International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:12, 2008

Strategies for Securing Safety Messages with Fixed Key Infrastructure in Vehicular Network

Nasser Mozayani, Maryam Barzegar, Hoda Madani

***Abstract*—**Vehicular communications play a substantial role in providing safety in transportation by means of safety message exchange. Researchers have proposed several solutions for securing safety messages. Protocols based on a fixed key infrastructure are more efficient in implementation and maintain stronger security in comparison with dynamic structures. These protocols utilize zone partitioning to establish distinct key infrastructure under Certificate Authority (CA) supervision in different regions. Secure anonymous broadcasting (SAB) is one of these protocols that preserves most of security aspects but it has some deficiencies in practice. A very important issue is region change of a vehicle for its mobility. Changing regions leads to change of CA and necessity of having new key set to resume communication.

In this paper, we propose solutions for informing vehicles about region change to obtain new key set before entering next region. This hinders attackers' intrusion, packet loss and lessons time delay. We also make key request messages secure by confirming old CA's public key to the message, hence stronger security for safety message broadcasting is attained.

***Keywords*—** Secure broadcasting, Certificate authority (CA), Key exchange, Vehicular network.

I. Introduction

REGARDING to widespread applications of wireless communication and networks in human's daily life, nearly all aspects of people's life deal with such applications. One of these applications is related to vehicles and driving so that aims of this network are safety provision and a better traffic management. Based on this need, a special kind of wireless network is assigned to inter vehicular communications. This network that's nodes are vehicles and has an ad hoc nature is called Vehicular Ad hoc Network (VANET). In VANET, a vehicle communicates with other vehicles (V2V) and also communicates with roadside infrastructures (V2I) by means of communication facilities[7].

Nasser Mozayani is associated professor of Computer Engineering Faculty, Iran University of Science and Technology, Narmak, Tehran 16846-13114, Tehran, Iran (e-mail: mozayani@iust.ac.ir).

Maryam Barzegar is with the Technical and Engineering Faculty of Olom Tahghighat, Islamic Azad University, Hesarak, Tehran, Iran (e-mail: m.barzegar@gmail.com).

Hoda Madani is with the Technical and Engineering Faculty of Olom Tahghighat, Islamic Azad University, Hesarak, Tehran, Iran (e-mail: hdmadani@yahoo.com).

This research is supported by Iran Telecommunication Research Center (ITRC).

The most important usage of these networks is informing vehicles in emergency cases such as car accident, urgent breaking or traffic jam [10]. In such cases, a vehicle can inform other vehicles by means of broadcasting safety messages. As a result other cars may have appropriate reaction regarding that event beforehand.

Each vehicle is equipped to a communicating device called OBU (On Board Unit), Roadside unit (RSU) also can provide additional traffic related messages for vehicles to make them know particular road conditions such as road constructions ahead and maximum curve turning speed.

Security is always a challenge in networks but in VANET it is more essential. Safety maintenance is accomplished in these networks by means of safety message exchange. Since these messages have direct impact on people's life, securing vehicular network will be a vital task. Safety Messages should be sent from credited transmitter (Authentication) and contain proper and unaltered information (Data Integrity). Privacy which includes private information of the vehicles is too important to prevent vehicle tracking. Maintaining non-repudiation in cases of accidents and crimes is necessary so the driver's identity can be retrieved from message and it can not repudiate it.

Prevention of possible attacks like replay attack and false message attack is important in these networks. Hence security mechanisms should be taken in safety message transmission and reception.

Most of the existing works [1], [8], [11] do not comply all applicable needs for securing safety message. Thus we first state needs for securing these networks. Then with respect to those needs, we select the most appropriate security protocol. At the end we resolve its implementation challenges by proposing solutions to increase its performance in large scale usage.

In this paper we have the following steps ahead: First we describe a typical VANET network's architecture. Then we have a look at related works for safety message security provision for VANET in section 3. In forth section we state requirement for satisfying security requirements and select a distinct protocol as our framework. In fifth section we try to resolve challenges of the selected protocol by proposing strategies for safe message exchange in boundary region. Finally in sixth section we bring security analysis and

evaluation and conclusion.

