Information and Media Technologies 7(4) : 1588–1595 (2012)
reprinted from: Journal of Information Processing 20(4) : 846–853 (2012)

Regular Paper

Elliptic curve ElGamal Threshold-based Key Management Scheme against Compromise of Distributed RSUs for VANETs

Na Ruan[1,a)] Takashi Nishide[1] Yoshiaki Hori[1]

Received: November 30, 2011, Accepted: June 1, 2012

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 an Elliptic curve ElGamal Threshold system-based key management scheme for safeguarding a VANET from RSUs being compromised and their collusion with 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 in terms of two types 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.

Keywords: Elliptic curve ElGamal Threshold Cryptosystem, key management scheme, Distributed RSU, VANET

1. Introduction

1.1 Background

The idea behind VANETs is to have a mechanism nearby vehicles on the road can communicate with each other in order to provide security and comfort for the drivers and passengers [18]. The fundamental vulnerability of VANETs comes from open peer-to-peer architecture. Unlike wired networks that have dedicated routers, the wireless channel in VANETs is public to both legitimate network users and attackers [17]. The attack may range from passive eavesdropping to active impersonation. Since compromising a vehicle or an 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.

1.2 Motivation

RSU is under some situations like mountain roads, where it is difficult to install RSUs. Furthermore, sometimes a mountain road does not have enough density of RSU nodes [1]. If one RSU misbehaves, the vehicles in its scope will be exposed to a dangerous environment. Considering the coverage range of a vehicle which is broadcasting a message in VANETs, we need to make sure that the vehicle 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 VANETs developers, since the vehicle network is random and mobile. And the authentication process should take place without affecting the privacy of the vehicles [18].

1.3 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 cannot be achieved without a regular maintenance of the equipment. Hao et al. [19] proposed a distributed key management scheme with protection against RSU compromise in VANETs using the group signature. The RSU acts as the key distributor in each group. However, misbehavior of a RSU has not been considered under this situation. Sharp et al. [5] combined a sensor network with a VANET for vehicle tracking. The interface problems between sensor network and VANETs should be paid attention to. Studer et al. [1] introduced the basic structure of VANETs and the basic requirement of a key management scheme in VANETs. At the same time, the authors also proposed a key management scheme based on temporary anonymous certification for combining efficient authentication, revocation and privacy in VANETs. It maintains almost the same overhead as the IEEE 1609.2 standard for VANETs security.

1.4 Challenging Issues

As a brief review of related works [6], [10], [13], [16], we find many schemes requiring both the vehicles and RSU to store a large number of pseudonyms and certificates, where it is inconvenient to implement a revocation scheme to abrogate the malicious

[1] Department of Informatics, Kyushu University, Fukuoka 819–0395, Japan
[a)] ruannana@gmail.com

Information and Media Technologies 7(4) : 1588–1595 (2012)
reprinted from: Journal of Information Processing 20(4) : 846–853 (2012)

vehicles and RSU. Moreover, lots of previous assumptions of implementing security applications on a VANET based on a ready vehicle cannot be achieved. The protection against compromised RSU is general purpose in VANETs.

The above reasons motivate us to propose the Threshold ElGamal system [11], [20] based key management scheme for distributed RSUs (DRSUs) in VANETs. Elliptic curve-based ElGamal Threshold system can provide quick processing time and shorter key size for equivalent security (For example, Elliptic curve ElGamal threshold cryptosystem needs 980 ms with a key of 163 bits in size while RSA-Threshold cryptosystem needs 3,000 ms with a key of 1,024 bits in size).

1.5 Organization

This paper is organized as follows: Section 2 describes basic definitions and notations of the Elliptic curve ElGamal threshold cryptosystem (ECCEG-TC). Section 3 provides our proposed model. Section 4 presents the analysis of security and overhead. Finally, we compare our proposal with other schemes in Section 5 and draw conclusions in Section 6.

2. Preliminaries

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

2.1 Secret Sharing Based on Polynomials

Before introducing the idea of secret sharing based on polynomials [3], the definition of Lagrange interpolation should be presented. Lagrange interpolation is used to reconstruct the secret key. In Lagrange interpolation, a $k-1$ degree polynomial $f(x)$ and a set of k points: $(x_1, y_1), (x_2, y_2), ..., (x_k, y_k)$ should be given in advance, where x_i are all distinct and y_i is equal to $f(x_i)$. By considering the Lagrange coefficients $\lambda_j(x)[x_1, x_2, ..., x_k] \doteq \prod_{i=1, i\neq j}^{k} \frac{x-x_i}{x_j-x_i}$, we know that $f(x)$ equals $\sum_{j=1}^{k} y_j \lambda_j(x)[x_1, x_2, ..., x_k]$. Correspondingly, the secret key $f(0)$ equals $\sum_{j=1}^{k} y_j \prod_{i=1, i\neq j}^{k} \frac{-x_i}{x_i-x_j}$.

