Threshold ElGamal-based Key Management scheme for distributed RSUs in VANET

Na Ruan, Takashi Nishide, Yoshiaki Hori
Department of Informatics, Kyushu University, Fukuoka, Japan
Email: ruanna@itslab.csce.kyushu-u.ac.jp, {nishide,hori}@inf.kyushu-u.ac.jp

***Abstract*—In Vehicular Ad Hoc Networks (VANETs), the vehicular scenario requires smart signaling, smart road maintenance and other services. A brand new security issue is that the semi-trusted Road Side Units (RSUs) may be compromised. In this paper, we propose a Threshold ElGamal system based key management scheme for safeguarding VANET from the compromised RSUs and their collusion with the malicious vehicles. We analyze the packet loss tolerance for security performance demonstration, followed by a discussion on the threshold. After discussion of the feasibility on privacy and processing time, overhead analysis is presented from two kinds of application scenarios: Emergency Braking Notification (EBN) and Decentralized Floating Car Data (DFCD). Our method can promote security with low overhead in EBN and does not increase overhead in DFCD during security promotion.**

***Index Terms*—Vehicular Ad Hoc Network, Distributed Road Side Units, Threshold ElGamal system, Key Management Scheme, Emergency Braking Notification, Decentralized Floating Car Data.**

I. Introduction

A. Background

The idea behind VANET is to have a mechanism based on which nearby vehicles on the road can communicate in order to provide safety and comfort to the drivers and passengers [18]. The fundamental vulnerability of VANET comes from open peer to peer architecture. Unlike wired networks that have dedicated routers, the wireless channel in VANET is accessible to both legitimate network users and attackers [17]. The attack may range from passive eavesdropping to active impersonation. Since compromising a vehicle or a RSU is possible, either trust relationship or tolerance [12] among them is very important in case of cooperative driving. There is no clear line of defense in VANETs from the security design perspective. These salient features of VANETs pose both challenges and opportunities in achieving the above security goals.

B. Motivation

RSU is lacking under some situations such as mountain road, where it is difficult to fix the RSU. Also, mountain road does not have enough density of the RSU nodes sometimes [1]. If one RSU misbehaves, the vehicles in its scope will be exposed under a dangerous environment. Considering the coverage range of broadcasting a message in VANET, we need to make sure that the vehicle which is broadcasting a message is not a selfish or malicious vehicle. Each car is assumed to carry out a certain amount of secure operations such as signing and time stamping [2]. Mobility is another concern to VANET developers, since vehicle network is random and mobile. And the authentication process should take place without affecting the privacy of the vehicles [18].

C. Related work

When the On Board Unit (OBU) of a vehicle has been registered at the Certificate Authority (CA), the vehicle is called a VANET ready vehicle [18]. Implementing security applications on a VANET ready vehicle can not be achieved without a regular maintenance of the equipment that VANET provides. Hao *et al.* [19] proposed a distributed key management scheme with protection against RSU compromise in VANET using group signature. The RSU acts as the key distributor in each group. However, misbehavior of RSU has not been considered under this situation. Sharp *et al.* [5] combined sensor network with VANET for vehicle tracking. The interface problems between sensor network and VANET should be payed attention. In [1], the basic structure of VANET and the basic requirement of a key management scheme in VANET are introduced. At the same time, the authors also proposed a key management scheme based on temporary anonymous certification for tacking together efficient authentication, revocation and privacy in VANET. It maintains almost the same overhead as the IEEE 1609.2 standard for VANET security.

D. Challenging issues

As a brief review of the related works [6, 10, 13, 16], we find many schemes requiring both the vehicles and RSU to store a large number of pseudonyms and certifications, where it is not convenient to implement a revocation scheme to abrogate the malicious vehicles and RSU. Moreover, lots of previous assumptions of implementing security applications on a VANET are based on that a ready vehicle can not be achieved without a regular maintenance of the equipment that VANET provides. The protection against compromised RSU is a general purpose in wireless network.

The above reasons motivate us to propose the Threshold ElGamal system [11, 20] based key management scheme for distributed RSUs (DRSUs) in VANET.