II. Network Architecture

At first we study interconnections between VANET components and present two layers as seen in figure 1:

1. Down Layer: This layer includes RSU, OBU and messages are broadcasted based on DSRC communication protocol [13]. For control message exchange, vehicles use 802.11e protocol to communicate with RSU.
2. Upper Layer: It includes base stations (BS) and central systems such as CA. The links between these components are either wired or wireless based on 802.11e protocol. An RSU receive all messages and requests from down layer and sends them to BS in upper layer. It also receives responses from CA and transmits them to the OBU.

   Hint: Control message are used for signaling purposes such as key request and reply.

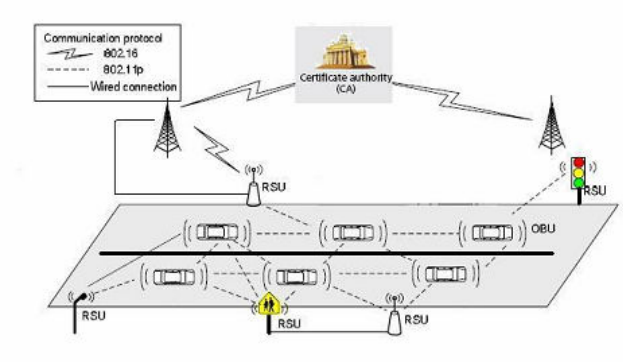

Fig. 1. Network Architecture

III. Related Work

Several jobs have been accomplished in field of securing vehicular networks. In most of them, security is generally considered. Rarely attention paid to securing safety message as an implementable method in vehicular network. In [11], a routing protocol is used based on geographical position to make its functions and services secure. After each vehicle's position is acquired by means of GPS receivers, their positions along with their identities are saved in a table inside OBU. This table is exchanged via periodically received message from other vehicles. These methods comply security aspects such as authentication, data integrity and non-repudiation, but the protocols have no concern with privacy and anonymity. The used approach in [11] is a public key infrastructure (PKI) and verification of received messages is applied logically based on speed, time and position of message's transmitter. In [8], positional information is sent to all other vehicles as done in [11]. This protocol maintains robustness to Sybil attacks. Also false message attacks can be detected easily because of logical investigation performed. Since these protocols are location based and are unable to preserve anonymity and privacy, they are fragile about tracking attacks and it's the main vulnerability of these methods.

In [2], [3], [6], researchers have used group signature to preserve anonymity and privacy of vehicles. In these methods, each vehicle is assigned to a group of vehicles. This is for the sake of anonymity preservation inside the group when secret information of nodes is only available to the group manager. Group manager is head of a group that's duties are key generation, signature generation and verification member registration, membership revocation and identity recovery of vehicles. Whereas a group manager has numerous tasks to do, its overload goes up when group's population increases. In [3], group manager uses a pair of public-private key for privacy preservation and a special key for maintaining authenticity in a group. In [1], anonymity of vehicles is satisfied by using an authentication protocol based on random symmetric keys. At first, some symmetric keys are selected from the key set randomly. Since some vehicles may receive identical keys in this random key assignment, a vehicles' identity can not be disclosed as long as it is not unique so it yields anonymity. Also key revocation becomes easier, because every car owns several keys. One of disadvantages of said method is high probability of attacks whereas adversaries can easily access some of keys and use them to send false message. In addition, to know identity of a vehicle we require all keys related to that vehicle, it is the second disadvantage of this protocol. These make message exchange needed for authenticating a vehicle cumbersome and time-consuming.

