A Survey on Group Key Technique and Co-operative Authentication in VANET

Jayanth S, Saravanan I S, Kapilavani R K

B.E. Student, Department of C.S.E., Prince Shri Venkateshwara Padmavathy Engineering College, Ponmar, Chennai, India

B.E. Student, Department of C.S.E., Prince Shri Venkateshwara Padmavathy Engineering College, Ponmar, Chennai, India

Assistant Professor, Prince Dr. K. Vasudevan College of Technology, Ponmar, Chennai, India

ABSTRACT: Amongst many different communication paradigms, Vehicular ad hoc networks (VANET's) are an area of developing techniques. It has become an upcoming technology of this modern world in vehicular communications. The main reason of using VANET is to exchange live messages regarding traffic congestions. A Trusted authority (TA) is designed to provide authentication services for users and managing keys of several users. Like in any other networks in VANET also there is a necessity to maintain authentication and confidentiality among the users. To authenticate the users the authority classifies users into primary, secondary and unauthorized users. First, a co-operative message authentication scheme is proposed by which the authentication burden of the TA is shared among the already authenticated primary users of the VANET. Second, a group key management technique is proposed by which a number of users are grouped together and one key-pair is assigned to the whole group. This is also used to update/rekey the key periodically instead of after every join/leave operations. Using these schemes the VANET users should be able to send and receive messages to and from authority and users through the road side units (RSU's) with a full of secured process.

KEYWORDS: Authentication and confidentiality, co-operative authentication, rekeying and group key management.

I. INTRODUCTION

Vehicular Ad hoc Networks (VANET's) are another form of Mobile Ad hoc Networks by extending mobile concepts to vehicular environment. It is generally a self-organizing, distributed network applied to vehicular environments. VANET is used to share information about traffic and road conditions, collision avoidance techniques along with other value added services [1]. Generally VANETs are networks that use group communications [2] in which the information from one user needs to be broadcasted to several users.
The general system model of VANET has 3 main components.

1. A Trusted Authority (TA) that acts as a verifier control that authenticates all the VANET users and manages the keys for all those users.
2. Road Side Units (RSUs) that are fixed infrastructures that are used to route the messages to and from the authority and the users.
3. On Board Units (OBUs) that each user has in their vehicle that contains sensors, DSDC medium and other devices for communicating with other users.

There are 2 types of communications possible between VANET components. The first is V2V (vehicle to vehicle) type in which a vehicle user communicates with another directly which is the purest form of infrastructure-less characteristic of ad hoc networks. The other is V2R (vehicle to RSU) type where a vehicle communicates with RSU which is a fixed infrastructure. These vehicles communicate using the Dedicated Short Range Communication (DSRC) protocol [3]. The RSU, OBU and TA communicate using this protocol which is based on the IEEE 802.11p radio technology. The vehicles can access the wireless channel either using a directional antenna or a unidirectional antenna. Because of this

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website:www.ijircce.com

Vol. 5, Issue 2, February 2017

wireless access VANETs are vulnerable to many attacks due to collision, eavesdropping, interference, jamming and other problems. To avoid these attacks only we introduce a concept of security in VANET. The intention of providing security is to maintain confidentiality among users by grouping them together and to efficiently provide authentication services. In many literature systems all the authentication services, key storage and updating services are performed by the authority. This imposes a huge overhead on the authority. Also this situation results in a scenario where it becomes easier to an attacker to attack only the authority end and collapse the whole system. It is inefficient if the authority is attacked that results to handing over the control to an attacker. This issue must be addressed to avoid the chance of attacking whole system by just bringing the authority under attacker's control

II. ASSUMPTIONS

We assume that the TA end is secure in order to implement this system. We make the following assumptions on the security of the whole system.

1. Every user knows the TA's public key after undergoing the registration process.
2. TA contains powerful firewalls and intrusion detection systems to avoid the unauthorized users.
3. TA possesses computational, communicational and storage capabilities compared to other RSUs and OBUs in the network.

III. RELATED WORK

Many literature systems in VANET worked on the schemes that provide authentication alone. Among various techniques used in the existing system a notable one was Elliptical Curve Digital Signature Algorithm (ECDSA) [4]. This algorithm uses a Public Key Infrastructure (PKI) in which each user has an asymmetric key-pair consisting of a public key and a private key. VANET on the other hand is a dynamic environment with a large number of users. It is a huge process to store and manage distinct key-pairs for each user. Also there are two attacks possible in ECDSA. The First is the attack possible on the Elliptical Curve Discrete Logarithm Problem (ECDLP). The second is the attack possible on the hash function.