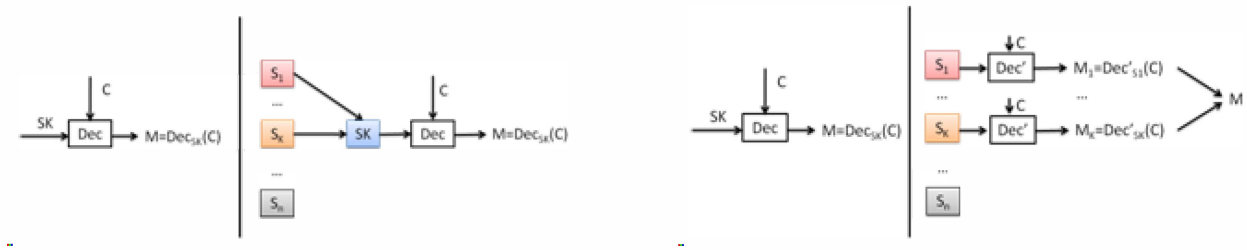
E. Organization

This work is organized as follows: Section II describes basic definitions and notions of Threshold ElGamal scheme which will be used for our proposal. Section III provides our proposal model. Section IV presents analysis of security and overhead. Finally, we draw conclusions and discuss our future work in Section V.

II. Preliminaries

In this section, secret sharing based on polynomial and corresponding Threshold ElGamal system are described.

978-1-4577-2004-8/11/$26.00 ©2011 IEEE



(a) Shamir secret sharing system

(b) Threshold ElGamal system

Fig. 1. Decryption in both Shamir secret sharing system and Threshold ElGamal system

A. Secret sharing based on polynomials

Before introducing the idea of secret sharing based on polynomial, the definition of lagrange interpolation should be presented firstly. Lagrange interpolation is used to reconstruct the secret key. In lagrange interpolation, a polynomial $f(x)$ and a set of $k+1$ points: $(x_0, y_0), (x_1, y_1)...(x_k, y_k)$ should be given firstly, where x_i are all distinct and y_i is equal to $f(x_i)$. As considering the lagrange coefficients $\lambda_j(x)[x_0, ..., x_k] \doteq \prod_{i=0, i\neq j}^{k} \frac{x-x_i}{x_j-x_i}$, we know that $f(x)$ equals $\sum_{j=0}^{k} y_j \lambda_j(x)[x_0, ..., x_k]$. Correspondingly, the secret key $f(0)$ equals $\sum_{j=0}^{k} y_j \prod_{i=0, i\neq j}^{k} \frac{x_i}{x_i-x_j}$.

To share a secret S, a (k, n)-threshold scheme is proposed. Choose $k-1$ random coefficients $a_1, ..., a_{k-1}$ and let $a_0 \doteq S$, the $f(x)$ equals $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + ... + a_{k-1} x^{k-1}$ **mod** q. Every participant is given a point in the polynomial. Participant i receives the pair $(i, f(i))$.

After encryption in this part, each participant is distributed one piece of the private key. To recover plaintext based on some pieces of a key by each k participants, we select Threshold ElGamal system for resolving this problem.

B. Threshold ElGamal system

We give a review of Threshold ElGamal system. It is in such a way that:

1) Key generation and message encryption are presented as follows:
   - $p = 2q + 1$, p, q primes.
   - Select x from Z_q randomly, while $y \doteq g^x$ **mod** p, g is a generator of the finite multiplicative group QR_p and its order is q.
   - Select $a_1, ..., a_{k-1}$ from Z_q randomly, while $a_0 \doteq x$.
   - $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + ... + a_{k-1} x^{k-1}$ **mod** q.
   - $PK \doteq (p, g, y)$, $SK_i \doteq f(i)$ for all i.
2) In $Enc_y(M)$ part, select r from Z_q randomly while $(c_0, c_1) \doteq (g^r, y^r \cdot M)$. M is the plaintext which is required to be protected.
3) Compared with decryption in Shamir secret sharing system (Fig. 1(a)) [11], Fig. 1(b) presents the decryption in Threshold ElGamal system by $Dec_x(c_0, c_1)$:
   - Different from Shamir secret sharing system which needs to collect all the fragments of ciphertext before decryption, each share holder i in Threshold ElGamal system creates a decryption fragment: $\mathbf{pad}_i = c_0^{SK_i}$.
   - Once the k fragments have been collected, reconstruct the pad: $\mathbf{pad} \doteq \prod_{j=0}^{k} (\mathbf{pad}_j)^{\lambda_j} = \prod_{j=0}^{k} (c_0^{SK_i})^{\lambda_j}$.
   - $M = c_1 / \mathbf{pad}$.

Indeed: $x = \sum_{j=0}^{k} SK_j \lambda_j$ and $c_0^x = c_0^{\sum_{j=0}^{k} SK_j \lambda_j} = \prod_{j=0}^{k} (c_0^{SK_j})^{\lambda_j}$.

