An Improved Privacy-Preserving Navigation Protocol in VANETs

Wonjun Cho, Youngho Park, Chul Sur, and Kyung Hyune Rhee*
Department of IT Convergence and Application Engineering, Pukyong National University
599-1, Daeyeon3-Dong, Nam-Gu, Busan 608-737, Republic of Korea
{fafata, pyhoya, kahlil, khrhee}@pknu.ac.kr

Abstract

Recent advance of vehicular technology offers opportunities for developing new navigation systems to overcome the problems of popular global positioning system (GPS) based navigation systems. In order to integrate vehicular technology into conventional GPS-based navigation systems securely, a secure and privacy-preserving navigation protocol that utilizes the real-time road information collected by a vehicular ad hoc network (VANET) was proposed in recent year. In this paper, we address the limitations of the previous work and propose an improved secure and privacy-preserving navigation protocol in VANETs. In particular, we focus on eliminating the system master secret distribution and update procedures for anonymous credential acquisition, and the need of an additional tamper-proof device to use and store the system master key. Moreover, the proposed protocol does not need conventional public key certificates, which put a heavy burden of pubic key management over a VANET. In order to achieve these goals, we consider the concept of a two person multisignature and identity-based cryptographic schemes as our building blocks.

Keywords: vehicular ad hoc networks, secure navigation protocol, privacy preservation

1 Introduction

It is common experience for a driver to find a route of a certain destination in an unknown region or to predict the fastest route in a congested area. Recently, global positioning system (GPS) technology has been adopted for navigation purposes and lots of vehicles have started to install GPS-based navigation systems to select better driving paths in terms of the physically shortest path or the vehicular low-density traffic path [1]. However, route finding procedure of these systems is based on a local map data. If the local map information is out of date, or if an event (e.g., traffic incident or disaster) occurs in real time, the GPS-based navigation system may guide to erroneous route.

In the meantime, vehicular technology has come a long way in the last decade, especially in safety driving and efficiency driving. Also, today's vehicles are become a smart car with assistance from wireless communication technology. It is generally referred to as vehicular ad hoc networks (VANETs). In VANET environments, vehicles are equipped with on-board units (OBUs) to perform mobile computing and communicate with road side units (RSUs) installed along the roads. The vehicles and RSUs can communicate using the dedicated short range communications (DSRC) standardized by the IEEE [2]. The common VANET models fall into two categories: 1) vehicle-to-vehicle (V2V) communications and 2) vehicle-to-infrastructure (V2I) communications. Vehicles are able to broadcast safety messages to other nearby vehicles (via V2V communications) and to RSU (via V2I communications) regularly to enable useful applications such as cooperative driving, probe vehicle data, and collect real-time road conditions [3, 4, 5]. Especially, Lu *et al* [4] presented a VANET-based navigation protocol that tracks available parking spaces and guides drivers to the available parking spaces. In their protocol, three RSUs provide the navigation function for a vehicle to find a vacant parking space in a parking lot. Chang *et al*

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 4, number: 4, pp. 80-92
*Corresponding author: Tel: +82-51-629-6247, Fax: +82-51-626-4887, Web: http://www.lisia21.net/

[3] proposed distributed wireless sensor networks based navigation approach, in which the gathering of real-time traffic information from distributed sensor nodes (vehicle) is performed through the WiMAX interface. Their approach predicts the optimal path based on real-time traffic and the minimal travel cost. Therefore, integrating vehicular technology into navigation systems becomes a very timely topic to overcome the problems of conventional GPS-based navigation systems.

Although many possible advantages of VANETs are known in the literature, several security concerns have to be addressed before all other implementation aspects of VANETs. For the last few years, many research works have concentrated on the design of secure VANETs to address potential security and privacy issues [6, 7, 8, 9]. Specifically, in a VANET-based navigation system, a driver associated with the vehicle must be authenticated to ensure he is a valid subscriber of the system. So, communication messages in the system should be authenticated to guard against the impersonation and message forgery attacks. On the other hand, privacy preservation must be achieved in the sense that the user-related private information, including driver's name, license plate, speed, position, and traveling routes as well as their relationships, has to be protected. Meanwhile, the authorities should be able to reveal the identities of message senders in case of billing purpose for navigation services or tracing the compromised subscriber who may launch a denial-of-service attack to threaten the system.