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

After generating a polynomial for sharing the private key, one piece of the private key is distributed to each participant. To recover the plaintext based on some pieces of a key by k participants, we select the Threshold ElGamal system for resolving this problem. ECCEG-TC is its efficient version.

2.2 Threshold ElGamal System

We give a review of the Threshold ElGamal system.

(1) Key generation and message encryption are presented as follows:
- $p = 2q + 1$, where p, q are primes.
- Select x from $\mathbb{Z}_q$ randomly, where $y \doteq g^x$ **mod** p, g is a generator of the finite multiplicative group QR_p and its order is q.
- Select $a_1, a_2, ..., a_{k-1}$ from $\mathbb{Z}_q$ randomly, where $a_0 \doteq x$.
- $f(i) = a_0 + a_1 i + a_2 i^2 + ... + a_{k-1} i^{k-1}$ **mod** q.
- $PK \doteq (p, g, y)$, $SK_i \doteq f(i)$ for all i.

(2) In $Enc_y(M)$ part, select r from $\mathbb{Z}_q$ randomly and compute $(c_0, c_1) \doteq (g^r, y^r \cdot M)$. M is the plaintext which is required to be protected.

(3) Compared with the reconstruction of a secret using the Shamir secret sharing system [11], **Fig. 1** presents the decryption under the Threshold ElGamal system by $Dec_x(c_0, c_1)$:
- Unlike the Shamir secret sharing system which needs to collect all the fragments of ciphertext before decryption, each share-holder i using the Threshold ElGamal system creates a decryption fragment: $\mathbf{pad}_i = c_0^{SK_i}$.
- Once the k fragments have been collected, reconstruct the pad: $\mathbf{pad} \doteq \prod_{i=1}^{k} (\mathbf{pad}_i)^{\lambda_i} = \prod_{i=1}^{k} (c_0^{SK_i})^{\lambda_i}$.
- $M = c_1 / \mathbf{pad}$.
- While: $x = \sum_{i=1}^{k} SK_i \lambda_i$ and $c_0^x = c_0^{\sum_{i=1}^{k} SK_i \lambda_i} = \prod_{i=1}^{k} (c_0^{SK_i})^{\lambda_i}$.

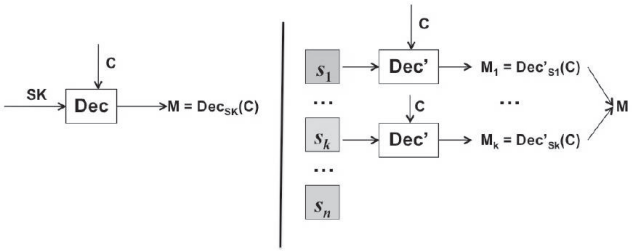


Fig. 1 Threshold ElGamal cryptosystem.

2.3 Elliptic Curve ElGamal Threshold Cryptosystem

Compared with the non-elliptic curve version, there is a general procedure for changing a classical system based on discrete logarithms into one using elliptic curves. It changes modular multiplication to the addition of points on an elliptic curve or changes modular exponentiation to multiplying a point on an elliptic curve.

Suppose that the Elliptic Curve Cryptosystem (ECC) has a point g on an elliptic curve E_p, where the order of g is q, and p is a large prime number.

(1) Key generation and message encryption are presented as follows:
- Calculate $y \doteq ag$, where g is the generator of the points on the elliptic curve group E_p, a is selected from $\mathbb{Z}_q$ randomly and is kept secret.
- Select $a_1, a_2, ..., a_{k-1}$ from $\mathbb{Z}_q$ randomly, where $a_0 \doteq a$.
- $f(i) = a + a_1 i + a_2 i^2 + ... + a_{k-1} i^{k-1}$ is constructed by the dealer of the private key.
- $PK \doteq (E, g, y)$, $SK_i \doteq f(i)$ **mod** q for all i.

(2) For encrypting $Enc_y(M)$, select r from $\mathbb{Z}_q$ randomly while $C_A = (rg, yr + M)$. M is the plaintext which is required to be protected.