Threshold ElGamal system can mainly avoid the following four aspects of attacks: node capture attack, malicious participant attack, passive attack and collusion attack.

III. Our proposal

A. Description of the whole scenario system

Architecture of a vehicular ad hoc network with our DRSUs-proposal is classified into three categories. Compared with original VANET [14], the three categories in our proposal are On Board Units, Distributed Road Side Units and Certificate Authorities. They have different security levels. An illustration of the system and functions of each entity is shown in Fig. 2.

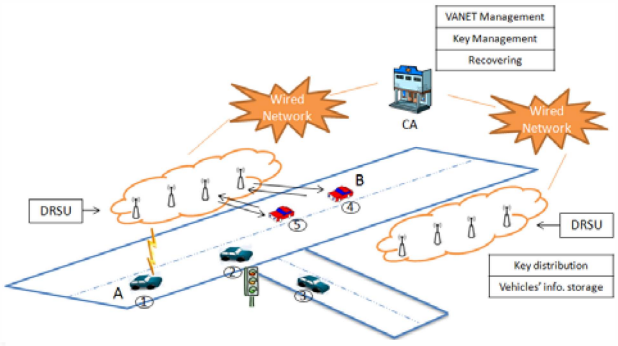


Fig. 2. Architecture of a vehicular ad hoc network with our proposal: Replace one RSU with four distributed RSUs

Certificate Authorities (CA) are called CA and are responsible as administrate department in VANET. They hold all the secrets and have responsibilities to solve disputes. They are used to do VANET management, key management and recovering. The authority has the highest security level. We assume it cannot be compromised.

Distributed Road Side Units (DRSUs) are a set of RSUs. RSUs are agents of the authority and deployed at the road sides. They are used to distribute key and store information from vehicles. However, there is a bottleneck problem of RSU in original VANET. If the RSU is compromised, the message in its coverage can not be transformed successfully, especially as the message is important and has higher safety requirements. The DRSUs group is semi-trusted with the medium security level. An RSU can be a powerful device or a comparatively simple one. The set of RSUs in a DRSUs group is comparatively simple ones.

TABLE I
NOTATION USED IN THE PROPOSAL

CA	Certificate Authorities
RSU	Road side unit
OBU	On Board unit
V_A	Vehicle A
V_B	Vehicle B
M	Message/ Plaintext
Pr_RSU	Private key of RSU
Pub_V_B	Public key of Vehicle B
C_{V_A}	Ciphertext from Vehicle A
$Enc_{Pub\_RSU_1}(M)$	Encryption of message M using the public key of RSU_1
$Dec_{Pr\_RSU_1}(C_{V_A})$	Decryption of ciphertext from V_A using private key of RSU_1
k	Threshold value
n	Number of distributed RSUs

On Board Units (OBUs) are ordinary vehicles on the road that have ability to communicate with each other through radio. After registered information on CA as required, an ordinary vehicle can join VANET and be assigned some initial values. OBUs have the lowest security level.

Because semi-trusted RSU may be compromised [19], our proposal is to develop the ability of anti-RSU compromised by malicious object if any. Several RSUs cooperate together as a DRSUs group, instead of one RSU. Combination of certain RSUs in each DRSUs group can recover the message. That is to say, our DRSUs scheme can tolerate partial compromise of some RSUs. The tolerance ability is based on system requirements. The notations used in our proposal are listed in TABLE I. We assume that the majority of OBUs and RSUs are honest. CA is responsible for the system initialization and is used to distribute secret keys to each system entity. OBUs report to the CA when they send or receive false messages. We also assume that wired network transmits data securely without packet loss.

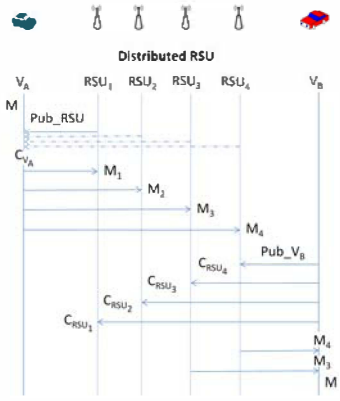


Fig. 3. Time flow chart of Distributed RSU

B. Details to the proposal description

As Vehicle B starts a registration when it is approaching one DRSUs group, the V_B sends its own public key to each RSU in the DRSUs group. If the number of compromised RSUs is not beyond boundary, V_B can recover the message under help of the left normal RSUs.