In [5], digital signature technique is used as an approach to make inter-vehicular network secure. In this paper, a combination of several mechanisms is utilized for VANET security. In car to car communication pair keys and session keys is used, but in the case of group communication and broadcasting a shared key is distributed among members before initiating any connection. For group management, a cellular partitioning is employed and the nearest node to origin of cell is selected as group manager whose duty is public key transmission. One of significant deficiencies of this method is lack of non-repudiation preservation in information exchange. It is because it doesn't leave any certain identity inside the message to be recognizable later. By the way, dynamic nature of group managers due to consecutive position change of members and lack of supervision for members are challenges exist in this protocol. In [4], a solution is proposed to make broadcasting secure in inter-vehicular communication. In this approach, a hybrid key infrastructure is employed to maintain the security aspects. Authentication is satisfied by a shared symmetric key in every region, so by this way, anonymity and privacy are also gained simultaneously. Non-repudiation is the other aspect satisfied by using a symmetric private key to encrypt message transmitter's identity. It's also robust against most of attacks and ease of implementation is another advantage of this protocol.

Totally, each of proposed solutions has its own advantages and disadvantages but SAB protocol proposed in [4] is more comprehensive.

In this work, we focus on security preserving in safety message broadcasting scheme. With respect to rapid change of configuration, in these networks and short response time of drivers to incidents, a selected method should lessen encryption-decryption delay and minimize message length.

IV. Security Requirement and System Assumptions

A. Security Requirement

Four security aspects are concerned in safety message broadcasting:

- Authentication: Every receiver vehicle should make sure of message transmitter's authority and authenticate it.
- Non-repudiation: Every vehicle should put part of its personal information so it can be recognized in the case of crime occurrence and insurance. Thus, repudiation becomes impossible by the transmitter.
- Privacy: Personal information of vehicles and drivers shouldn't be accessible by other vehicles and the anonymity should be preserved to stop tracking. The exception is for authorized organizations.
- Data integrity: The transmitted message should contain valid information not to be altered by attackers.

According to above issues, the security mechanism should offer a solution that complies the desired aspects.

In security topics, for maintaining both authentication and anonymity, we use a group infrastructure [9]. In this style, each vehicle should be registered in a group and receive its public authentication key (AK) before any message transmission. For signing a message, the vehicle uses group authentication key and encryption function and sends it along with original message. Therefore it is not obligatory for each member to have other members' private information such as their identity and public key for authenticating them. Receivers verify a member's authenticity by signature verification. It's attained by reconfirmation of encryption function with authentication key to the received message and comparing the result to the signature.

$$V \rightarrow *, M, HMAC_{Ak}(M)$$

Also, receivers can make sure of transmitted data integrity, after they verified the signature.

By applying above approach, three security dimensions authentication, data integrity and privacy are being maintained. This should be reminded that, confidentiality aspect of security is not obligatory in this application. The reason is broadcasting nature of safety message, where messages can be received by all vehicles (valid or invalid) and their information is apparent to all, this makes no problem.

About preserving non-repudiation, a vehicle's identity should be attached to the message, so it can be tracked whenever desired. Accordingly, vehicle tracking is only allowed just for authorized organization. So the vehicle should encrypt its identity and only authorized organizations is capable of decryption. Hence, encryption of car's identity should be done by means of assigned public key (PU) from authorized organization and be put in a distinct field to inside original message.

$$V \rightarrow *, M, HMAC_{Ak}(M), E(id_V)_{PU}$$

Since vehicle's identity is encrypted by a public key, other vehicles are not able to recognize it and just authorized organization own the private key associated to the public key can access its identity. It is worth to say that public key should be assigned to the vehicles immediately after they manufactured as well as AK.

As mentioned before, our aim is to propose an applicable solution for security maintenance of safety messages broadcasting in VANET, so its practical implementation has most priority. Various activities have been done about security establishment in vehicular ad hoc networks, but few paid attention to maintaining security in broadcasting platform. The proposed schema at [4] is one of protocols that heeds broadcasting and contains security issues like group signature and other trends to make security preserving reasonable.

B. System Assumptions

As implied in previous methods, we need a key infrastructure for AK and PU generation and distribution.

We can divide all proposed methods to two principal categories:

1- Methods that rely on group signature with a dynamic selection of group manager, we call these dynamic methods.

2- Methods that make use of a fixed infrastructure for key management, we call these static methods.