(3) For decrypting $Dec_x(M)$, different participants use their own secret key SK_i to compute C_i, where $C_i = (i, rSK_i g, ry + M)$. Then compute $b_i rSK_i g$, where $b_i = \prod_{i=1, i\neq j}^{k} \frac{-x_i}{x_i-x_j}$ **mod** q.

(4) After that, $\sum_{j=1}^{k} b_j rSK_j g$ is calculated. Its sum equals ry.

Information and Media Technologies 7(4) : 1588–1595 (2012)
reprinted from: Journal of Information Processing 20(4) : 846–853 (2012)

(5) Finally, $(M + ry) - ry = M$, the original message M.

3. Our proposal

3.1 Description of the whole scenario system

The architecture of a vehicular ad hoc network with our DRSUs-proposal consists of three entities. Compared with the original VANETs [14], the three entities 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**.

Certificate Authorities (CA) are called CA and are responsible for the Administrating Department in VANETs. They hold all the secrets and have the responsibility of solving disputes. They are used to do VANETs 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 keys and store information from vehicles. However, there is a bottleneck problem of a RSU in the original VANETs. If the RSU is compromised, the message in its coverage cannot be transformed successfully, especially if the message is important and has higher security requirements. The DRSUs group is semi-trusted with a 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.

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

Because a semi-trusted RSU may be compromised [19], our proposal is to develop the ability of tolerating the compromising of RSU. Several RSUs cooperate as a DRSUs group, instead of working individually. Combination of certain RSUs in each DRSUs group can recover the message. That is to say, our DRSUs scheme can tolerate partial compromising of RSUs. The tolerance ability is based on system requirements. The notations used in our proposal are listed in **Table 1**. 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 a wired network transmits data securely without packet loss.

There are two necessary requirements for the application scenario. One is for the security application, Emergency Braking notification (EBN). The other one is for the efficiency application, Decentralized Floating Car Data (DFCD).

Emergency Braking Notification (EBN): While a vehicle brakes hard, the Emergency Electronic Braking notification application [21] sends a message to other vehicles following behind. This application will help the driver of the following vehicles by giving an early notification that the lead vehicle is braking hard even when the driver's visibility is limited. This information could be integrated into an adaptive cruise control system.

Decentralized Floating Car Data (DFCD): This application [21] warns the driver when he intends to make a lane change and his blind spot is occupied by another vehicle. The application receives periodic updates of the positions, headings and speeds of surrounding vehicles via V2V communication. In case of a positive detection, a warning is provided to the driver.

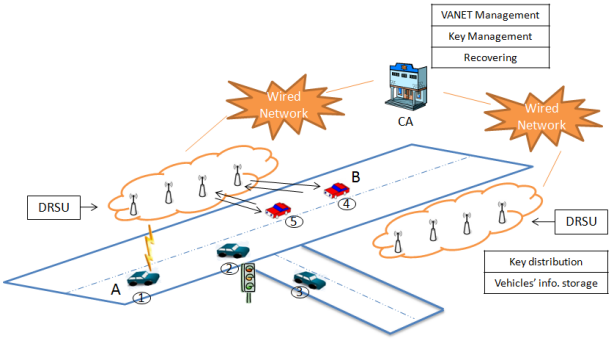


Fig. 2 Architecture of a vehicular ad hoc network with our proposal: Replace one RSU with four distributed RSUs.

Table 1 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

3.2 Details of the Proposal Description

Vehicle B starts registration when it approaches the group of DRSUs so that V_B sends its own public key to each RSU in the DRSUs group. If the number of compromised RSUs is not beyond a pre-specified threshold, V_B can recover the message using the remaining normal RSUs.

In Fig. 2, we use four distributed RSUs to replace one RSU. In the original VANETs structure, CA is used to generate keys. After 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: $M = D_{Pr\_RSU}(C_{V_A})$. This RSU stores the message M until Vehicle B enters its radio range. It 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 generation and V_B also decrypts the message from each of the distributed RSUs. The difference is that Pr_RSU is divided into four sub keys. Four distributed RSUs store the four sub keys respectively.