Recently, Chim *et al* [10] proposed a VANET-based secure and privacy-preserving navigation protocol (VSPN) which makes use of anonymous credentials to provide secure navigation services to drivers. Based on anonymous credentials and the destination of the driver, the system can automatically search for a route which yields minimum traveling delay in a secure manner using the real time information of the road condition. To acquire and use anonymous credentials for secure navigation services, in [10], the system master secret must be distributed to every vehicle which equips an additional tamper-proof device. However, this feature might bring about critical security threat when one tamper-proof device is compromised. In fact, it can be expected that such a tamper-proof device will be compromised eventually (e.g., Infineon Trusted Platform Modules) [11]. Furthermore, [10] cannot provide non-transferability to prevent an insider attacker from sharing his/her anonymous credentials. That is, it is possible to incite a registered user who obtains credentials to illegally share the credentials with unregistered users for financial gain.

In this paper, we propose a new secure and privacy-preserving navigation protocol that resolves the aforementioned problems of [10]. In particular, we focus on eliminating the system master secret distribution and update procedures for anonymous credential acquisition, hence the need of an additional tamper-proof device for safe keeping of the system master key. Moreover, the proposed protocol does not need conventional public key certificates, which put a heavy burden of pubic key management over a VANET. In order to achieve these goals, we consider the concept of two person multisignature [12] and identity-based cryptographic schemes [13] as our building blocks.

The rest of the paper is organized as follows. The next section outlines our system model and security objectives to induce the motivation of the paper. In Section 3, we present the proposed protocol for secure and privacy-preserving navigation services in VANETs. We give the security and performance evaluations of the proposed protocols in Section 4. Finally, we conclude the paper in Section 5.

2 System Model

2.1 Architecture

In this section, we describe our system model, in which communication nodes are either the trusted authority (TA), RSUs, or vehicles as shown in Figure 1. The detailed description of system components is as follows:

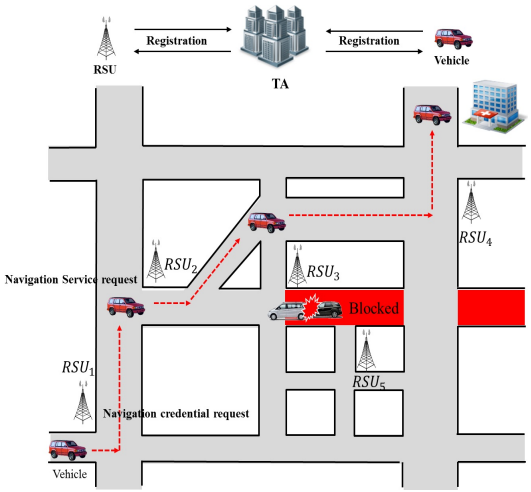


Figure 1: System architecture

- TA is public and trusted agencies. For instance, transportation authorities or corporations with administrative rights can take on a role as TA. It is in charge of the registration of RSUs and vehicles deployed on a VANET, and issues cryptographic materials through initial registration. In addition, it should be able to trace a vehicle's real identity in case of billing purpose for navigation services or tracing the compromised subscriber who may threaten the system.

- RSUs are installed along the roads and subordinated to the TA. Each RSU has a local database storing real time map information (e.g., traffic volume, events information) about its vicinity. It performs the route searching process to provide navigation services for drivers and also performs cryptographic operations for supporting secure and privacy-preserving navigation services to each vehicle within RSUs' communication range. Also, they may not disclose any inner information without the authorization of the TA.

- Each vehicle equips OBU to communicate with RSUs to request navigation services. In our system model, every vehicle is bootstrapped with its own identity-based secret key during the initial phase, described in the subsequent section, to performs cryptographic operations such as signature generation/verification and encryption/decryption of messages for secure and privacy-preserving navigation services.

For the sake of clarity, we make the following assumptions:

- RSUs communicate with each other and with TA through a fixed secure channel by the internet or any other reliable communication links with high bandwidth.

- Vehicles are equipped with an embedded computer, a GPS receiver, a wireless network interface compliant to standards like 802.11p incorporated with dedicated short range communications (DSRC) [2].

- TA, RSUs, and vehicles have clocks for generation of time stamp and check valid time of credentials. They can use GPS satellites as a synchronized time source [14].

- The adversary can overhear V2V and V2I communications to obtain any messages from vehicles or RSUs to enjoy free navigation services in case it is going to the same destination.

- The adversary can try to identify vehicles or to trace the traveling routes of a vehicle by packet analysis.
- The TA can inspect all RSUs at high level and maintain the compromised entities list.

