



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

Thesis for the Degree of Master of Engineering

Privacy-Preserving Navigation Protocol for Vehicular Cloud



Department of IT Convergence and Application Engineering

The Graduate School

Pukyong National University

February 2014

Privacy-Preserving Navigation Protocol for Vehicular Cloud

차량 클라우드를 위한 익명 네비게이션 프로토콜

Advisor: Prof. Kyung-Hyune Rhee

by

Wonjun Cho

A thesis submitted in partial fulfillment of the requirements
for the degree of

Master of Engineering

in Department of IT Convergence and Application Engineering,
The Graduate School,
Pukyong National University

February 2014

Privacy-Preserving Navigation Protocol
for Vehicular Cloud

A dissertation
by
Wonjun Cho



Approved by :

(Chairman) Man-Gon Park

(Member) Kyung-Hyune Rhee

(Member) Sang Uk Shin

February 2014

Contents

Contents

| | |
|--|------------|
| List of Tables | ii |
| List of Figures | iii |
| 1 Introduction | 1 |
| 1.1 Background | 1 |
| 1.2 Overview and Contribution | 3 |
| 2 Preliminary | 4 |
| 2.1 Vehicular Cloud Computing | 4 |
| 2.1.1 Service models | 5 |
| 2.1.2 Formation of Vehicular Cloud Infrastructure | 7 |
| 2.2 Related Work | 9 |
| 2.3 Cryptographic Tools | 10 |
| 2.3.1 Identity based key agreement scheme | 11 |
| 2.3.2 Hierarchical ID-based signature | 12 |
| 3 Vehicular Cloud Computing based Privacy-Preserving Navigation | 14 |
| 3.1 System Model | 14 |
| 3.2 Security Requirements | 16 |

| | | |
|----------|---|-----------|
| 3.3 | Proposed Protocol | 18 |
| 3.3.1 | System Setup | 18 |
| 3.3.2 | Navigation Credential Request | 21 |
| 3.3.3 | Navigation Service Request | 22 |
| 4 | Analysis | 25 |
| 4.1 | Security | 25 |
| 4.2 | Computational cost | 27 |
| 5 | Conclusion | 32 |
| | References | 34 |



List of Tables

| | | |
|-----|--|----|
| 3.1 | Notations and descriptions. | 19 |
| 4.1 | Computational costs of VSPN and the proposed protocol. | 29 |



List of Figures

| | | |
|-----|--|----|
| 3.1 | System architecture | 14 |
| 3.2 | Navigation credential request protocol. | 24 |
| 4.1 | RSU's valid service ratio for processing navigation credential request. | 31 |



차량 클라우드를 위한 익명 네비게이션 프로토콜

조 원 준

부경대학교 대학원 IT 융합응용공학과

요약

최근 도요타와 MS의 PHV drive support, 볼보와 Infrasy Cloud의 제휴, IBM과 GM의 Onstar와 같이 차량과 운전자, 차량 제조업체들을 연결하여 서비스의 개선과 차량 운행보조를 목적으로 차량 클라우드가 활발히 연구되고 있다. 차량 클라우드는 휴대전화와 마찬가지로 차량 또한 수천가지의 어플리케이션을 사용하게 될 것이며, 이 과정에서 클라우드는 업무의 부하를 처리하기 위한 수단이 되고 있다. 이를 이용하기 위해서는 개인의 정보와 같은 민감한 정보들이 클라우드에 공유되어야 하고 안전한 서비스 제공을 위해서는 프라이버시 보호가 필수적으로 만족되어야 한다. 본 논문에서는 차량 클라우드를 이용한 네비게이션 서비스 모델을 제안하며 신원기반 암호를 적용하여 서비스 제공 단계에서 사용자의 신원 정보를 노출하지 않는 네비게이션 프로토콜을 설계하였다. 또한 제시한 보안 프로토콜의 안전성을 보이고 실험결과를 통하여 제안한 기법의 효율성을 검증한다.

Chapter 1. Introduction

1.1 Background

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 [8]. 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 [4, 16, 5].

VANET can indeed be used to offer such services, but these come with a cost, both at network and hardware levels. For example, traffic monitoring and incident reporting systems employ inductive loop detectors(ILDs), cameras, microwave sensors. Each ILD costs around \$8,200 and the ILDs are connected by optical fiber that costs \$300,000 per mile.

In recent years, motor-vehicle manufacturer has been working with IT ven-

dor to provide several computational services at low cost to the vehicle drivers. For example, In April 2011 Microsoft Corporation and Toyota Motor Corp. launched a strategic alliance to jointly fabricate a software platform dedicated to managing the information systems for electric vehicles. These technologies now pose new opportunities and challenges for not only motor-vehicle manufacturer but also to vendor of computers and communication technologies. A primary goal of the Vehicular cloud computing is to offer on-demand solutions for unpredictable events in a proactive fashion.