Taking RSU_1 and RSU_2 as an example, RSU_1 stores the sub key $Sub(Pr\_RSU)_1$ and RSU_2 stores the sub key $Sub(Pr\_RSU)_2$. Both nodes can decrypt and obtain the 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 RSU_1 and RSU_2. If we

Information and Media Technologies 7(4) : 1588–1595 (2012)
reprinted from: Journal of Information Processing 20(4) : 846–853 (2012)

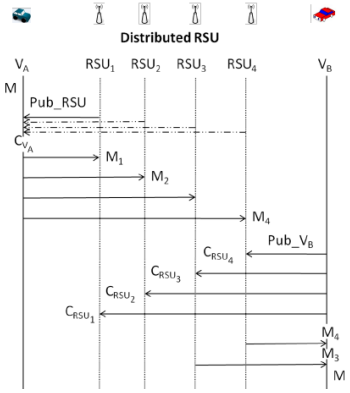


Fig. 3 Time flow chart of distributed RSU.

assume the threshold value k is 2, any two of the four distributed RSUs can recover the message M. As V_B enters the radio range of DRSUs, it receives the $pad = pad_1 + pad_2$. V_B obtains the original message M using the help of two nodes in the DRSUs. It is worth mentioning that, V_B receives all the pads from any of the sub-RSUs and does not consider they are malicious or not. If V_B gets more pads than the threshold, it can recover the plaintext M. Even if a malicious RSU does not send the pad, V_B will not be affected because V_B can combine the other correctly received good pads to recover the plaintext M.

The corresponding time flow chart of distributed RSUs is given in **Fig. 3**. First, one of the four distributed road side units sends its public key Pub_RSU to V_A. 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 using its own private key. Each private key is a fragment of the original private key. Thus, each of the four units can decrypt part 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 security message M from the DRSUs, V_B can do so using 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 any two of the four units and then recover the original message.

3.3 Advantage of Our Proposed System

In the original VANETs structure, there is one private key in each RSU and no cooperation between each of the two RSUs. This paper presents an ECC-TC 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 the final plaintext. As it is needed to recover the private key in advance, we need to designate a sink node for this work. It will be the bottleneck of the network. Our assumed network structure can guarantee the availability of the distributed road side units.
- Threshold cryptography achieves the security needs of confidentially and integrity against malicious attackers. It provides data integrity and availability in a hostile environment and can employ verification of the correct data sharing. All these can be achieved without revealing the private key. Thus, the DRSUs do not need to update their keys frequently nor communicate with the CA continually. This is helpful for saving energy in VANETs.
- As for using the Threshold ElGamal system-based key management scheme, we cannot get the original plaintext with the help of the RSUs when the number available is less than the threshold value. Even if some of the semi-trusted road side units are physically captured, attackers need to capture enough monitoring nodes to surpass the threshold.

In all, we should keep in mind that the Threshold ElGamal system has advantages in node capture attack, malicious participant attack, passive attack and collusion attack. Besides these, its ECC version can provide equivalent security with shorter processing time and smaller key size.

4. Analysis

Security challenges in VANETs 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 needs to be solved, privacy preservation and anonymization are also the important security problems. The above challenges lead to four types of possible security-related problems in VANETs: RSU units captured attack, passive vehicular attack, malicious participant attack and collusion with vehicles. Thus, the compromised RSUs tolerance should be considered in our proposal.

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

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

Our experiment has been executed on a Toshiba Dynabook SS with a Core2, 1.40 GHz CPU and 2,048 MB RAM memory. We implemented our experiment using the MATLAB. Each group of the experimental data has been calculated to an accuracy of within one minute.

4.1 Packet Loss Tolerance

Under the assumption of Dedicate Short Range Communication (DSRC) [8], [9], the probability of successfully transmitting ciphertext from one Vehicle to one RSU is: P_{V2R}. Correspondingly, the probability of not receiving the ciphertext from RSU is: $1 - P_{V2R}$. At the same time, the threshold parameters of the

Information and Media Technologies 7(4) : 1588–1595 (2012)
reprinted from: Journal of Information Processing 20(4) : 846–853 (2012)

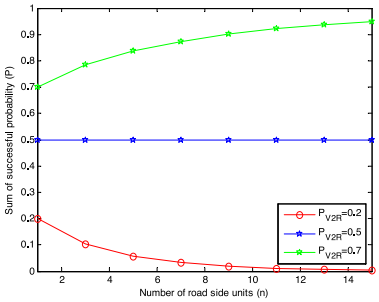


Fig. 4 Successful probability P as $n = 2k - 1$, under $P_{V2R} = 0.2$, 0.5 and 0.7, respectively.