In Fig. 2, we use four distributed RSUs to replace one RSU. In original VANET structure, CA is used to generate keys. After the one RSU got the key from CA and received the encrypted message $C_{V_A} = E_{Pub\_RSU}(M)$ from V_A, it decrypts the message by its own private key Pr_RSU: $M = D_{Pr\_RSU}(C_{V_A})$. One RSU stores the message M until Vehicle B enters the radio range of the RSU. The RSU will send the message M to V_B by Pub_V_B. V_B decrypts M by its own private key Pr_V_B. In our proposal, CA is also used for key generating and V_B also decrypts message from each of the distributed RSU. The difference is that Pr_RSU is divided into four sub keys. Four distributed RSUs store the four sub keys respectively. If we assume the threshold value k is 2, it means each two of the four distributed RSUs can recover the message M. Taking $node_1$ and $node_2$ as an example, $node_1$ stores the sub key $Sub(Pr\_RSU)_1$ and $node_2$ stores the sub key $Sub(Pr\_RSU)_2$. Both the two nodes can do decryption and obtain sub message $Sub(M)_1 = pad_1 = D_{Sub(Pr\_RSU)_1}(C_{V_A})$ and $Sub(M)_2 = pad_2 = D_{Sub(Pr\_RSU)_2}(C_{V_A})$, respectively. Certainly, the other two nodes also do the same decryption as $node_1$ and $node_2$. As V_B enters radio range of DRSUs, it receives the $pad = pad_1 + pad_2$. V_B obtains the original message M under the help of each two nodes in DRSUs. It is worth mentioning that, V_B receives all the pads from each of the sub-RSUs and does not consider they are malicious or not. If V_B gets more than threshold pads, it can recover the plaintext M. Even if a malicious RSU does not send the pad, V_B will not be effected by the loss because V_B can combine the sent good pads to recover the plaintext M.

The corresponding time flow chart of distributed RSUs is given in Fig. 3. One of the four distributed road side units sends its public key Pub_RSU to V_A firstly. After encrypting the plaintext M by Pub_RSU, V_A sends the ciphertext $C_{V_A} = Enc_{Pub\_RSU}(M)$ to the four units. After receiving C_{V_A}, each RSU decrypts the message M by its own private key. Each private key is section of original private key. Thus, each of the four units can decrypt parts of M, which is denoted by $DeC_{Pr\_RSU_n}(C_{V_A})$. They are $M_1 = DeC_{Pr\_RSU_1}(C_{V_A})$, $M_2 = DeC_{Pr\_RSU_2}(C_{V_A})$, $M_3 = DeC_{Pr\_RSU_3}(C_{V_A})$ and $M_4 = DeC_{Pr\_RSU_4}(C_{V_A})$, respectively. When V_B enters the broadcast range of DRSUs, V_B sends its public key Pub_{V_B} to the four units. Each of the four units encrypts the message that is kept by Pub_{V_B}: $Enc_{Pub\_V_B}(M_n)$. If RSU_1 and RSU_2 have been compromised and V_B wants to receive the important and safety message M from DRSUs, V_B can do this work under the help of RSU_3 and RSU_4. That means V_B only needs to receive $pad_n = Enc_{Pub\_V_B}(M_n)$ from each two of the four units, it can recover the original message.

C. Advantage of our proposal system

In original VANET structure, there is one private key in each RSU and no cooperation between each two RSUs. This paper presents a threshold ElGamal cryptosystem-based key management scheme. One private key is divided into several sub-keys in our scheme. The advantages of our proposal are listed as follows:

- Shamir secret sharing system needs to recover a private key first, and then use the private key for final plaintext. As it is needed to recover private key first in Shamir secret sharing system, we need to set a sink node for this work. It will be a bottleneck of the network. Our assumed network structure can promise the availability of distributed road side units.

- Threshold cryptography achieves the security needs as confidentially and integrity against malicious attackers. It also provides data integrity and availability in a hostile environment and can also employ verification of the correct data sharing. All these can be achieved without revealing the private key. Thus, DRSUs do not need to update key frequently and communicate with CA continually. This is helpful for saving energy in VANET.
- As using Threshold ElGamal system-based key management scheme, we can not get the original plaintext with the help of RSUs whose number is less than the threshold value. Even if some of the semi-trusted road side units are physically captured, attackers need to capture threshold of nodes for monitoring.

In all, we should keep in mind that Threshold ElGamal system has advantages in node capture attack, malicious participant attack, passive attack and collusion attack.