2.2 Security Objectives

We clarify our security objectives in order to provide secure and privacy-preserving navigation services in VANET environments. The concerns of our design are summarized as follows:

- *Authentication and Authorization* : Only legitimate entities should take part in the VANETs. In addition, the origin of the messages should be authenticated to guard against the impersonation and message forgery attacks. Also, only a legitimate subscriber which has service access rights should be able to get navigation service to guarantee the quality of service in service-oriented VANET applications.
- *Confidentiality* : To avoid having navigation service illegally from unauthorized vehicles who may not want to pay for navigation service, navigation query and result should be kept confidential from eavesdroppers.
- *Identity Privacy Preservation* : The real identity of a vehicle should be kept secret from other vehicles as well as RSUs for privacy preservation.
- *Traceability* : The TA should have the ability to reveal the real identity of a vehicle in case of service charge for using the navigation service or non-repudiation property of messages.
- *Non-transferability of credential* : Vehicles (or users) cannot afford to share navigation service credentials with other vehicles.

With privacy concerns being rapidly raised in wireless communications, user anonymity has become an important property for secure VANET applications. There are variety of flavors for user anonymity such as user identity protection, user untraceability, k-anonymity, blender anonymity and so on [15, 16], and various notions may be implemented in different application environments [17]. The notion of anonymity in the proposed protocol is defined against the eavesdropping attackers rather than the service provider because the service provider has to disclose user's real identity for accounting, billing and revocation purposes. Therefore, user anonymity means to guarantee that the adversary cannot determine the real identity of the user in this paper.

Another challenge of anonymous credential management is non-transferability in subscription-based value added services. In other words, a user should not share his/her credential with other users [18]. As one drawback of VSPN [10], a common credential, which does not encode any user certifying data, is used for anonymous navigation service request. Hence, it is possible to incite a registered user who obtains a credential to illegally share the credential with unregistered users for financial gain. To resolve this problem and guarantee non-transferability, we design an anonymous navigation service credential which encodes the registered user's own certifying secret key so as to restrain from sharing the credential maliciously.

3 Proposed Protocol

In this section, we propose a new secure and privacy-preserving navigation protocol based on the concept of two person multisignature and identity-based cryptographic schemes to resolve the problems of the previous work. Table 1 describes the notations used in the proposed protocol.

Table 1: Notations and descriptions.

notation	description
$\mathbb{G}_1, \mathbb{G}_2$	bilinear map groups with the same prime order q
$P \in \mathbb{G}_1$	a generator of $\mathbb{G}_1$
s, α	TA's master secrets
P_{TA}, P_{NV}	TA's public keys
sk, pk	conventional private and public key pair
VID_i	real identity of a vehicle v_i
PID_i	pseudo identity of a vehicle v_i
VSK_i	ID-based private key of a vehicle v_i
RSK_j	ID-based private key of an RSU_j
$Enc_k(\cdot)$	symmetric encryption under key k
$Dec_k(\cdot)$	symmetric decryption under key k
$ID\_Enc_{id}(\cdot)$	ID-based encryption under given id
$ID\_Dec_{sk_{id}}(\cdot)$	ID-based decryption under private key sk_{id}
$MAC_k(\cdot)$	message authentication code under key k
θ_T	navigation service token for the current time period T
Crd_i	navigation credential of a vehicle v_i

3.1 System Setup

To initialize the system, TA performs the following operations:

1. Choose bilinear map groups $(\mathbb{G}_1, \mathbb{G}_2)$ of the same prime order q and a random generator $P \in \mathbb{G}_1$. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a bilinear map.

2. Pick a random $s \in Z_q^*$ as a master secret for identity-based key generation and sets $P_{TA} = sP$ as the corresponding public key.

3. Pick a random $\alpha \in Z_q^*$ as a secret for generating navigation credential and sets $P_{NV} = \alpha P$ as the corresponding public key.

4. Publish the public system parameters $params = \{\mathbb{G}_1, \mathbb{G}_2, q, \hat{e}, P, P_{TA}, P_{NV}, H_1\}$, where $H_1 : \{0,1\}^* \to \mathbb{G}_1$ is a hash function mapping an arbitrary message to a point in $\mathbb{G}_1$.

In our system, cryptographic keys for OBUs on vehicles and RSUs are given by the TA through the initial setup as follows:

- If the registered entity is a vehicle, each vehicle v_i submits its identity VID_i to the TA. Then the TA first computes $PID_i = Enc_{pk_{TA}}(VID_i)$ and generates v_i's private key as $VSK_i = sH_1(PID_i)$. The TA stores (VID_i, PID_i) in its storage and provides v_i with (PID_i, VSK_i) securely.

- On the other hand, RSU_j's private key is directly derived from its identity as $RSK_i = sH_1(RSU_j)$ by the TA.

In addition, the TA also generates a navigation service token for the current period T as $\theta_T = \alpha H_1(NAVI|T)$, where $NAVI$ is a keyword denoting the navigation service. The TA distributes θ_T securely to RSUs at the beginning of T, and θ_T will expire after the predefined time period (e.g., a day).