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 [14, 15, 18, 20]. 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. Moreover, in Vehicular Cloud, all the users, including the attackers, are equal. The attackers and their targets may be physically co-located on one machine. The attackers can utilize system loopholes to reach

their goals, such as obtaining confidential information and tampering with the integrity of information and the availability of resources.

1.2 Overview and Contribution

In this thesis, we propose a new secure and privacy-preserving navigation protocol for vehicular cloud that resolves the limitations of the previous work. 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 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 public key management over a vehicular cloud. In order to achieve these goals, we consider the concept of two person multisignature [9] and identity-based cryptographic schemes [6] as our building blocks. In addition, the proposed protocol will be analyzed in terms of security requirements and efficiency such as RSU computational costs. To consider cloud computing of vehicular environment, we introduce vehicular cloud and summarize feasible service model of vehicular cloud.

The rest of the thesis is organized as follows. The next chapter briefly introduce the vehicular cloud computing and feasible service models. In chapter 3, we present the proposed protocol for secure and privacy-preserving navigation services in vehicular cloud. We give the security and performance evaluations of the proposed protocols in chapter 4. Finally, we conclude the thesis in chapter 5.

Chapter 2. Preliminary

2.1 Vehicular Cloud Computing

Cloud computing is used to describe data acquisition or distribution through the Internet and wireless networks. As a logical expansion of the similar Software as a Service (SaaS) design, where software users get remote access to applications rather than downloading them, cloud computing services also use existing networks as a conduit for remote services. One of the ways that cloud computing could really assist in better motor-vehicle manufacturer, according to a number of motor-vehicle manufacturer, is by allowing for a smaller center console. With less hardware under the dash, and many data tasks outsourced to a remote server, vehicles could get slimmer control boards, and a bit more leg room.

Another advantage of cloud-based computing in vehicles relates to a driver's financial investment and a car's insurance value. With fewer expensive data storage elements in the vehicle, motor-vehicle manufacturer might be able to decrease the cost of computerized vehicles.

Cloud services could enable more efficient GPS-enabled augmented reality devices. One example is a lane departure warning system now common on some luxury vehicles. This system typically relies on satellite signals to help keep a car traveling in a safe path. Other similar features include pre-collision warnings, which, in some vehicles, employ radar and automated braking to prevent a crash. These systems generally use physical sensors, but cloud com-

puting would enable more consolidation for the acquisition of key satellite signals, while possibly making some kinds of physical sensors obsolete because of the large amount of physical data that could be sent over cloud services.

Ford motor company combines social networks, GPS location and real-time vehicle data in ways that help drivers go where they want efficiently by using the cloud. Toyota and Microsoft announced a new \$12 million partnership to bring cloud computing to Toyota vehicles. The partnership will equip Toyota vehicles with the advanced technology to access road information, infotainment service and GPS services, while on the road. The technology will provide viable solutions for essential safety information for drivers.

2.1.1 Service models

In this section, several service models of vehicular cloud are outlined. The case of for vehicular cloud computing can be argued by considering the unique advantages of vehicular cloud computing, and a wide range of potential vehicular cloud computing service models have been recognized. One of most important advantages of vehicular cloud computing is data aggregation by using cloud storage, where various organizations. For instance, police or business can use the stored data in the cloud to perform various operation.

- *Network as a service* : Although some vehicle will have network connections through mobile phone networks or other fixed access point, some vehicles do not have network connections. These valuable resources can be shared on the road by giving net access to those who are interested in renting it from the vehicles. The vehicle who is willing to share this resource, they will advertise such information to all vehicles around them

on the road. This information can pass among the vehicles in the local proximity who can act as an access point to the internet.

- *Storage as a service* : While some vehicles have enough on-board storage capabilities, other vehicles may require additional storage to execute their applications. Due to the small size and the inexpensive price of storage, it is reasonable that the on-board storage of vehicles will have multiple tera-bytes of storage. Thus, the vehicle with huge storage can provide storage as a service.
- *Cooperation as a service* : Vehicular Networks can provide a variety of services, such as driver safety, traffic information, warning of road conditions, parking assistance and advertisements. But these come with a cost, both at network and hardware levels. For example, traffic monitoring and incident reporting systems employ inductive loop detectors(ILDs), cameras, microwave sensors. Each ILD costs around \$8,200 and the ILDs are connected by optical fiber that costs \$300,000 per mile. Mousannif *et al* [17] introduced Cooperation as a Service which provides several free services without any infrastructure, by exploiting the advantages of vehicular cloud computing. Cooperation as a service uses a mechanism by which the drivers express their interest for a service or a set of services network where the vehicles having the same service subscribed to cooperate the subscriber by necessary information regarding the service he subscribed to by publishing the information to the network.
- *Surveillance as a service* : M. Gerla *et al* [10] introduce Photo Surveillance in vehicular cloud that delivers images on demand to citizens by

using vehicles' on board cameras. In [10], The surveillance service selects a group of vehicles to take photo shots of a give urban landscape within a given timeframe as requested by a customer. To participate in this service, vehicles register to the cloud manager. They also update their location to the cloud manager. Each vehicle keep track of their movements for a predefined time period. They propose the vehicle selection procedure for the photo shot. This service can help for forensic and insurance claim in case of an accident.