IV. Analysis

Security challenges in VANET are categorized into: authentication versus privacy; availability; low tolerance for errors; mobility; key distribution; incentives and bootstrap [4, 18]. Even though authentication and location detection are the most important security problem which need to be solved, the preserving privacy and anonymization is also the important security problem. The above challenges lead to four types possible secure problems in VANET: RSU units' captured attack, passive vehicular attack, malicious participant attack and collusion with vehicles. Thus, the compromised road side units tolerance should be considered in our proposal firstly.

As the same time as providing the driver with the required privacy and prevent spoofing, our proposal helps to decrease the additional overhead. Thus, our proposal can defend compromised RSU's attack. We do secure challenges analysis via discussion on compromised RSUs tolerance. We analyze performance of networking and wireless communication challenges by analysis of overhead.

We refer the simulation result of practical data about VANET from [7]. The application scenario are as follows: Vehicles might be in the range of gateways for more than two seconds (if range of mote hardware is limited to 50-80 m), as while its speed is up to 70km/h.

A. Packet loss tolerance

Under the Dedicate Short Range Communication (DSRC)[8, 9], the probability of successfully receiving a ciphertext from one Vehicle to one RSU is: P_{V2R}. Correspondingly, The probability of receiving no ciphertext from RSU is: $1-P_{V2R}$. At the same time, the threshold parameters of Threshold ElGamal scheme is: (k,n). Thus, the number of RSUs for recovering ciphertext is : ${}_nC_k$. If there are k' road side units that have successful $P_{V2R} > 0$, the probability P of recovering ciphertext from DRSUs with receiving probability P_{V2R} is:

$$P = \sum_{n \geq k' \geq k} P_{V2R}^{k'}(1 - P_{V2R})^{n-k'} \times {}_nC_{k'}.$$

In this equation, P depends on three variables (k, n, P_{V2R}). Before analyzing the affection of (k,n) to P, the relationship between P_{V2R} and P is discussed under certain assumption of (k,n):

By using a (k,n) threshold scheme with $n = 2k-1$ [3], there is a robust key management scheme. We can recover the original key even when floor value of $n/2$: $\lfloor n/2 \rfloor = k-1$ of the n RSUs are compromised, but attackers can not reconstruct the key even when misbehavior of DRSUs exposes $\lfloor n/2 \rfloor = k-1$ of the remaining k RSUs. Thus, we plot the relevance between P_{V2R} and P in Fig. 4. The probability P can reach higher value even if under the situation with lower P_{V2R}. Higher probability of recovering ciphertext leads to a lower message loss rate. If a certain of road side units are compromised to be unable to maintain regular job, it is still tolerated by our proposal.

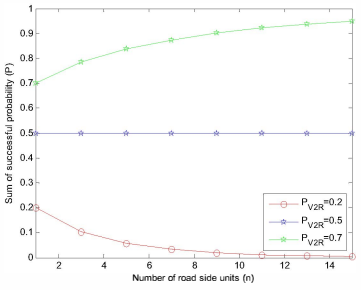


Fig. 4. Successful probability P as $n = 2k-1$, under $P_{V2R} = 0.2$, 0.5 and 0.7, respectively.

1) As P_{V2R} equals 0.5, the success probability P of recovering ciphertext under DRSU maintains to 0.5, even as the number of RSUs is increasing gradually. It shows that P does not keep direct ratio or inverse ratio to P_{V2R} as there is the existed turning point $P_{V2R} = 0.5$.
2) P keeps direct ratio to the road side units n, when P_{V2R} is lower than the extreme value 0.5. It means P reduces and is close to zero as the requirement for the number of RSUs is increased, even though the message loss rate has been reduced in DRSUs work. On the contrary, P also have a little increasing as n increased, under the situation that the value of P_{V2R} is bigger than the extreme value.
3) On the contrary, we should analyze more the relationship between P and P_{V2R} if we want to obtain of behavior of P more exactly. This work is given in Fig. 5.

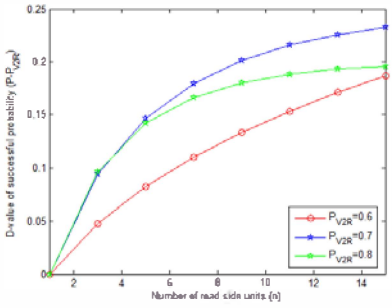


Fig. 5. D-value of successful probability $P(DRSUs) - P(oneRSU)$ as $n = 2k-1$, under $P_{V2R} = 0.6$, 0.7 and 0.8, respectively.