3.2 Navigation Credential Request

Suppose that a vehicle v_i wants to get secure and privacy-preserving navigation services through a VANET. v_i has to acquire a navigation credential from RSUs on the road. Figure 2 summarizes the navigation credential request protocol between a vehicle v_i and a road side unit RSU_j.

v_i		RSU_j
1	$\xrightarrow{NVC\_REQ}$	
2.		$a \in Z_q^*, X = aP;$
	$\xleftarrow{auth : \{X\}}$	
3. $b, r \in Z_q^*, X' = bP, Y = rH_1(PID_i);$ $k = \hat{e}(rVSK_i, X)\hat{e}(H_1(RSU_j), bP_{TA});$ $\phi = MAC_k(X, X', Y);$		
	$\xrightarrow{auth : \{X', Y, \phi\}}$	
4.		$k = \hat{e}(Y, aP_{TA})\hat{e}(RSK_j, X');$ check $\phi \stackrel{?}{=} MAC_k(X, X', Y);$ $C = Enc_k(\theta_T);$ $\phi' = MAC_k(X, X', Y, C);$
	$\xleftarrow{crd : \{C, \phi'\}}$	
5. check $\phi' \stackrel{?}{=} MAC_k(X, X', Y, C);$ $\theta_T = Dec_k(C);$ check $\hat{e}(\theta_T, P) \stackrel{?}{=} \hat{e}(H_1(NAVI\|T), P_{NV});$ $Crd_i = VSK_i + \theta_T.$		

Figure 2: Navigation credential request protocol.

1. v_i sends a navigation credential request message NVC_REQ to RSU_j.

2. Upon receiving the request message, RSU_j chooses a random $a \in Z_q^*$ and computes $X = aP$. RSU_j sends $auth : \{X\}$ to v_i for initiating authenticated key agreement.

3. v_i chooses a random $b, r \in Z_q^*$ and computes $X' = bP$, $Y = rH_1(PID_i)$. v_i generates the shared key $k = \hat{e}(rVSK_i, X)\hat{e}(H_1(RSU_j), bP_{TA})$ and responds with $auth : \{X', Y, \phi\}$ to RSU_j, where $\phi = MAC_k(X, X', Y)$ is an authentication code.

4. RSU_j generates the shared key $k = \hat{e}(Y, aP_{TA})\hat{e}(RSK_j, X')$, and checks $\phi \stackrel{?}{=} MAC_k(X, X', Y)$. The consistency of the shared key k between v_i and RSU_j can be proven as follows:

$$\begin{aligned} k &= \hat{e}(rVSK_i, X)\hat{e}(H_1(RSU_j), bP_{TA}) \\ &= \hat{e}(rsH_1(PID_i), aP)\hat{e}(H_1(RSU_j), bsP) \\ &= \hat{e}(rH_1(PID_i), asP)\hat{e}(sH_1(RSU_j), bP) \\ &= \hat{e}(Y, aP_{TA})\hat{e}(RSK_j, X') \end{aligned}$$

If it holds, RSU_j encrypts the navigation service token as $C = Enc_k(\theta_T)$ and sends $crd : \{C, \phi'\}$ to v_i, where $\phi' = MAC_k(X, X', Y, C)$ is an authentication code.

5. v_i checks $\phi' \stackrel{?}{=} MAC_k(X, X', Y, C)$. If it holds, then decrypts $\theta_T = Dec_k(C)$. In order to obtain a valid navigation credential, v_i verifies the navigation service token as $\hat{e}(\theta_T, P) \stackrel{?}{=} \hat{e}(H_1(NAVI|T), P_{NV})$. The correctness of the verification can be proven as follows:

$$\begin{aligned} \hat{e}(\theta_T, P) &= \hat{e}(\alpha H_1(NAVI|T), P) \\ &= \hat{e}(H_1(NAVI|T), \alpha P) \\ &= \hat{e}(H_1(NAVI|T), P_{NV}) \end{aligned}$$

Finally, v_i can compute $Crd_i = VSK_i + \theta_T$ as its credential. This Crd_i will be used for access to navigation services.

3.3 Navigation Service Request

Once obtaining a navigation credential, v_i can get navigation services for guiding routes to its destination from RSUs on the road.

1. v_i first composes the navigation request message $M = \{PID_i, ts, DEST, \kappa\}$, where $DEST$ represents its desired destination, ts indicates time stamp, and κ is a random key which is for RSU_k to encrypt the navigation result at a later stage.