- *Infotainment as a service* : For a safe and comfortable journey on the road, people often need some kind of information. A vehicle would be a mobile information storage and an vehicular cloud can be envisioned as a huge wireless networks with very dynamic membership. It would be beneficial for a vehicle to query the information of other vehicle in the vicinity in order to increase the fidelity of its own information. Vehicular cloud will play a essential role in bringing together a huge number of contents resources.

2.1.2 Formation of Vehicular Cloud Infrastructure

This chapter considers formation of vehicular cloud Infrastructure.

- *Stationary Vehicular Cloud* : In some cases a vehicular cloud may behave as a conventional cloud especially in static environments. For example, a small company employing about hundreds of people and concentrating on offering IT services and support. There will be parked hundreds vehicle in parking lot. Everyday, the computational resources in those vehicles are sitting idle. By providing some incentive, the company may actively

request the formation of a stationary vehicular cloud for its staff, who will rent the resources. The resulting static vehicular cloud will accumulate the storage and computational resources of the participating vehicles sitting in the parking lot for the purpose of creating a computer cluster and a huge distributed data storage center which with proper security safeguards, can be come and important asset for company.

- *Linked with a fixed infrastructure* : Vehicular cloud can create and evolves in an area instrumented and be deployed by some form of a static infrastructure that supports the management of various activities. In urban environments such infrastructure contain inductive loop detectors, video cameras, radar sensors and access points are helpful for vehicular cloud. Vehicular cloud benefits from the interaction with the existing static infrastructure. For example, a city block where minor traffic incident has occurred. The congested vehicles will harvest all of their resources as a pool, and indicate the higher authority to reschedule traffic lights to de-congest that area as soon as possible.
- *Dynamic formation* : The architectural support of the formation of this type of vehicular cloud will involve the unique element. A broker elected among the vehicles that will attempt to form of vehicular cloud. The broker will acquire authorization from the a higher authority for the formation of an vehicular cloud. A unique broker will invite the vehicles for vehicular cloud formation in the area after receiving authorization. The vehicle will decide to accept the invitation or not on a autonomous basis. When a sufficient number of vehicles are in place, then the broker will decide to announce the vehicular cloud formation. The vehicular

cloud will harvest their resources to form a large computing entity like supercomputer.

2.2 Related Work

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 [13]. 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.

Especially, Lu *et al* [16] 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* [4] 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.

Recently, Chim *et al* [7] 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 [7], 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) [21]. Furthermore, [7] 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.

2.3 Cryptographic Tools

Since the invention of public key cryptography in the significant work by Diffie and Hellman, various cryptographic primitives and protocols have been developed. Such primitives have been used to secure different aspects of communication and address privacy issues in networked systems. We overview some of these protocols, focusing on those relevant to this thesis.

2.3.1 Identity based key agreement scheme

Key agreement is a cryptographic protocol, where two or more participants, who each have a long-term key, exchange ephemeral messages over an open network with each other. Using the long-term keys and key tokens, these participants generate a session secret shared between them. This secret is used to establish a session key and to perform various security functions, for example, key confirmation, entity and data authentication and confidentiality. The open network is controlled by an adversary, who aims to infiltrate the protocol. A secure key agreement protocol guarantees that the adversary does not succeed. The first feasible identity-based key agreement scheme from pairing on elliptic curves was proposed by Smart[6], by combining the ideas from previous works.

In this chapter, we introduce Smart's key agreement scheme[6]. Smart's identity key agreement protocol involves two user who wish to establish a shared secret session key, and and a TA from whom they each require their own private key. To provide a private key generation, the TA uses their key pair. The public key is $P_s = sP \in \mathbb{G}_1$, where P is a generator of \mathbb{G}_1 and the private key is $s \in Z_q^*$. When a user registers with TA, the TA issues a private key $S = sH_1(ID)$ for the user, where $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}_1$ is a hash function.

Suppose that the TA issues the following private keys for A and B respectively: $S_A = sH_1(ID_A)$, and $S_B = sH_1(ID_B)$.

A and B each randomly choose an ephemeral private key $a, b \in Z_q^*$ and compute the values of the corresponding ephemeral public keys, $T_A = aP$ and $T_B = bP$. Then they exchange the public keys.