Threshold ElGamal scheme is: (k, n). Thus, the number of RSUs for recovering the 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 effect of (k, n) on P, the relationship between P_{V2R} and P is discussed under the following 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 $\lfloor n/2 \rfloor = k - 1$ of the n RSUs are compromised, but attackers cannot 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 a higher value even when P_{V2R} is lower. Higher probability of recovering ciphertext leads to a lower message loss rate. If a certain number of road side units are compromised such that they cannot maintain their availability, it is still tolerated by our proposal.

(1) As P_{V2R} equals 0.5, the successful probability P of recovering ciphertext under DRSU remains to be 0.5, even if the number of RSUs is increasing gradually. It shows that P does not keep the direct ratio or inverse ratio to P_{V2R} as there is the existing turning point $P_{V2R} = 0.5$.

(2) P keeps the direct ratio to the road side units n, when P_{V2R} is lower than the extreme value 0.5. It means P drops and is close to zero as the requirement for the number of RSUs is increased, even though the message loss rate has been reduced. On the contrary, P also increases slightly as n increases, under the situation that the value of P_{V2R} is bigger than the extreme value.

(3) On the contrary, we should analyze deeply the relationship between P and P_{V2R} if we want to obtain the behaviors of P more exactly. This work is given in **Fig. 5**.

We know from Fig. 4 that the successful probability P increases as the number of road side units n increases. However the increase is not linear, when P_{V2R} is greater than 0.5. Moreover, we can analyze the advantage of our scheme by comparing with the case of one RSU scheme. Both reasons force us to analyze the discrepancy (D-value) between the successful probabilities $P(DRSUs)$ 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 the successful probability: $P(DRSUs) - P(oneRSU)$ is greater than zero as the number of road side units n increases.

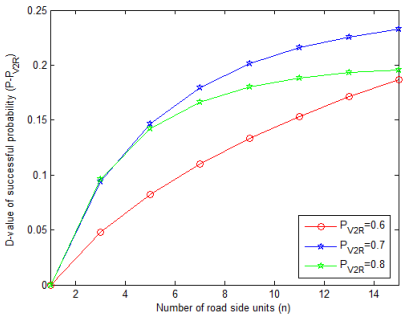


Fig. 5 D-value of successful probability $P(DRSUs) - P(oneRSU)$ as $n = 2k - 1$, under $P_{V2R} = 0.6$, 0.7 and 0.8, respectively.

Table 2 Security versus implementation.

		Implementation		
		High	Middle	Low
Security	Weak	×	$n = k$	$k < n \cap k \rightarrow n$
	Middle	$n = 2k - 1$	$k < n < 2k - 1$	⁄
	Strong	$n > 2k - 1$	⁄	⁄

(2) There is another turning point $P_{V2R} = 0.7$ in the area of probability [0.5, 1]. If we do not consider the overhead and only focus on the successful communication probability, P_{V2R} can provide the highest P as it is very 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.

4.2 Compromised RSUs tolerance

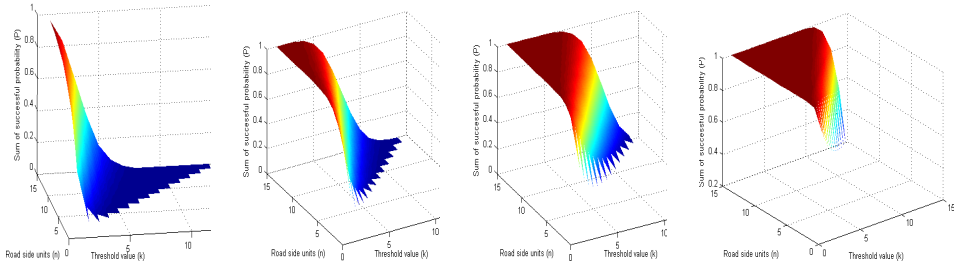
Both Fig. 4 and Fig. 5 show the impact of P_{V2R} under the defined value of (k, n) on 1) P; 2) $P(DRSUs) - P(oneRSU)$, respectively. Recall that P is related to (k, n, P_{V2R}). We discuss the trade-off between security level and implementation overhead based on the values of (k, n) in **Table 2**. Then, an overall discussion on the effect of the different values of (k, n) for successful probability P is presented in **Fig. 6**.