In dynamic methods, nodes need membership in a group and receiving keys before any connection. According to high speed of vehicles and rapid change of network topology, the established groups are not stable and may decompose. Group manager determination and key distribution are also complicated and time-consuming. Since each vehicle has a chance to be group manager, all vehicles should be facilitated to perfect equipments. The other disadvantage is for tracking a vehicle via a specific message, it is necessary to find the vehicle was group manager at the time the message was dispatched.

The above mentioned issues make network vulnerable against most attacks. For instance, an attacker may be selected as a group manager and may disorder network's functionalities.

These are our motivation to select static methods. In static methods, key management is more convenient and applicable relative to dynamic schemes.

Here in static methods, we have a fixed central entity for key management. For more scalability, it's better to make use of a hierarchical structure due to large number of vehicles and network size expansion. For this reason, we divide a country to multiple regions with respect to density of vehicles and assign a CA (Certificate Authority) to each region. For synchronized management, we connect all CAs to a central

CA called CA_{ROOT}. Any CA is responsible for key generation, distribution and management and it is the only trust entity for tracking vehicles.

When we select static methods, we have to consider its specific requirements. In static methods, we have defined regions under CA supervision. Since each CA has a key set for securing message exchange in its own region, a vehicle face problems when it's region changes. The problem is the vehicle has still its old key set belong to former CA where it needs new key set for communication in new CA's territory.

Regarding to high mobility and transportation between regions, managing boundary region for key replacement is a critical issue. Hence, continuity maintenance and avoiding interruption in boundary regions is of CA's duties. The proper management of boundary regions reduces vulnerabilities and attacker's intrusion.

V. The Proposed Schema

In this paper, we propose an applicable approach based on SAB protocol [4] and optimize it in regional boundaries. SAB protocol doesn't have any strategy for managing regional boundaries.

Because safety message exchange between vehicles is dependent on CA's key set, positional change from a region to a new region may make problems for message exchange. Therefore region change awareness and sending request for new key set (AK and PU_{CA}) is an essential task for vehicles.

Since regional borders are located far away from CA, processes of key request transmission, authenticity verification and key assignment becomes time-consuming, so interruption happens because of lack of new keys, especially when vehicles running high speed. This halt leads to loss of vital information about accidents and unpredicted events, so life and property damage are unavoidable whereas vehicles all rely on network facilities and warning systems. By the way, this interruption can be a chance for intruders and adversaries to make serious attack on the network.

Because of this, the scheme of information exchange at regional boundaries becomes a serious challenge. It can be a problem for every protocol based on region partitioning that depends on central manager in each region. As a result, it makes the task more convenient if we delineate CA territory assignment and determine region lines or curves, before we go to message exchange issues.

A. CA Selection Schemes

According to reliance on keys in security methods, generation and distribution of keys needs a distinct infrastructure and process. To make protocols more scalable, we should first distribute management and control. It means that instead of determining just a CA, we can designate multiple CA in different locations and specify a central CA for management of CAs [12]. The connection style between CAs is shown in Figure 2.

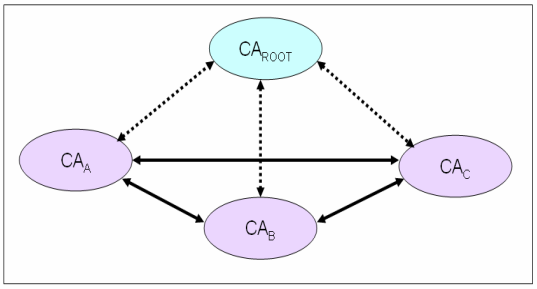

Fig. 2. Relations between CA

CA determination scheme in a country depends on geographical area and density of vehicles. We have to consider that CAs shouldn't be close to each other to avoid abundant key request exchange. It's because, transition rate between two CA increases when they are close. In case of high vehicle density in a CA, we can specify some definite RSUs under CA's control and distribute CA's heavy overload among them. A rational assignment of CA to various regions is desired. It's because this proper assignment will decrease message exchange delay and impede intruders or adversaries. In the sequel, we focus on how to determine boundary lines as it plays a significant role in reducing interruption at regional boundaries.