We know from Fig. 4 that the successful probability P increases as the number of road side units n increasing, but not increases linear, when P_{V2R} is greater than 0.5. Another aspect, we can analyze the advantage of our scheme by comparing with the one RSU scheme. Both of two reasons push us to

analyze the difference value between successful probability $P(DRSUs)$ and $P(oneRSU)$, when n equals $2k-1$, under P_{V2R} equals 0.6, 0.7 and 0.8, respectively (Fig. 5):

1) The D-value of successful probability: $P(DRSUs) - P(oneRSU)$ is greater than zero as the number of road side units n increasing.
2) There is another turning point $P_{V2R} = 0.7$ in the area of probability [0.5, 1]. If we do not consider about the overhead and only focus on the successful communication probability, P_{V2R} is appreciated for providing highest P as it is close to 1. However, $P_{V2R} = 0.7$ provides the biggest D-value between DRSUs and one RSU. Then, the D-value becomes smaller as the value of P_{V2R} is far away from the extreme value 0.7.

B. Compromised RSUs tolerance

Both Fig. 4 and Fig. 5 show the impact of P_{V2R} under defined value of (k,n) on *a)* P ; *b)* $P(DRSUs) - P(oneRSU)$, respectively. Recall that P is related to (k,n,P_{V2R}), we discuss the trade off between security and implementing overhead based on the value of (k,n) in Table II. Then, an overall discussion on the affection of different values of (k,n) for success probability P is presented in Fig. 6.

TABLE II
SECURITY VERSUS IMPLEMENTING

		Implementing		
		High	Middle	Low
Security	Weak	$\times$	$n = k$	$k < n \cap k \to n$
	Middle	$n = 2k-1$	$k < n < 2k-1$	/
	Strong	$n > 2k-1$	/	/

After omit one illogical situation and three reduplicate situations, we conclude the trade-off range in the left five situations. $n = k$ means all the RSUs in one DRSUs group need to collaborate together for message recovering. It provides weak security as it allows no compromised of RSUs. $k < n \cap k \to n$ means k is less than but approached to n. The overhead of implementing reduces as the value of k reduces. However, security is still low as k approaches to n. Recall to Section IV.A, there is a robust system when n equals $2k-1$. Of course, the overhead increases while n is increasing. Table II can help researchers to select parameters and set threshold, when considering one system setting up.

We assumed both threshold value k and road side units n are changing from 1 to 15, under the condition that n is greater than k. Thus, there is no value of the probability P, when n is smaller than k (Fig. 6).

1) As the number of n is fixed and greater than k, the value of probability P decreases as the increasing of k. Because there need more pieces of *pad* for M recovering, when the threshold value k is increased.
2) In Fig. 6(a), the successful probability P reduces quickly, as P_{V2R} equals 0.2. That means $P_{V2R} = 0.2$ can not run the system well. In fact, $P_{V2R} = 0.2$ is not expected by original VANET [14].
3) Fig. 6(b), Fig.6(c) and Fig. 6(d) show that lower k leads to higher probability P under higher n, which is helpful for our network system. For example, alteration of k from 2 to 6 can guarantee P to approach 0.99, while n is defined to 15 (Fig. 6(c)).

Even if receivers do miss a small number of heartbeat messages, applications still work. The VANET heartbeat messages used for most safety applications are frequently broadcast (every 100ms) and each message overrides the values from previous messages (i.e., the vehicle's current position and velocity is more important than where it was a few moments ago).

C. Privacy

In the message loss rate analysis part, higher connecting probability is preferred. From the opposite aspect of proving higher connecting probability between vehicles to RSUs and vehicles to vehicles, it is totally understandable that most drivers on the road want their identity to be kept private. Recall to Fig. 3, the safety message M is send to RSUs by V_A. If V_B want to obtain the M, it obtain the k units pad_n from all of the n units in one DRSUs group. Less that k units can not recover the message. From another aspect, V_B communicates with DRSUs and is prevented from communication with V_A. Our proposal provide that there are no disclosures on any private information among the drivers or vehicles. The advantage of our proposal is that it does not create any additional overhead.