After omitting one illogical situation and three duplicated situations, we conclude the trade-off range in the remaining five situations. When $n = k$, all the RSUs in one DRSUs group need to collaborate together for message recovery. It provides weak security as it allows no compromise of RSUs. When $k < n \cap k \rightarrow n$ means k is less than but approached n. The overhead of implementation reduces as the value of k reduces. However, the security level is still low as k approaches n. Recall from Section 4.1 that there is a robust system when n equals $2k - 1$. Surely, the overhead increases while n is increasing. Table 2 can help researchers to select parameters and set the threshold, when setting up one system.

The application scenario has defined the speed of vehicles and the range of mote hardware, and we assumed both threshold value k and road side units n ranges 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) If the fixed n is greater than k, the value of probability P decreases as k increases. It is because we need more pieces of *pad* for recovering M when the threshold value k is in-

Information and Media Technologies 7(4) : 1588–1595 (2012)
reprinted from: Journal of Information Processing 20(4) : 846–853 (2012)



(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.

creased.

(2) In Fig. 6 (a), the successful probability P reduces quickly, as P_{V2R} equals 0.2. That means $P_{V2R} = 0.2$ cannot run the system well. In fact, $P_{V2R} = 0.2$ is not expected by the original VANETs [14].

(3) Figure 6 (b), Fig. 6 (c) and Fig. 6 (d) show that a lower k leads to higher probability P under higher n, which is helpful for our network system. For example, P approximates to 0.99 when k varies from 2 to 6, while n is set to 15 (Fig. 6 (c)).

Even if receivers miss a small number of status messages, applications still continue to function. The VANETs heartbeat messages used for most security applications are frequently broadcasted (i.e., every 100 ms) and each message overrides the values of previous messages (i.e., the vehicle's current position and velocity are more important than where it was a few moments ago).

4.3 Privacy

In the analysis part of message loss rate, 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 private. Recall from Fig. 3, the security message M is sent to RSUs by V_A. If V_B wants to know M, it obtains the k units pad_i from all of the n units in one DRSUs group. Less than k units cannot recover the message. From another aspect, V_B communicates with DRSUs and is prevented from communicating with V_A.

Our proposal provides that there are no disclosures of any private information among the drivers or vehicles. Existing schemes use additional digital signature or encryption twice for enhancing privacy. Compared to them, the advantage of our proposal is that no additional overhead is necessary.

4.4 Processing Time

Another challenge for VANETs implementation is the range of coverage of message broadcasting. In the key distribution and key recovery related proposal, a message may be lost when too much processing time is required and vehicles become out of the coverage range before the whole security proposal is finished.

We use ECCEG-TC for the key management in our VANET system. We define the necessary requirements of the network scenario, the specific sender and receiver. Our analysis considers both the security implementation and the communication performance. Ertaul et al. [15] summarized the processing time of RSA and Elliptic Curve-ElGamal Threshold Cryptography implementations for secure data forwarding in MANETs. They provide certain implementation parameters of ECCEG Threshold cryptography. For the processing time, we refer to Ertaul et al.'s work.

Table 3 Processing time of RSA-TC and ECCEG-TC for equivalent security.

For threshold (15, 15)		Upper bound RSA-TC	Lower bound ECCEG-TC
key sizes		1024	163
Timing	Encryption	1,100 ms	600 ms
	Combination	800 ms	80 ms
	Decryption	1,100 ms	300 ms
Timing in all		3,000 ms	980 ms

Ertaul et al. estimated that the (1) total encryption time, (2) share generation time for encryption and (3) combination+decryption time in RSA-TC with (15, 15) threshold value and the key of 1,024 bits in size are (1) 1,100 ms, (2) 800 ms and (3) 1,100 ms, respectively, namely, around 3,000 ms in total. It is worth mentioning that ECCEG-TC only needs 980 ms with a key of 163 bits in size to provide equivalent security. We summarize the processing time in **Table 3**. The total encryption timing increases gradually with the increase of n and k. Share generation timing for encryption increases as the value of k increases. Combination+decryption performs similarly to encryption in terms of time. Combination time is the time required to combine partially encrypted message to recover the original message. It increases with n and k. In our proposal, k is fixed to 2 and even if n is increased to 15, we can meet the scenario requirements. RSA Threshold Cryptography (RSA-TC) is more expensive in terms of encryption and decryption times irrespective of the values n and t as compared to Elliptic curve-ElGamal Threshold Cryptography (ECCEG-TC). Thus, we can consider the processing time of RSA-TC as the upper bound and the processing time of ECCEG-TC as the lower bound.

Recalling the scenario, the vehicular speed is around 70 km/h and hardware radio range is around 50–80 m. In the hardware radio range, each vehicle has 2,500–4,000 ms for communication. It guarantees that around three nodes can finish their communication within the radio range under the required processing time of ECCEG-TC.