B. Boundary Line Determination

Determining boundaries for CA and assigning their own regions in an optimum scheme is always desired. Hence it's better to choose regional lines on furthest distance relative to the central CA. They are usually located in roads and inter-cities.

To shun consecutive key request exchange, regional lines should be in positions that vehicles' direction of movement does not change consecutively and the change should be foreseeable. For instance regional lines should not be posed around U-turns, squares or intersections. It's because when the vehicle exits a CA's territory and enters the new CA's area before new CA processes its key request, it turns back to former CA's region and re-sends the request to former CA. This increases CA overload dramatically.

Another solution is to make use of mobility prediction methods to assess direction of movement and trajectory. By applying this method, key request messages decrease in boundary regions. It's noticeable that one key pairs of authentication key and public key are needed for message exchange in each region, thus regions under CA coverage should not have any common area.

$$\forall\, i, j \Rightarrow R_i \bigcap R_j = \phi$$

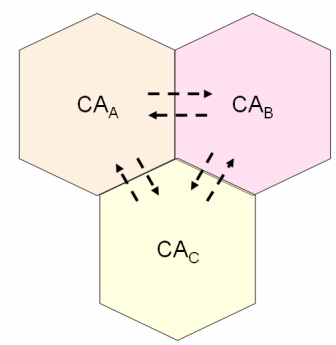

Fig. 3. Regional boundaries

C. Message Exchange in Regional Lines

When a vehicle receives messages that cannot decrypt them, it will sense region change. To prevent time delay and data loss, vehicles must receive public and authentication key of new CA before entrance to its territory. So vehicles should be able to recognize neighbor CA and send it key request in advance. We proposed two methods that can be accomplished by CA or the vehicle itself.

1- By old CA: In this solution, current CA sends region change message and waits for new keys request from vehicles. It performs these by means of boundary RSU. If this RSU received the reply message including key request, it sends this message to current CA. This CA also announces the request to new CA and waits for response. New CA then asks CA home (CA_h)[1] for validity of this vehicle. If CA_h confirmed it new CA will send authentication key and public key to the vehicle by means of boundary RSU, unless it books this vehicle invalid at CA_h database. Thus, the vehicle will have new keys before arriving new region. In this method, the vehicle is made aware of entering new CA region when it receives message that are not decryptable by former keys so it replaces old keys with new ones.

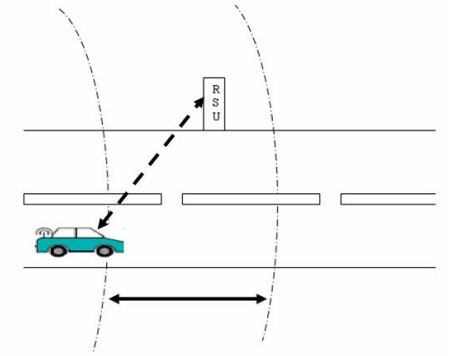

Fig. 4. Boundary region

It's noticeable that boundary's zone should be wide enough that all vehicles could receive new CA key set before entering new region.

2- By the vehicle: In previous method, existence of RSU around boundary regions for informing vehicles is necessary. That approach may be unsuccessful due to lack of infrastructure around border or failure occurrence in message transmission stages. In this method, the vehicle itself is responsible for region change awareness. Vehicles receive all regional boundaries after they entered to a CA's region. Each vehicle will have a table of boundary coordination with their associated CA so it can measure degree of closeness to boundaries by calculating the distance periodically. If the distance lowers from a threshold, it sends key requests to the RSU near to boundary. Whereas these request are so momentous, vehicles should receive acknowledge from related RSU and re-send the request in the case of no reception. Actually, this method is accomplished by means of a look-up table and computation of distance to boundary. Hence the vehicle will have key set before new region arrival.

To increase reliability, we can use hybrid method that's a combination of two solutions presented above.

D. Securing Key Exchange Process

When a vehicle changes its region, one of the important issues is reception of correct keys. Since safety messages contents are critical and securing them is achieved by means of keys, preserving integrity of keys is essential. To do this, we have to apply a security mechanism for keys protection.