2. For secure navigation service, v_i encrypts the navigation request message as $C = ID\_Enc_{RSU_k}(M)$ and requests navigation service by sending $navi\_req : \{C, \sigma\}$ to RSU_k, where $\sigma = (U_1, U_2)$ is the signature generated as following:

   - $U_1 = cP$, for a random $c \in Z_q^*$
   - $U_2 = Crd_i + cH_1(M)$

3. Upon receiving the navigation service request, RSU_k decrypts the request message as $M = ID\_Dec_{RSK_k}(C)$ and verifies $\hat{e}(P, U_2) = \hat{e}(P_{TA}, H_1(PID_i))\hat{e}(P_{NV}, H_1(NAVI|T))\hat{e}(U_1, H_1(M))$. The correctness of the verification can be proven as follows:

$$\begin{aligned} \hat{e}(P, U_2) &= \hat{e}(P, Crd_i + cH_1(M)) \\ &= \hat{e}(P, VSK_i + \theta_T + cH_1(M)) \\ &= \hat{e}(P, VSK_i)\hat{e}(P, \theta_T)\hat{e}(P, cH_1(M)) \\ &= \hat{e}(P, sH_1(PID_i))\hat{e}(P, \alpha H_1(NAVI|T))\hat{e}(P, cH_1(M)) \\ &= \hat{e}(sP, H_1(PID_i))\hat{e}(\alpha P, H_1(NAVI|T))\hat{e}(cP, H_1(M)) \\ &= \hat{e}(P_{TA}, H_1(PID_i))\hat{e}(P_{NV}, H_1(NAVI|T))\hat{e}(U_1, H_1(M)) \end{aligned}$$

   If it holds, RSU_k can be convinced that the requesting vehicle of PID_i has a valid token to access navigation service. Then, RSU_k stores (PID_i, κ) locally and proceeds to route search sub-protocol among other RSUs cooperatively.

4. RSU_k initiates route searching process to find optimal driving route to the $DEST$ and broadcasts route request message to all its neighbor RSUs, then this route request is forwarded to the RSUs which are close to the $DEST$.

5. RSU_k collects route reply of each RSU placed along the reverse path from $DEST$ to its location and decides the traveling route that has optimal road condition such as highest average speed or unblocked by traffic jam. This result is provided to the requesting vehicle as encrypted under the key κ.

Note that the distinction of this paper as compared to VSPN [10] is about navigation credential management for authorizing secure navigation service, and the details of the sub-protocol in step 3 is similar to VSPN while we use vehicle's pseudonym *PID* instead of navigation session number in VSPN for maintaining navigation routing table. Therefore, we just briefly sketched the route search sub-protocol in step 3, but we can refer to VSPN's sub-protocols.

4 Analysis

In this section, we give analysis of the proposed protocol in terms of security and computational cost for secure navigation services in VANETs.

4.1 Security

We analyze and discuss the security of the proposed protocol with respect to the security requirements stated in Section 2.

1. *Authentication* : The authentication of vehicles and RSUs can be assured by the identity-based private keys, VSK_i for a vehicle and RSK_i for a road side unit, issued by the TA through the initial setup. We adopted the identity-based authenticated key agreement protocol [13] for mutual authentication between a vehicle v_i and a road side unit RSU_j in navigation token request. Therefore, when we assume the security of the underlying identity-based cryptography, no one can launch an impersonation attack unless the entity is registered to the TA.

2. *Authorization* : In order to get navigation services, v_i must have the navigation credential Crd_i which is generated by combining TA's navigation service token $\theta_T = \alpha H_1(NAVI|T)$ for the current time period and v_i's private key VSK_i (i.e., $Crd_i = VSK_i + \theta_T$). Because the navigation service token θ_T is the function of BLS signature [19] with TA's secret α, nobody can generate and forge the token. Furthermore, the navigation request message attaches signature $\sigma = (U_1, U_2)$, which is the result of [12], to show vehicle v_i's service privilege. Therefore, only valid vehicles which obtained the navigation service token after authenticated to an RSU_j can request navigation services.

3. *Identity Privacy Preservation* : In the proposed protocol, an attacker cannot obtain vehicle's real identity from eavesdropping on navigation services. Identity related information of a vehicle v_i is $rH_1(PID_i)$ for key agreement with RSU_j during the navigation service token request protocol, and PID_i encrypted under identity-based encryption of RSU_k's ID during the navigation service request. Here, PID_i is v_i's pseudonym as the result of $Enc_{pk_{TA}}(VID_i)$ for the real identity. Therefore, neither an attacker nor an RSU can reveal the real identity of v_i from PID_i.

4. *Confidentiality* : To avoid getting navigation contents illegally from unauthorized vehicles, the navigation service token for generating credential is encrypted under the secret key k (i.e., $Enc_k(\theta_T)$) and transmitted to a vehicle in the navigation credential request protocol. Also, navigation query of a vehicle is encrypted under RSU's ID-based public key, and navigation result is encrypted under the key κ randomly selected in navigation service request protocol. Hence, confidentiality requirement is satisfied in our protocol.