4.5 Overhead

Overhead includes cryptographic overhead and processing overhead. The cryptographic overhead in our proposal is the series of fragments of private key per message. The processing overhead is related to processing time and beacons frequency per

Information and Media Technologies 7(4) : 1588–1595 (2012)
reprinted from: Journal of Information Processing 20(4) : 846–853 (2012)

Table 4 The advantages of our scheme.

	malicious actions of RSU (Advantage of GS-based Scheme)				RSU stopped completely
	Appropriating ID	Without acknowledgement	Colluding with vehicles	Deny of reporting	
GS-based Scheme	Yes	Yes	Yes	Yes	No
Our Scheme	Avoid the four aspects of attacks: Node capture attack; Malicious participant attack;Passive attack; Collusion attack.				Yes
Other advantages of our Scheme	1. Provide a lower overhead during system processing. 2. Provide a good tolerance on message loss rate.				

time unit.

We consider the distinctive features of a vehicular communication system: transportation security and efficiency application. As mentioned earlier, EBN and DFCD are two main methods driving VC system deployment. Especially, the security of EBN is the biggest challenge among VC enabled applications. Their stringent time constraints and their critical nature can affect 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. Even if the communication between each vehicle and each RSU fails sometimes, it is tolerated under DFCD requirements. The extreme situation in DFCD with our scheme is: $n = k = 1$.

5. Comparison with Other Schemes

Sampigethava et al. [14] propose the semi-trusted RSU and gave a figure which concludes the semi-trusted system (RSU, location server and other sources). This paper is used for providing location privacy for VANET. It does not focus on semi-trusted RSUs. In Rabieh et al. [22], RSU is also semi-trusted. Since it is semi-trusted, it can only be used to forward the envelope to the CA. Ferrer et al. [23] give an overview on the safety and privacy in VC. Even though all the entities were semi-trusted, it does not present the RSU-related infrastructure. Hao et al. [19] developed security protocols for the distributed key management, which are capable of identifying the compromised RSUs and their collusion with the malicious vehicles if any.

Hao et al.'s protocol frame for communication is based on Group Signature. The design adopts a short group signature with a group private generator and a tracing key. RSU holds the group private key generator. The proposed protocol is used to detect whether vehicles are using their group private keys. This proposal can avoid the system from four attacks: appropriating the ID of other vehicles; Receiving key without acknowledgment; Colluding with vehicles; Deny of reporting. However, the proposal shows obvious disadvantages: They only considered the situation where RSUs behave maliciously. They do not consider the situation where RSUs do not work totally. Also, after a 9 ms verification delay for the group signature, the average message loss ratio was 45%. In particular, the message loss ratio reaches as high as 68% when the traffic load was 150 vehicles. Both the results show that the message loss rate increases easily under the Hao et al. scheme. Moreover, the Hao et al. scheme costs a great deal of overhead. And the mobility of the VANET prevents the network from making a static group.

As mentioned earlier, our scheme cannot only avoid the four aspects of attacks: node capture attack, malicious participant attack, passive attack and collusion attack, but also provide a lower overhead during system processing and a good tolerance on message loss rate. Our scheme can tolerate that certain RSUs do not work completely. The scheme of Hao et al. has no such advantage. The results of our comparison are summarized in **Table 4**.

6. Conclusions

In this paper, we proposed an Elliptic curve ElGamal Threshold based key management scheme as protection against RSU compromised in a VANET.

Because of the use of the ElGamal Threshold based key management scheme, the private key is divided into several pieces and distributed to each RSU in one DRSUs group. The DRSUs group acts as one RSU. Any combination of threshold pieces in the DRSUs group can be used to decrypt the 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 kind of scheme prevents the sender from exposing the privacy to receivers. Our proposed system guarantees the successful recovery probability, which is helpful for an EBN scenario and does not influence the efficiency application in a DFCD scenario.

ElGamal threshold cryptosystem is suitable for MANETs, while the RSA threshold cryptosystem is not [15]. It is worth mentioning that both the Elliptic curve ElGamal threshold cryptosystem and the RSA threshold cryptosystem can provide threshold secret sharing without a trusted third party. However, VANETs should consider security with low overhead and ECCEG-TC provides the lower bound of processing time. Thus, our work propose an ECCEG-TC based key management scheme against the compromise of distributed RSUs for VANETs.