D. Processing time

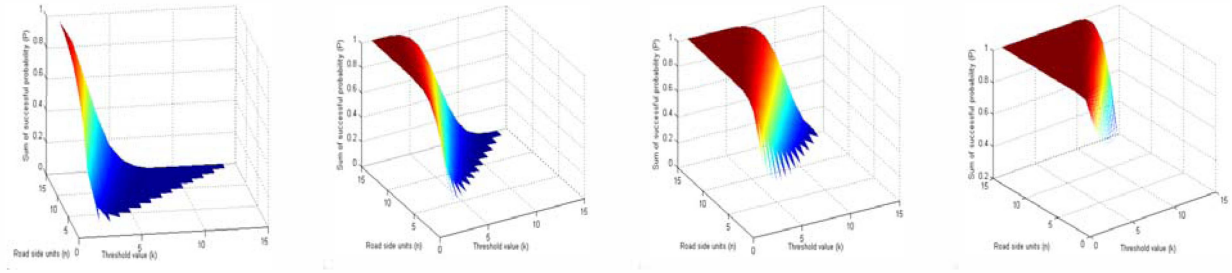
Another challenge for VANET implementing is the range of coverage of the broadcasting a message. In key distribution and key recovery related proposal, a message can be lost in the case that the proposal need to much processing time and out of the coverage range before the whole security proposal has been finished.

Ertaul *et al.*[15] concluded the processing time of RSA and Elliptic Curve-ElGamal Threshold Cryptography implementation for secure data forwarding in MANET, respectively. Because in our proposal, k is fixed to 2 even n is enlarged to 15 can catch up the scenario requirements. RSA Threshold Cryptography (RSA-TC) is much expensive in terms of encryption and decryption timings irrespective of n and t values as compared to Elliptic curve- ElGamal Threshold Cryptography (ECCEG-TC). Thus, we take RSA-TC into consideration of the upper bound value of processing time, even though our proposal comes from ElGamal-based Threshold Cryptography. Ertaul *et al.* evaluated that the total encryption timing, share generation timing for encryption and combination+decryption timing in RSA-TC for (15,15) threshold value and 1024 key sizes are 1100ms, 800ms and 1100ms, respectively, namely, around 3000ms in all. It is mentioning that ECCEG-TC just costs 1900ms for 196 key sizes to provide equivalent security. The total encryption timing increases gradually with increase in n and k. Share generation timing for encryption increases as k value increased. Combination+decryption timing has similar behavior to encryption timings. Combination time is the time required to combine partially encrypted message to retrieve original message. It also increases with n and k.

Recall to the scenario, the vehicular speed is around 70km/h and hardware radio range is around 50-80m. In the hardware radio range, each vehicle has 2500-4000ms for communication. It guarantees that at least 2 nodes can finished their communication within the radio range, even under the upper bound processing time.

E. Overhead

Overhead concludes cryptographic overhead and processing overhead. The cryptographic overhead in our proposal is the series *pad* of private key per message. The processing



(a) $P_{V2R} = 0.2$ (b) $P_{V2R} = 0.5$ (c) $P_{V2R} = 0.7$ (d) $P_{V2R} = 0.9$

Fig. 6. Impact of threshold k and road side units n on successful probability P

overhead is related to processing time and beacons frequency per time unit.

Considering the distinctive features of vehicular communication system: transportation safety and efficiency application, there are two correspondingly requirements for the application scenario. One is for safety application, Emergency Braking notification (EBN). The other one is for efficiency application, Decentralized Floating Car Data (DFCD). EBN and DFCD are two main driving for the VC system deployment. Especially the safety EBN, it is the most challenging among VC enabled applications. Their stringent time constraints and their critical nature can effect the well-being of the vehicle passengers. P_{V2R} is required to be close to 1. When considering the robustness in DFCD application, it is concerned with how effectively data generated by one vehicle can propagate to an area and a platoon. Even if the communication between each vehicle and each RSU is failed sometimes, it is tolerated in DFCD requirement.

V. Conclusion and discussion for future work

In this paper, we propose a Threshold ElGamal-based key management scheme for protection against RSU compromise in VANET. The private key is divided into several pieces and distributed to each RSU in one DRSUs group. The DRSUs group acts the behavior as one RSU. Any combination of threshold pieces in the DRSUs group can be used to decrypt ciphertext, which can help to improve the probability of successful communication and tolerate threshold packet loss between each vehicle and each DRSUs group. The ciphertext which comes from the sender will be decrypted and stored by DRSUs as several pieces of plaintext. This is capable to be away from exposing the privacy of sender to receivers.

