Cyclic Group Key Administration Techniques for Multicasting in VANETs

D. Sudharani
Department of Computer Science and Engineering
Gudlavalleru Engineering College
Gudlavalleru-521356

K. Amrutasagar
Department of Computer Science and Engineering
Gudlavalleru Engineering College
Gudlavalleru-521356

ABSTRACT
Vehicular Ad Hoc Networks (VANETs) are the most popular application of wireless communication technologies. There are two types of communications i.e.vehicleto vehicle(V to V) and vehicle to road side units (V to RSU). To communicate with other vehicle or to receive services from Trusted authorities (TA) group communication can be held. The group key will be changed during member join into the group or member leave from the group to provide forward secrecy and backward secrecy. To reduce no of rekeying operation this paper proposed cyclic group key administration and provides security member join into the group or member leave from the group to provide forward secrecy and backward secrecy.

Keywords
Trusted authorities, Vehicular secret key, cyclic group theory, rekeying operations

1. INTRODUCTION
Vehicular Ad-hoc Network (VANETs) [1] are the most popular application of wireless communication technologies. VANET consists of three major components, namely the Trusted Authority (TA), Road Side Units (RSUs) and vehicles. The TA provides a variety of online premium services to the VANET users through RSUs. The RSUs are fixed at the road sides which are used to connect the vehicles to the TA.VANETs are developed to provide attractive services such as safety services and comfort services. Two types of communications are performed in VANETs. The first type is the Vehicle to Vehicle (V2V) communication in which the moving vehicles can communicate with each other and the second type is the Vehicle to RSU (V2R) communication in which the moving vehicles can communicate with the RSUs which are located aside the roads In a VANET group chance to share information between members and with TA also. V2V and V2R communications are performed through an open wireless channel,these communications are vulnerable to various kinds of attacks.VANETs one special type of adhoc networks broadcasting approach is used for data dissemination.

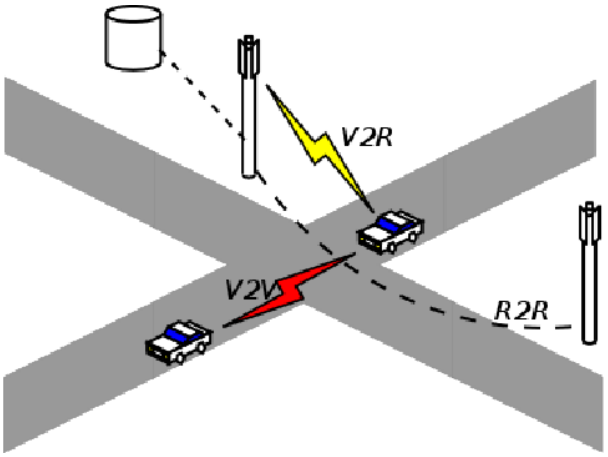

Fig.1 Vehicle to Vehicle (V to V) and Vehicle to RSU in VANET

2. PREVIOUS WORK
A group key management scheme in which the TA computes two different group keys intended for two different groups in VANETs. The group is a very important concept in the previous paper. Based on the money paid to the TA, a very simple Service Level Agreement (SLA) is considered between the TA and the vehicle users, which categorize the vehicle users into three groups, namely Primary Users (PUs), Secondary Users (SUs). The PUs are eligible to get attractive services such as comfort services, safety, and interactive services from the TA. The PUs are authorized VANET users who receive these services from the TA side periodically. The SUs are also authorized VANET users who receive the attractive services such as safety services from the PUs without making any requests to them, but they cannot receive the information directly from the TA. The PUs can communicate with each other by means of V2V communications. However the SUs can also communicate with each other after getting the SUs group key from the TA through PUs. Both the PUs and the SUs will have a valid VSK received from the TA. To disseminate the information from the TA side to PUs side in a secure way, the TA encrypts the information using a common group key which is derived using individual vehicles secret key of Pus by using Chinese Remainder Theorem (CRT) [2].

Let k1,k2,k3,...,kn be pair wise relatively prime positive integers, and let a1,a2,a3,...,an be positive integers. Then, CRT states that the pair of congruence's, $X \equiv a1 \bmod k1$, $X \equiv a2 \bmod k2$,...,$X \equiv an \bmod kn$ has a unique solution mod $\partial g = n\ i=1(ki)$. To compute the unique solution.

The key management scheme implemented 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 takes single broadcast messages from TA to inform the group members in order to recover the updated group key. The Number Theory Research Unit (NTRU) based group key management scheme uses a multiplication ring from which it chooses some polynomial values as private and public keys from which it computes a common group key. Hence, the multiplication operation used in this scheme is performed by using the convolution product method. All the remaining schemes use a multiplicative group for choosing and computing the keys.

3. PROPOSEDWORK

This paper proposes a cyclic group key administration by using VSK. VSK generated by using Chinese Remainder Theorem (CRT). Mainly concentrating on rekeying operations because to increase computational speed. A cyclic group key administration is to reduce number of rekeying operations at the time of user joining in to the group and user leave from the group for providing forward secrecy and backward secrecy [3].

A cyclic group or monogamous group is a group that is generated by a single element. That is, it consists of a set of elements with a single invertible associative operation, and it contains an element g such that every other element of the group may be obtained by repeatedly applying the group operation or its inverse to g. Each element can be written as a power of g in multiplicative notation, or as a multiple of g in additive notation. This element g is called a generator of the group. Here uses VSK for the cyclic node i.e. g. The group key also changes at the time of user join and leave operations. Technically we say forward secrecy and backward secrecy. A forward secrecy is the technique of preventing a PU from accessing current communication after leave operation. When a PU leaves the group, he or she may try to derive the group key by using any attacking methods. A Backward secrecy is the technique of preventing a new PU from accessing the previous communication before joining the group. In order to access the previous communication, an adversary needs to obtain the previous group key. Due to the reasons for every user join and leave operations group key will be changed for the security purpose .and the information also will be exchanged between group member's. Group members also able to know from which member we received information at the time of disturbances. Based on the VSK information will be passes. Due to this no of keys reduced and information also secured this process will be done in cyclic manner [4].