An appropriate message structure quarantines key protection against attackers and prevents key alteration during exchange process.

In our scheme, we use the same keys were used for securing safety message in old CA to encrypt key request message being sent to new CA. Figure 5 shows key request message format:

Req
ID_{OCA} ,ID_{CAh}
$E(M, ID_V, E(Req, ID_{OCA}, ID_{CAh})_{SK})_{PUOCA}$

Fig. 5. Key request message format

Req defines type of request that is request for public key and authentication key of new CA.

ID_{OCA}, ID_{CAh} are identities of old CA and home CA respectively.

In third field, M includes velocity, position, time and direction. ID_V is identity of vehicle and $E(Req, ID_{OCA}, ID_{CAh})_{SK}$ is encryption of first and second field of the message with secret key (SK) of the vehicle. All of three mentioned entries are encrypted with the public key of current CA.

Encryption of content of third field with PU_{OCA} key is for privacy preserving of the vehicle against attackers to prevent tracking. Indeed encrypting Req, ID_{OCA} with SK makes the message robust to masquerading attack.

[1] Each vehicle first register at CA_h and all information about vehicles and driver are first existent at this CA.

We have also defined a format for reply message as shown in Figure 6:

Rep
ID_{NCA}
$E(PU_{NCA}, AK)_{SK}$

Fig. 6. Reply message format

Rep defines type of request that here is reply for key request message.

ID_{NCA} is identity of new CA.

In third field, public key and authentication key of new CA are encrypted with vehicle's secret key (SK). Encryption of PU_{NCA} and AK with secret key makes protection of these keys from disclosure.

VI. Analysis and Evaluation

Threat Analysis

A. Serious Attacks on Boundary Region

Boundary regions are vulnerable points in fixed infrastructure. Attackers and intruders can abuse of interruption takes place for new key reception.

The most probable attacks are as follow:

False message attack: In this attacks goal of attacker is to mislead vehicles that cross boundaries and enter new region. This attack is from credible vehicles by transmitting repetitious encrypted messages with valid keys of old CA's region. If no attack occurs, the vehicle can be aware of region change when it receives multiple messages that are not able to decrypt them. Therefore, it sends key request to the CA and will make sure of region change when it receives new key set. In false message attack, the attacker tries to hinder vehicles from region change awareness.

Our proposed scheme stops this attack by informing the vehicle of region change, so it will have new key set before entering to new region.

Loss of credibility: If false message attack happens or any other reason that prevents vehicles from sensing region change, the vehicle resumes disseminating safety message with old keys that are not valid keys in this region. This causes the vehicle to be identified as an attacker in new region, so the vehicle will lose its credibility. Our work also stops this event by means of informing the vehicle and making it credible by new key assignment before it crosses boundary.

B. Attacks to Control Message

Control message at regional boundaries have important information about keys, thus securing their transmission is very essential. So we have proposed secure format for it. In this section, we analyze the resistance of this format against some important attacks.

Tracking: Since boundaries are bottlenecks in regions and vehicles density is lower than in cities, attackers tend to track vehicles by accessing to identity of vehicle or preparing a list of vehicles enters to a region for special reasons. This can be achieved from key exchange message. To repel this attack, we encrypt identity of vehicles with CA's public key as shown in Figure. 5, that only CA is able to decrypt it for checking vehicle's creditability.

Masquerading: A very important attack at regional boundaries is that the attackers try to access key set by sending key request message as well as other credible vehicles. The attacker may access to valid identity of vehicle but it can not generate this part of message ($E(Req, ID_{OCA})_{SK}$) with secret keys of vehicle. It's because only home CAh and the vehicle associated with that identity have SK and can generate that part. As a result, this attack is repelled.

Performance Evaluation

C. Time Delay

A good security mechanism has short delay for encryption, decryption and key exchange. In our proposed scheme, for sending safety message vehicles generate message digest by means of HMAC function and encrypt ID with P-224 curve. The HMAC operation is very faster than encryption and its delay is not considerable in comparison with encryption delay. In reception of message, the vehicle only generate message digest with AK and compares it with received message digest that takes very short time. Other decryption processes are accomplished by CA that does not influence overall delay.