5. *Traceability* : Even though it is hard for an attacker and an RSU to know the real identity of a vehicle, TA should have the capability to reveal vehicle's real identity so that the vehicle can be charged for using navigation service as well for non-repudiation. As mentioned before, vehicle's PID_i is the encryption of its real identity under TA's public key. Hence, only the TA can reveal the real identity of a vehicle for given PID_i.

6. *Non-transferability of credential* : As discussed in the above, a vehicle v_i's navigation credential Crd_i is the combination of TA's navigation service token θ_T and v_i's private key VSK_i derived from v_i's pseudonym PID_i. Moreover, navigation service request message $M = \{PID_i, ts, DEST, \kappa\}$ is singed under the credential, as $\sigma = (cP, Crd_i + cH_1(M))$, during the navigation service request protocol which requires the requesting vehicle v_i to prove that its secret VSK_i corresponding to PID_i is encoded in the credential by submitting signature. Hence, to enable unregistered vehicles to access navigation service by sharing the credential Crd_i, they should share both Crd_i and v_i's secret key VSK_i which would lead to the compromise of v_i's secret key. Consequently, the proposed credential management scheme can guarantee the non-transferability of credential by encouraging legitimate vehicles not to share their credentials with other vehicles.

4.2 Computational cost

In this section, we evaluate and compare the computational costs of the proposed protocol with VSPN [10]. Let T_{pair} and T_{mul} be the time required to perform bilinear pairing and scalar point multiplication over an elliptic curve, respectively. Also, let T_{as-enc}, T_{as-dec}, T_{sig}, T_{vrf}, and T_{re-enc}, T_{re-dec}, be the time required to perform conventional asymmetric encryption and decryption, signature generation and verification, and proxy re-encryption and decryption operations, respectively. Here, we considered the proxy re-encryption scheme of [20] for T_{re-enc} and T_{re-dec} as referenced in VSPN. We did not take any other negligible computation such as symmetric encryption and cryptographic hash functions into account.

We estimated the computational costs of the proposed scheme by categorizing into sub-procedure and sub-protocol; navigation service token generation by the TA, navigation request, and navigation service request. Table 2 shows the results as comparing with VSPN. From security management perspective, anonymous credential management is the main function of the proposed protocol for secure navigation service. In Table 2, our navigation credential request protocol itself requires more computational cost than VSPN. However, before requesting navigation credential in VSPN, vehicles must perform master key requesting protocol unless the vehicles do not possess the newly updated master key. Therefore, the total computational cost of the proposed protocol to complete the credential request is advantageous, and VSPN's credential cannot guarantee the non-transferability as we discussed in security analysis.

Table 2: Computational costs of VSPN and the proposed protocol.

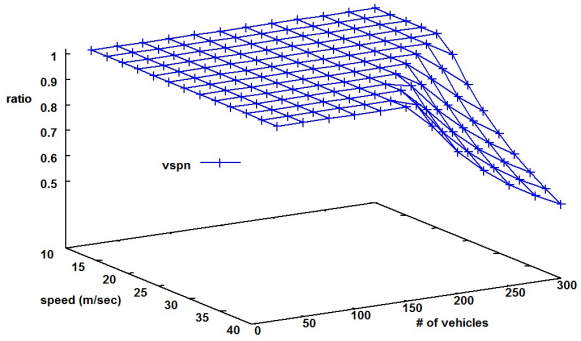
	VSPN		Proposed	
	OBU	RSU	OBU	RSU
Generating navigation service token	T_{mul} (by TA)		T_{mul} (by TA)	
Master key request	$T_{sig} + T_{as-dec} + T_{re-dec}$	$2T_{pair} + T_{mul} + T_{re-enc} + T_{vrf} + T_{as-enc}$	-	-
Navigation credential request	$5T_{mul} + T_{as-enc}$	$2T_{pair} + T_{mul} + T_{as-enc}$	$2T_{pair} + 4T_{mul}$	$2T_{pair} + 2T_{mul}$
Navigation service request	T_{as-enc}	$T_{as-dec} + 2T_{pair}$	$2T_{mul} + T_{as-enc}$	$4T_{pair} + T_{as-dec}$

In addition, to show the efficiency of the proposed protocol, we compared RSU's valid serving ratio for processing navigation credential request within RSU's coverage range R_{rng} following the analytic method of [7]. RSU's performance depends on the number of requesting vehicles n and moving speed s