References

[1] Studer, A., Shi, E., Bai, F. and Perrig, A.: 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] Studer, A., Bai, F., Bellur, B. and Perrig, A.: Flexible, Extensible, and Efficient VANET Authentication, Technical Reports (2008).
[3] Shamir, A.: How to Share a Secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (Nov. 1979).
[4] Parno, B.: Challenges in Securing Vehicular Networks, *Workshop on Hot Topics in Networks* (*HOTNETS-IV*) (2005).
[5] Sharp, C., Schaffert, S., Woo, A., Sastry, N., Karlof, C., Sastry, S. and Culler, D.: Design and implementation of a sensor network system for vehicular tracking and autonomous interception, *2nd European Workshop on Wireless Sensor Networks* (*EWSN 05*) (2005).
[6] Nilsson, D.K., Larson, U.E. and Jonsson, E.: Low-Cost Key Management for Hierarchical Wireless Vehicle Networks, *IEEE Intelligent Vehicles Symposium* (2008).
[7] Weingartner, E.: Hybrid sensor-vehicular-networks in the context of next-generation networking, available from

Information and Media Technologies 7(4) : 1588–1595 (2012)
reprinted from: Journal of Information Processing 20(4) : 846–853 (2012)

⟨http://www3.informatik.uni-wuerzburg.de/euroview/2007/Presentations/Presentation-Weingaertner.pdf⟩.

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

[9] Calandriello, G., Papadimitratis, P., Hubaux, J.P. and Lioy, A.: On the Performance of Secure Vehicular Communication Systems, *IEEE Trans. on Dependable and Secure Computing* (2010).

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

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

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

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

[14] Sampigethava, K., Huang, L., Li, M., Poovendran, R., Matsuura, K. and Sezaki, K.: CARAVAN: Providing Location Privacy for VANET, *3rd International Workshop on Vehicular Ad Hoc Networks* (2006).

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

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

[17] Sivagurunathan, S., Subathra, P., Mohan, V. and Ramaraj, N.: Authentic vehicular Environment Using a Cluster Based Key Management, *European Journal of Scientific Research*, Vol.36, No.2 (Sep. 2009).

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

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

[20] Desmedt, Y. and Frankel, Y.: Threshold cryptosystems, *CRYPTO 89*, Vol.435/1990, pp.307–315 (1990).

[21] Aboobaker, A.K.K.: Performance Analysis of Authentication Protocols in Vehicular Ad Hoc Networks (VANET), Technical Report, University of London (Mar. 2010).

[22] Rabieh, K.M. and Azer, M.A.: Combating Sybil Attacks in Vehicular Ad Hoc Networks, *The 3rd International Conference on Wireless and Mobile Networks* (*WiMo-2011*) (June 2011).

[23] Ferrer, J.D. and Wu, Q.: Safety and Privacy in Vehicular Communications, *Privacy in Location-Based Applications, Lecture Notes in Computer Science*, Vol.5599, p.173. ISBN 978-3-642-03510-4, Springer Berlin Heidelberg (2009).

Na Ruan was born in AnQing, AnHui, China on 1985. She is currently a Ph.D. candidate at Kyushu University, Japan. She received her M.S. and B.S. degrees in communication from China University of Mining and Technology, China, in 2010 and 2007, respectively. Her research interests include security protocols, wireless sensor network and vehicular ad hoc network.

Takashi Nishide received a B.S. degree from the University of Tokyo in 1997, an M.S. degree from the University of Southern California in 2003, and a Dr.E. degree from University of Electro-Communications in 2008. From 1997 to 2009, he had worked at Hitachi Software Engineering Co., Ltd. developing security products. Since 2009, he has been an Assistant Professor in Kyushu University. His primary research is in the areas of cryptography and information security.

Yoshiaki Hori received his B.E., M.E, and D.E. degrees on Computer Engineering from Kyushu Institute of Technology, Iizuka, Japan in 1992, 1994, and 2002 respectively. From 1994 to 2003, he was a Research Associate at the Common Technical Courses, Kyushu Institute of Design. From 2003 to 2004, he was a Research Associate at the Department of Art and Information Design, Kyushu University. From 2004, he was an Associate Professor at the Department of Computer Science and Communication Engineering, Kyushu University. Since 2009, he has been an Associate Professor of the Department of Informatics, Kyushu University. His research interests include network security, network architecture, and performance evaluation of network protocols on various networks. He is a member of IEEE, ACM, and IPSJ.