4. SYSTEM OVERVIEW

4.1 Step1: Registration of user

1. The VANET user can register his / her vehicle through offline having details like Name, Address, Phone no, Email id, Type of user. This process will be done by TA. TA is responsible for sharing information among VANET group.

2. After completing the registration process, the TA provides the VSK to the registered user, which is unique for every vehicle and the TA also maintains the list of all the vehicles and the irrespective VSKs in its storage area. The VSK is used for creating the Hash Code (HC) and the HC is verified by the TA for authentication and then the TA provides AC to the authenticated VANET users.

3. Based on the services users divides into primary users (PU) and secondary uses (SU) group.

4. Here this paper proposes six types of groups i.e. Primary Users with their respective vehicle category and Secondary Users also.

5. TA has the responsibilities like group information Maintenance and information passing.

4.2 Step2: TA authentication process and authenticating code

1. Each vehicle selects a random number N. After selecting the random number, it successively creates a Hash Code (HC) using N and VSK by SHA_256 algorithm.

$$HC = SHA\_256(VSK||N)$$

2. The TA generates the HC using the random number N and the VSK by SHA_256 algorithm and then verifies the newly computed HC value with the HC which is sent from the vehicle side[5].

4.3 Step3: Group Communication

1. Based on the group category services will be provided. To provide security for group member's key updation is required for every member join into the group and every member leave from the group. So that number of rekeying operation increased. To reduce such problems this paper proposed cyclic group key administration.[6].

2. TA can multicast the information to the authenticated vehicles. The authenticated vehicles can broadcast that information to other vehicles in a secure way. To multicast the information from the TA side and to broadcast the information from one vehicle to other vehicles. The TA generates two different group keys for two different groups of users, namely primary user group and secondary user group. In the generated group keys, one group key is used for multicasting the information. After user joins and leave group key will be changed for the purpose of security using only VSK. So that no of rekeying operations reduced.[7].

5. RESULTS

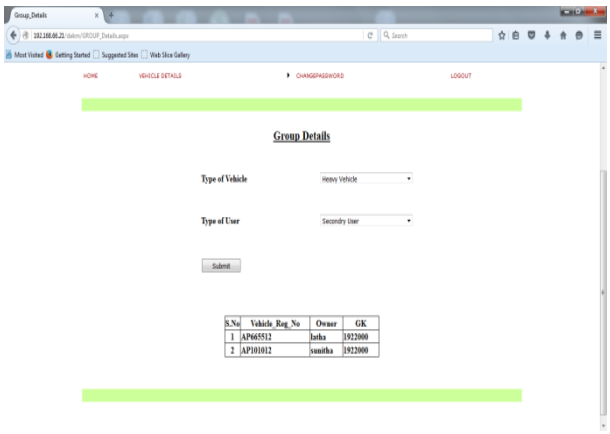

Fig 2: Group details of heavy vehicle and secondary user

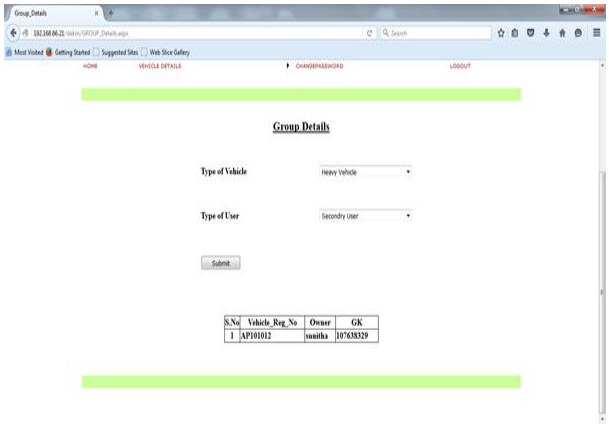

Fig 3: Group details of heavy and secondary vehicle after user exit

From the above figure 2 and figure 3 user names like sunitha and latha having same Group key 1922000. After user Latha exit from the group, then the group key is changed i.e.107638329 for the security purpose. Here the rekeying of group key will be done in the respective type of group only.

6. CONCLUSION

This paper proposed how to communicate with group members with less number of rekeying operations. The group key will be changed during member join into the group or member leave from the group to provide forward secrecy and backward secrecy. VSK is generated by using Chinese Remainder Theorem (CRT) and the information passing between VANET members. Vehicle Secret Key (VSK) a cyclic group VANET group can be performed in a by updating small amount of information and multicasting data to the group members. The results of proposed cyclic group key communication provide less no of keys while in the user communication can be done.

7. REFERENCES

[1] CarlosdeMoraisCorederioandDharmaPrakashAgarwal,"AdHoc and Sensor Networks: Theory and Applications"

[2] J. Zhou and Y. H. Ou, "Key tree and Chinese remainder theorem based group key distribution scheme".

[3] Alonso, J.Meta l(1991) "Group theory from a geometrical view point".

[4] Melisa Hajyvahabzadeh"An efficient group key management using code for key calculations for simulations on join/leave CKCS".

[5] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs".

[6] J.A.M.Naranjo, J.A.L.Ramos, andL.G.Casado,"A suite of algorithms for key distribution and authentication in centralized secure multicast environments".

[7] P. Vijayakumar, S. Bose, and A. Kannan, "Centralized key distribution protocol using the greatest common divisor method" Comput.Math.