In another system there is a short-lived certificate provided for each user that can be updated using Efficient Certificate Management Scheme for Vehicular Ad Hoc Networks (ECMSV) [5]. But updating this certificate becomes another overhead posed on the TA.

Another approach to provide Co-operative Message Authentication (CMAP) [6] has been proposed that finds out malicious information broadcasted by malicious user .But in this system if there is no verifier then malicious messages can be broadcasted to legitimate users also.

Yet another approach is to use the RFID authentication protocol that uses the hash chain method [7]. But even here only authentication of the message is maintained but the confidentiality is left aside.

An Anonymous Batch Authentication is another approach [8] proposed by taking into account the situation where multiple requests are approaching the authority at the time. But this system has proposed a single broadcast that is made to all the requests. But here the problem is that the same batch can contain any number of both authorized and unauthorized users.

A Group Signature Based [9] security is provided in an approach by which a group of users share a same group signature to communicate with the authority. But here the authority also needs to calculate the group signature. The Vehicles in the group are being dynamic, it is a difficult task for the TA to continuously calculate the group signature and update it. This again imposes an overhead on the authority.

A Pseudonym Based Authentication [10] has also been proposed in which the users in the VANET use a pseudonym instead of their true identity to provide conditional privacy. But this scheme is not applicable for large-scale applications and does not consider the varying mobility of the vehicles.

A Distributed Key Management Framework with Co-operative Message Authentication in VANET [11] has been also proposed that uses short group signatures. Again even in this system all the jobs are performed by the authority.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website:www.ijircce.com

Vol. 5, Issue 2, February 2017

IV. SYSTEM MODEL

The System model that depicts the proposed system is demonstrated in Fig.1.

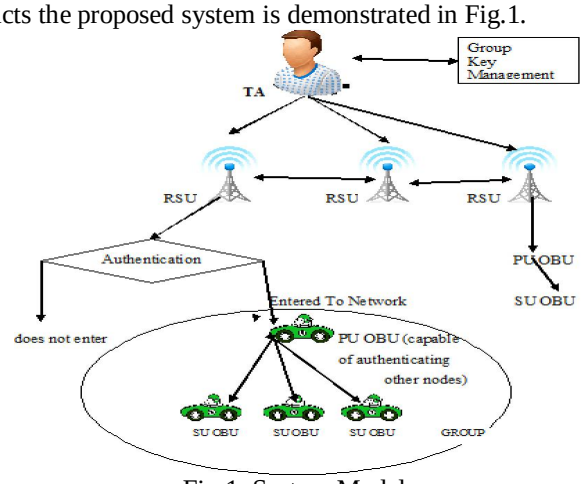

Fig.1. System Model

Trusted Authority (TA): TA takes the responsibility of providing authentication of the users, manage and store the keys for encrypt and decrypt the message shared amongst the VANET users. It is also responsible for registering the users and storing their information that is used later to authenticate them by verifying the stored credentials.
Road Side Units (RSUs): RSU's are the fixed infrastructures that can capable of routing message from TA and OBUs and vice versa. RSUs are connected with the TA in a secure wired connection and are managed, monitored by the TA.
On Board Unit: Each user in the VANET contains an OBU that is embedded inside their vehicle. The OBU consists of Tamper Proof Device (TPD), vehicle sensors like GPS, DSRC medium, Event Data Recorder (EDR),decision making agent, fuzzy rule base and inference engine.

V. ATTACKS

Since all the communication between vehicles and RSUs happen through an open wireless channel, there are many kinds of attacks possible. Listed below are some of the possible attacks.

A. Identity Possession Attack: It is an attack in which one entity pretends to be another in order to get some of the privileges an authenticated user possess.
B. Sybil Attack: It is a type of attack in which an entity that pretends to be more than one entity at the same time.
C. Replay Attack: In this type of attack, the attacker repeats the same valid message or delays the transmission of those messages in order to disturb the traffic.
D. Collision Attack: It is an attack that happens when two or more vehicles share an improper agreement and act as a legitimate user to co-operatively defraud.