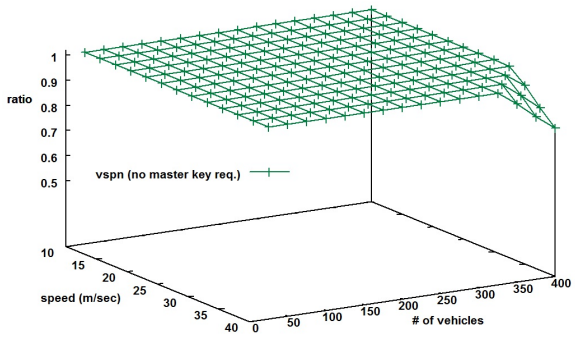
passing RSU's coverage range. Then, the valid serving ratio S_{RSU}, which is the fraction of the number of actually processed to the number of requests, can be measured by the following formula where ρ is the probability for each vehicle in RSU's range to request navigation credential, and T_{crd} is the computational time to perform navigation credential request of Table 2. We estimated cryptographic overhead by using the pairing-based cryptography library of [21] on Pentium-III 1GHz machine to measure the processing time.

$$S_{RSU} = \begin{cases} 1, & \text{if } \frac{R_{rng}}{T_{crd} \cdot \rho \cdot s \cdot n} \geq 1 \text{ ;} \\ \frac{R_{rng}}{T_{crd} \cdot \rho \cdot s \cdot n}, & \text{otherwise.} \end{cases}$$

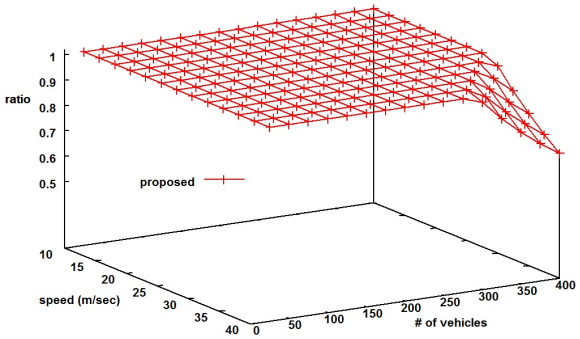
Figure 3 shows valid RSU's serving ratio for processing credential request under VSPN and our protocol with different vehicle density and speed within R_{rng}=1,000m and ρ=0.8. Note, in VSPN, that if a vehicle newly joins the service or does not possess the last updated master key, the vehicle must obtain the master key from an RSU before requesting navigation credential. On the other hand, once obtaining the master key, master key request is not required until next master key update. Figure 3-(a) and 3-(b) respectively show the results for those cases, and 3-(c) shows the result of the proposed protocol. From the results, we can observe that our credential request protocol outperforms VSPN's credential request protocol including master key request, and less efficient than VSPN with no master key request assuming all vehicles already obtained the master key but the difference is slight.



(a) Valid service ratio of VSPN including master key request processing.



(b) Valid service ratio of VSPN without master key request processing.



(c) Valid service ratio of the proposed protocol

Figure 3: RSU's valid service ratio for processing navigation credential request.

5 Conclusion

In this paper, we have proposed a new secure and privacy-preserving navigation protocol that overcome the problems of [10]. The proposed protocol removes the system master secret distribution and update procedures for anonymous credential acquisition and conventional public key certificates. For secure navigation services, our protocol is based on the concept of two person multisignature and identity-based cryptographic schemes for mutual authentication between a vehicle and rode side unit in navigation service token request. We have provided the analysis to confirm the fulfillment of the security objectives and the efficiency of the proposed protocol.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (NRF-2013R1A1A4A01009848).

References

[1] J. Jeong, S. Guo, Y. Gu, T. He, and D. H. Du, "Trajectory-based data forwarding for light-traffic vehicular ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 743–757, May 2011.

[2] US Federal Communication Commission, "Dedicated. Short Range Communication Report and Order," December 2003. [Online]. Available: http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-03-324A1.pdf/

[3] B.-J. Chang, B.-J. Huang, and Y.-H. Liang, "Wireless sensor network-based adaptive vehicle navigation in multihop-relay wimax networks," in *Proc. of the 22nd International Conference on Advanced Information Networking and Applications (AINA'08), Okinawa, Japan*. IEEE, March 2008, pp. 56–63.

[4] R. Lu, X. Lin, H. Zhu, and X. Shen, "Spark: A new vanet-based smart parking scheme for large parking lots," in *Proc. of the 28th IEEE International Conference on Computer Communications (INFOCOM'09), Rio de Janeiro, Brazil*. IEEE, April 2009, pp. 1413–1421.

[5] C. L. P. Chen, J. Zhou, and W. Zhao, "A real-time vehicle navigation algorithm in sensor network environments," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 4, pp. 1657–1666, December 2012.