Since frequency of safety message reception is more than its transmission, this method is acceptable [4].

To exchange key set at regional boundaries, these stages are needed, as shown in Figure. 7:

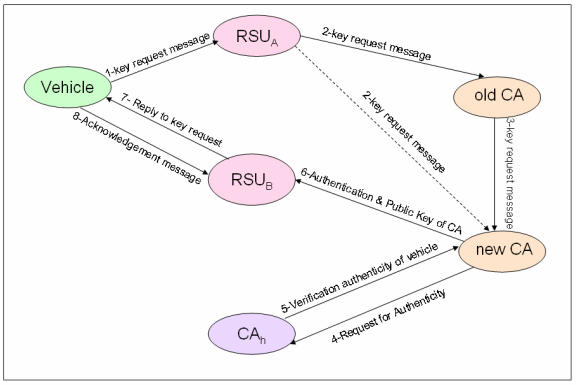

Fig. 7. Key request to key reception stages

1- Key request message transmission to nearest RSU (D_1).

2- Message type recognition by the RSU and sending it to old CA. In SAB protocol this message is sent to new CA

(dash line in Figure.7) after entering it and in this protocol stage 3 is bypassed (D_2).

3- Message type recognition by CA and sending it to new CA that the vehicle is coming to its territory based on direction of movement (D_3).

4- Message type recognition by new CA and verifying vehicle's authenticity by sending authenticity request to CAh (D_4).

5- Authenticity Verification of the vehicle by CAh and sending the reply to new CA (D_5).

6- If the vehicle is authenticated, new CA sends authentication and public keys as reply message to the vehicle; unless sending a message to CA_h to refuse vehicle's authentication (D_6).

7- Reply message is sent by RSU in broadcasting way to be received by that certain vehicle (D_7).

8- Decryption of message by the vehicle and sending Acknowledge (ACK message) to that RSU (D_8).

$$D = D_1 + D_2 + D_3 + D_4 + D_5 + D_6 + D_7 + D_8$$

According above mentioned process, a total delay (D) occurs that this delay is related to factors such as degree of closeness to RSU, connection style of components and overload of the components (RSU, CA).

The longest delay (D') occurs when the vehicle enters to new CA until perception of new region entrance and sending key request message. In SAB protocol, this delay adds to D and hence lots of attacks may happen.

$$D_{total} = D + D', \quad D' >> D$$

By these two proposed methods, the vehicles are announced before entering to new CA by means of current CA or by the vehicles itself and the D' is eliminated. Hence, this method reduces key exchange process delay.

D. Securing Safety Message and Control Message with Same Key Set

Using the least number of keys for securing a system is very noticeable. In some proposed security methods for VANET, different keys are use for securing each communication that makes key management more sophisticated and time-consuming. In this way, the more key exchange process is needed and hence it is more vulnerable. In our scheme, we have used three keys (AK, PU_{CA}, SK) for securing both safety and key exchange message. Also we proposed a secure format based on them. Therefore our schema reaches irresistible security and faces fewer risks.

E. Comparison with Other Methods

In this section, we compare some methods for securing broadcasting safety messages. As shown in table 1, we compare four methods that have mechanisms for securing safety messages. The performance criteria for comparisons are resistance against important attacks, compliance of 4 security dimensions, time delay and number of required keys. We show our proposed method as D-SAB (Developed SAB) in the table.