Hence, to overcome these issues our scheme of co-operative message authentication and group key management can be efficiently utilized.

VI. REGISTRATION OF THE USERS

The VANET user undergoes an offline registration process to make use of the VANET technology.
STEP 01: The users go to the TA's place directly offline to register him/herself and the vehicle.
STEP 02: The user provides his/her name, contact information, vehicle's information along with his/her fingerprint.
STEP 03: The TA immediately stores the information with the fingerprint.
STEP 04: After successfully registering the TA provides the user with his public key and the user's private key.

- The private key is used to generate a hash code by the PJW hash code algorithm.
- TA compares this hash code with that of the stored one and authenticates the user if they match.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website:www.ijircce.com

Vol. 5, Issue 2, February 2017

VII. PROPOSED CO-OPERATIVE MESSAGE AUTHENTICATION

In the proposed co-operative message authentication the verification overhead is shared with the VANET users. In this scheme already authenticated users can do the job of verifying the hash code of other users to authenticating them.

The general process of authenticating the user is as follows.

1. The User, who needs to enter the VANET, scans his/her fingerprint using the fingerprint Scanner device.
2. Then a hash code corresponding to the fingerprint is generated.
3. This hash code is encrypted with the user's key and sent to the TA through the RSUs.
4. The TA receives the code, decrypts it and compares this hash code with the one stored.
5. If it is a match, then it authenticates the user and adds him/her to the VANET.
6. Else, the vehicle is any other vehicle that does not possess the VANET technology.

Now, if multiple requests for authentication approach the authority simultaneously then to share the load an authenticated VANET user can do the job of authenticating other users. An depiction of such authentication is shown in Fig.2.

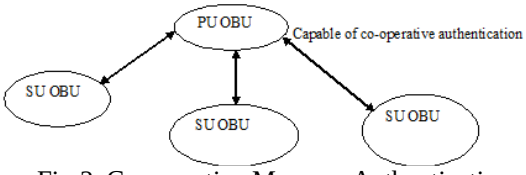

Fig.2. Co-operative Message Authentication

In this process of co-operative message authentication, the request that is waiting for authentication will be handed over to an authenticated VANET user if the TA is busy. In this process the user sends the hash code to another user who is already authenticated. Now, the authenticated user has access to the TA's database and it authenticates the user.

Doing the authentication job, the user that provides the authentication service becomes the Primary user (PU) and the user who gets authenticated will become the Secondary user (SU). By this scheme the verification overload on the TA can be reduced by sharing the responsibility with a primary user.

VIII. PROPOSED GROUP KEY TECHNIQUE

In this proposed system of group key technique we address the issue of storing and managing distinct key-pairs of each VANET user. So, instead of assigning each user a key-pair, a group of users can share a group key-pair.

A. GROUPING AND MANAGING GROUP USERS

The users are grouped in bases of which user gets to control which users. The Secondary users that are accessed through the same primary user can be grouped into one group with the corresponding primary user. This group is assigned a single key-pair to reduce the storage overhead as shown in Fig.3.

Any information exchanged between the TA and Secondary users needs to be routed through the corresponding primary user only. So the primary user has the access on all of its secondary users. So, we need not unnecessarily store the information of the secondary users. So, all the secondary users that can be accessed through the same primary user are grouped and are accessed by using the credentials of the primary user alone. So, this will reduce the issue of storing unnecessary information. That storage space can be used for useful purposes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website:www.ijircce.com

Vol. 5, Issue 2, February 2017

B. KEY UPDATING OR RE-KEYING

The key assigned as the public key is known to all of the VANET users. So for maintaining secure exchange of messages the public key of the system must be updated. Most of the existing systems perform rekeying operations only after every join/leave operation. But that will be inefficient because the time difference between any two successive join/leave operations will be very less nearing negligible time. So, instead of performing rekeying after join/leave, the keys can be updated periodically after a time quantum. By doing this we assure efficient rekeying and user gets the correct updated key.