[6] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "Gsis: A secure and privacy preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, November 2007.

[7] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. of the 28th IEEE International Conference on Computer Communications (INFOCOM'08), Phoenix, USA*. IEEE, April 2008, pp. 1229–1237.

[8] Y. Park, C. Sur, C. D. Jung, and K.-H. Rhee, "An efficient anonymous authentication protocol for secure vehicular communications," *Journal of Information Science and Engineering*, vol. 26, no. 3, pp. 785–800, May 2010.

[9] C. Sur, Y. Park, K. Sakurai, and K. H. Rhee, "Providing secure location-aware services for cooperative vehicular ad hoc networks," *Journal of Internet Technology*, vol. 13, no. 4, pp. 631–644, July 2012.

[10] T. Chim, S. Yiu, L. C. Hui, and V. O. Li, "Vspn: Vanet-based secure and privacy-preserving navigation," *IEEE Transactions on Computers*, vol. PP, no. 99, pp. 1–14, August 2012.

[11] C. Tarnovsky, "Deconstructing a Secure Processor," February 2010. [Online]. Available: https://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html

[12] C. Gentry and A. Silverberg, "Hierarchical id-based cryptography," in *Proc. of the 8th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'02), Queenstown, New Zealand, LNCS*, vol. 2501. Springer-Verlag, December 2002, pp. 548–566.

[13] L. Chen, Z. Cheng, and N. P. Smart, "Identity-based key agreement protocols from pairings," *International Journal of Information Security*, vol. 6, no. 4, pp. 213–241, July 2007.

[14] K. Behrendt and K. Fodero, "The perfect time: An examination of time-synchronization techniques," in *Proc. of the 32rd Annual Western Protective Relay Conference, Spokane, USA*. Washington State University, October 2005, pp. 1–18.

[15] D. He, C. Chen, J. Bu, S. Chan, and Y. Zhang, "Security and efficiency in roaming services for wireless networks: challenges, approaches, and prospects," *IEEE Communications Magazine*, vol. 51, no. 2, pp. 142–150, February 2013.

[16] D. Hughes and V. Shmatikov, "Information hiding, anonymity and privacy: a modular approach," *Journal of Computer Security*, vol. 12, no. 1, pp. 3–36, January 2004.

[17] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "Sat: A security architecture achieving anonymity and traceability in wireless mesh networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 2, pp. 295–307, April 2011.

[18] Y. Yang, R. H. Deng, and F. Bao, "Privacy-preserving rental services using one-show anonymous credentials," *Security and Communication Networks*, vol. 2, no. 6, pp. 531–545, December 2009.

[19] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proc. of the 7th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'01), Gold Coast, Australia, LNCS*, vol. 2248. Springer-Verlag, December 2001, pp. 514–532.

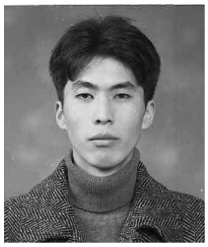
[20] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security*, vol. 9, no. 1, pp. 1–30, February 2006.

[21] "Pairing-Based Cryptography Library." [Online]. Available: http://crypto.stanford.edu/pbc

Author Biography

Wonjun Cho is received the B.S. degree from Dongeui University, Republic of Korea in 2010. He is currently a master course student in the Department of IT Convergence and Application Engineering, Pukyong National University. His research interests are in the areas of secure vehicular ad hoc networks, cryptographic algorithms.

Youngho Park received his M.S. and Ph.D. degrees in Department of Computer Science and Information Security from Pukyong National University, Republic of Korea in 2002 and 2006, respectively. He is currently a postdoctoral researcher in Department of IT Convergence and Application Engineering, Pukyong National University. His research interests are related with information security, applied cryptography and network security; secure ad hoc network, authentication, key management, and identity-based cryptosystem.



Chul Sur received his M.S. and Ph.D. degrees in the Department of Computer Science from Pukyong National University, Republic of Korea in 2004 and 2010, respectively. He is currently a postdoctoral researcher in the Department of IT Convergence and Application Engineering, Pukyong National University. His research interests are related with applied cryptography, network security, and secure e-commerce.

Kyung Hyune Rhee received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute (ETRI), Republic of Korea from 1985 to 1993. He also worked as a visiting scholar in the University of Adelaide, the University of Tokyo, and the University of California, Irvine. He has served as a Chairman of Division of Information and Communication Technology, Colombo Plan Staff College for Technician Education in Manila, the Philippines. He is currently a professor in the Department of IT Convergence and Application Engineering, Pukyong National University, Republic of Korea. His research interests center on key management and its applications, mobile communication security and security evaluation of cryptographic algorithms.