Table. 1. Comparison of four security methods for safety messages

Performance Criteria \ Method		Position Base	Group Signature	Random Symmetric Key	SAB	D-SAB
4 Security Dimensions		Except Privacy	✓	✓	✓	✓
Attacks To Safety Messages	**Tracking**		✓	✓	✓	✓
	Masquerading	✓	✓	✓	✓	✓
	False Message	✓				✓
Attacks To Control Messages	**Tracking**		✓	✓		✓
	Masquerading					✓
Delay	**Generate Message**	T_E	T_E	T_E	T_E	T_E
	Receipt Message	T_D	T_D	T_D	T_H	T_H
	Key Exchange	-	T_{EX}	T_{EX}	T_{EX}	-
Number of Key		$2n+N_G$	$2n+N_G$	n.k	$n+2N_{CA}$	$n+2N_{CA}$
Type of Infrastructure		Dynamic	Dynamic	Dynamic	Static	Static

T_E time of encryption
T_D time of decryption
T_H time of generating message digest with HMAC
T_{EX} time of key exchange
N number of vehicles
N_G number of group
N_{CA} number of CAs

VII. Conclusion

In this paper, we proposed an applicable method for securing safety message and solve problems that we face to for implementation. First, we selected a fixed key infrastructure that has less overload and delay. This infrastructure has several fixed regions with central manager called CA that has its own keys to assign each vehicle. The most important problem in this infrastructure is key exchange at boundaries between regions. In this paper, we obviate this problem by informing vehicles to receive new key in advance. In this method, we made vehicles aware of region change by means of current CA or vehicles themselves before entering new region. By using this solution, we avoid many attacks that may occur at these points and prevent vehicles from possible invalidity.

We also proposed a secure format for key exchange message by means of the same keys used for securing safety message. At the end, we evaluated our method by resistance against attacks, time delay and overhead criterias and compared it with other methods.

In this paper, we explained more about securing safety

message based on fixed key infrastructure and remove some challengeable problems. So securing other applications such as pair wise communication, traffic information based on this key infrastructure may be considered for future works. Optimum methods for CA selection and region assignment are also another research area.

REFERENCES

[1] Yong Xi, Kewei Sha, Weisong Shi, Loren Schwiebert, Tao Zhang, Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks, In Proceedings of the 8th International Symposium on Autonomous Decentralized Systems (ISADS), March 2007
[2] X. Sun, X. Lin, and P.-H. Ho, Secure Vehicular Communications Based on Group Signature and ID-based Signature Scheme, in Proceedings of International Conference on Communications (ICC), June 2007.
[3] J. Guo, J.P. Baugh, and S. Wang, A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework, Proceedings of the Mobile Networking for Vehicular Environments (MOVE) workshop in conjunction with IEEE INFOCOM, May 2007.
[4] Christine Laurendeau and Michel Barbeau, Secure Anonymous Broadcasting in Vehicular Networks, Proceedings of the 32nd IEEE Conference on Local Computer Networks (LCN), October 2007
[5] M. Raya and J. P. Hubaux, Securing vehicular ad hoc networks, Journal of Computer Security, Vol. 15, No. 1, pp. 39-68, 2007
[6] Zhang J., Ma L., Su W., Wang Y. Privacy-Preserving Authentication Based on Short Group Signature in Vehicular Networks, Data, Privacy, and E-Commerce, ISDPE, Nov 2007
[7] T. Leinmueller, L. Buttyan, JP Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, E. Schoch SEVECOM - Secure Vehicle Communication, 15th IST Mobile and Wireless Communication Summit Mykonos, June 2006.
[8] Yan G., Choudhary G., Weigle M. C., Olariu S. Providing VANET Security through Active Position Detection, VANET'07, September 2007.
[9] Douligeris C., Serpanos D. N., Network Security Current Status and Future Directions, Wiley-Interscience Publishing, chapter 1, IEEE 2007.
[10] Anjum F, Mouchtaris P, Security For Wireless Ad Hoc Networks, Wiley-Interscience Publishing, chapter 8, IEEE 2007.
[11] C. Harsch, A. Festag, and P. Papadimitratos, Secure Position-Based Routing for VANETs, 2007 IEEE 66th Vehicular Technology Conference (VTC 2007), September 2007.
[12] ITU-T Recommendation X.843, Information technology – Security techniques –Specification of TTP services to support the application of digital signatures, 2000.
[13] IEEE Vehicular Technology Society, 5.9 GHz Dedicated Short Range Communications(DSRC)- Overview, [Online]:Available:http://grouper .ieee.org/ \groups/scc32/dsrc/.