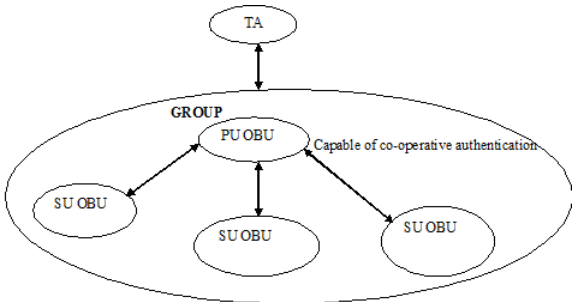

Fig.3. Group key Management

We minimize the computation overhead on TA and users while updating a key. The TA needs to perform only a simple addition or subtraction to generate a new key and the users need to perform only one modulo division to get the updated key.

IX. PERFORMANCE ANALYSIS

Comparing the proposed system with some of literature system, we can study the issues that were noticed in them and those that addressed in proposed scheme. The following Table.1 explains it.

ASPECTS	LITERATURE SYSTEMS	PROPOSED SYSTEM
Security	Authentication only.	Both Authentication and confidentiality
Authentication	Done by TA	Done by TA and PU
Key Management	Information of all users are stored individually necessarily	Only the information of necessary users stored in terms of group keys
Rekeying	Done after every join/leave	Done periodically
Overhead	Computational and storage overhead on TA	Load on TA is shared thereby minimizing the overhead

Table.1. Comparison of proposed system with literature system to analysis performance.

X. CONCLUSION AND FUTURE WORK

Thus a co-operative message authentication scheme has been proposed by which the verification burden of the TA is shared with the primary users to authenticate other users. Also, a group key management scheme has been proposed by which the TA store only one key-pair by which all the users of the group can be accessed, Thus, the proposed system addresses the issues of computational and storage overhead on the TA by sharing authentication responsibility with PUs and storing only group keys through which all the users of VANET can be accessed. The future developments of this work may devise proposing new methods to provide authentication and confidentiality services along with vehicle's location privacy privileges.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website:www.ijircce.com

Vol. 5, Issue 2, February 2017

REFERENCES

[1] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security , vol. 15, no. 1, pp. 39-68, 2007.
[2] Chung Kei Wong, Mohamed Gouda and Simon S. Lam, "Secure Group Communications Using Key Graphs", IEEE/ACM transactions on networking, vol. 8, no. 1, February 2000.
[3] J. B. Kenney, "Dedicated Short Range Communications (DSRC)", IEEE 2011.
[4] D. Johnson, A. Menezes and S. Vanstone, "The Elliptical Curve Digital Signature Algorithm (ECDSA)", Int. J. Inf. Security, vol. 1, no. 1, pp. 36-63, August 2001.
[5] A. Wasef, Y. Jiang and X. Chen, "ECMV: Efficient certificate management scheme for vehicular networks", in Proc. IEEE GLOBECOM, New Orleans, LA, USA, pp. 1-5, 2008.
[6] W. Shen, L. Liu and X. Cao, "Co-operative message authentication in vehicular cyber-physical systems", IEE transaction in Emerging Topics Computation, vol. 1, no. 1,pp. 84-97,June 2013.
[7] I. Syamsuddin, T. Dillon and S.Han, "A survey of RFID authentication protocols based on hash chain method", in Proc. 3rd ICCIT , vol. 2,pp. 559-564, 2008.
[8] Jiun-Long Huang, Lo- Yao Yeh and Hung-Yu Chien, "ABAKA: An Anonymous Batch Authentication and key agreement scheme for value added services in vehicular ad hoc networks ", January 2011 .
[9] Jinhua Guo, John P. Baugh and Shengquan Wang, "A group signature based secure and privacy preserving vehicular communication framework", IEEE, September 2007.
[10] Dijiang Huang, Satyajayant Misra, Mayank Verma and Guoliang Xue, "PACP: AN efficient pseudonymous authentication-based conditional privacy protocols for VANETs", IEEE Transaction on Intelligent Transportation Systems, vol. 12, no. 3, September 2011.
[11] Yong Hao, Yu Cheng, Chi Zhou and Wei Song, "A distributed key management framework with cooperative message authentication in VANETs", March 2011.

BIOGRAPHY

1. **Jayanth S** is a student pursing B.E. Department of Computer Science and Engineering in Prince Shri Venkateshwara Padmavathy Engineering College.

2. Saravanan I S is a student pursuing B.E. Department of Computer Science and Engineering in Prince Shri Venkateshwara Padmavathy Engineering College.

3. Kapilavani R K is an Assistant Professor working in the Department of Computer Science and Engineering, Prince Dr. K. Vasudevan College of Information Technology,