Our proposal system guarantees the successful recovery probability especially helpful for EBN scenario and does not influence the efficiency application in DFCD scenario. It is worth mentioning that, both threshold ElGamal cryptosystem and threshold RSA cryptosystem can provide threshold secret sharing without the third trustworthy party. However, VANET should consider to prompt security with low overhead and threshold RSA cryptosystem is unsuitable while threshold ElGamal cryptosystem is suitable for MANETs [15], we select Elliptic Curve-ElGamal threshold cryptosystem for our future work.

Acknowledgment

The first author is supported by the governmental scholarship from China Scholarship Council.

References

[1] A. Studer, E. Shi, F. Bai, A. Perrig, Tracking together efficient authentication, revocation and privacy in VANETs, *7th Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Networks* (SECON 09), 2009.

[2] A. Studer, F. Bai, B. Bellur, A. Perrig, Flexible, Extensible, and Efficient VANET Authentication, *Technical reports*, 2008.

[3] A. Shamir, How to Share a Secret, *Communications of the ACM*, vol. 22, no. 11, pp.612-613, November 1979.

[4] B. Parno, Challenges in Securing Vehicular Networks, *Workshop on hot topics in networks* (HOTNETS-IV), 2005.

[5] C. Sharp, S. Schaffert, A. Woo, N. Sastry, C. Karlof, S. Sastry, D. Culler, Design and implementation of a sensor network system for vehicular tracking and autonomous interception, *Second European Workshop on Wireless Sensor Networks* (EWSN 05), 2005.

[6] D. K. Nilsson, U. E. Larson, E. Jonsson, Low-Cost Key Management for Hierarchical Wireless Vehicle Networks, *IEEE Intelligent Vehicles Symposium*, 2008.

[7] E. Weingartner, Hybrid sensor-vehicular-networks in the context of next-generation networking, http://www3.informatik.uni-wuerzburg.de/euroview/2007/Presentations/Presentation-Weingaertner.pdf.

[8] F. Bai, H. Krishnan, V. Sadekar, G. Holland, T. ElBatt, Towards Characterizing and Classifying Communication-based Automotive Applications from a Wireless Networking Perspective, *IEEE Workshop on Automotive Networking and Applications* (AutoNet 06), 2006.

[9] G. Calandriello, P. Papadimitratis, J. P. Hubaux, A. Lioy, On the Performance of Secure Vehicular Communication Systems, *IEEE transactions on dependable and secure computing*, 2010.

[10] H. Wang, Z.F. Wu, X. Tan, A New Secure Authentication Scheme Based Threshold ECDSA for Wireless Sensor Network, *Security and Management* (SAM), 2006.

[11] H. Lipmaa, Lecture 9: Secret Sharing, Threshold Cryptography, MPC, *T-79.159 Cryptography and Data Security*, Helsinki University of Technology, 2004.

[12] H. Jiang, S. Chen, Y. Yang, Z. Jie, J. Xu, L. Wang, Estimation of Packet Loss Rate at Wireless Link of VANET–RPLE, *6th International Conference on Wireless Communications Networking and Mobile Computing* (WiCOM), 2010

[13] J. M. Bohli, A. Hessler, O. Ugus, D. Westhoff, A secure and resilient WSN roadside Architecture for intelligent transport systems, *ACM conference on Wireless network security* (WiSec), 2008.

[14] K. Sampigethava, L. Huang, M.Li, R.Poovendran, K. Matsuura, K.Sezaki, CARAVAN: Providing Location Privacy for VANET, *3rd international workshop on Vehicular ad hoc networks*, 2006.

[15] L. Ertaul, N. J. Chavan, RSA and Elliptic Curve-ElGamal Threshold Cryptography (ECCEG-TC) Implementations for Secure Data Forwarding in MANETs, *Security and Management*, 2007.

[16] M. Nekovee, Sensor networks on the road: the promise and challenges of vehicular ad hoc networks and grids, *British Telecommunications*, 2005.

[17] S. Sivagurunathan, P. Subathra, V. Mohan and N. Ramaraj, Authentic vehicular Environment Using a Cluster Based Key Management, *European Journal of Scientific Research*, vol. 36, no. 2, September, 2009.

[18] S. Guennouni, A study of Security Requirements for Vehicular Ad hoc Networks (VANET) Communication, *Masters Project, Old Dominion University*, 2009.

[19] Y. Hao, Y. Cheng and K. Ren, Distributed key management with protection against RSU compromise in group signature based VANET, *IEEE GLOBECOM*, 2008.

[20] Y. Desmedt, Y. Frankel, Threshold cryptosystems, *CRYPTO 89*, vol. 435/1990, pp. 307-315, 1990.