At the conclusion of the protocol A computes $K_{AB} = \hat{e}(S_A, T_B)\hat{e}(aH_1(ID_B), P_s)$ and B computes $K_{AB} = \hat{e}(S_B, T_A)\hat{e}(bH_1(ID_A), P_s)$.

2.3.2 Hierarchical ID-based signature

ID-based encryption, whether hierarchical or not, has a clear advantage over PKI. It does not require online public key lookup. On the other hand, it is not so clear that ID-based signatures have an advantage over traditional signature schemes using PKI. Indeed, any public-key signature scheme may be transformed into an ID-based (hierarchical) signature scheme by using (a hierarchy of) certificates, since certificates bind an identity to a public key. The previous comments notwithstanding, we present a Hierarchical ID-based Signature (HIDS) scheme based on the difficulty of solving the Diffie-Hellman problem in the group G_1 . When viewed in isolation, this HIDS scheme is not especially useful for the reasons stated above (though it may be more efficient). However, as will be explained later, the HIDS scheme becomes quite useful when viewed in combination with the HIDE scheme as a complete package.

In this chapter, We introduce Gentry's HIDS scheme[9]

A HIDS schemes is specified by five algorithms: Root Setup, Lower-level Setup, Extraction, Signing, and Verification.

- *Root Setup*: The root Public Key Generator (PKG) takes a security parameter K and returns *params* and a root secret. The system parameters include a description of the message space \mathcal{M} and the signature space \mathcal{S} . The system parameters will be publicly available, while only the root PKG will know the root secret.
- *Lower-Level Setup*: Lower-level users must obtain the system parameters of the root PKG. In HIDE schemes, a lower-level user is not permitted to have any lower-level parameters of its own. However, this constraint does

not necessarily preclude a lower-level PKG from generating its own lower-level secret, which it may use in issuing private keys to its children. In fact, in our HIDE scheme, a lower-level PKG may generate a lower-level secret, or it may generate random one-time secrets for each Extraction.

- *Extraction*: A PKG with ID-tuple (ID_1, \dots, ID_t) may compute a private key for any of its children by using the system parameters and its private key.
- *Signing*: A signer inputs $params$, its private key d , and $M \in \mathcal{M}$ and outputs a signature $S \in \mathcal{S}$.
- *Verification*: A user inputs $params$, the ID-tuple of the signer, $M \in \mathcal{M}$, and $S \in \mathcal{S}$ and outputs valid or invalid.

Signing and verification must also satisfy a consistency constraint, namely when d is the private key generated by the Extraction algorithm for ID-tuple, then $\forall M \in \mathcal{M} : \text{Verification}(params, ID\text{-tuple}, M, S) = \text{valid}$ where $S = \text{Signing}(params, d, M)$.

Chapter 3. Vehicular Cloud Computing based Privacy-Preserving Navigation

3.1 System Model

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

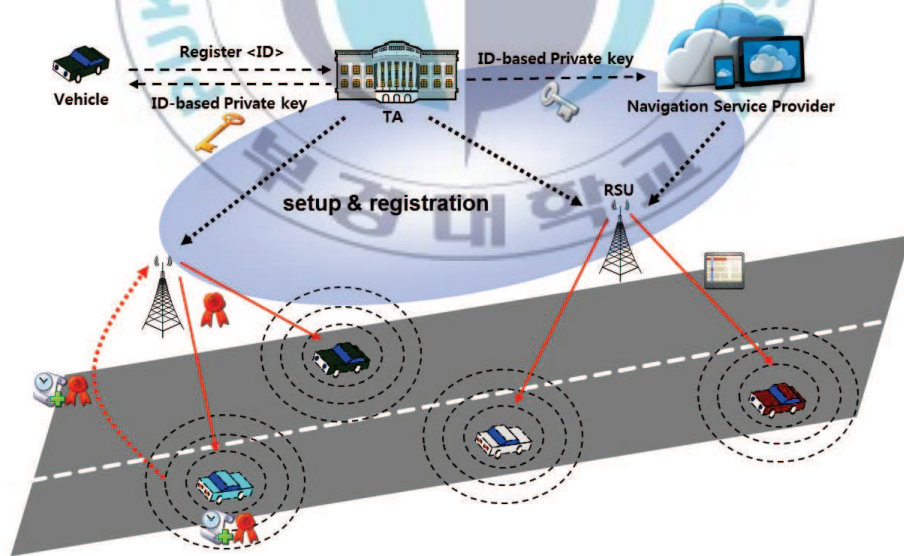


Figure 3.1: System architecture

- TA is public and trusted agencies. For instance, transportation authori-

ties 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. RSUs acts as a broker between vehicle and Cloud Service Provider. It manages Cloud Service Provider who participate in the mobile cloud. When vehicle sends a request to the RSU, RSU selects the proper Cloud Service Provider to perform the requested service. Each RSU has a local database storing real time map information (e.g., traffic volume, events information) about its vicinity. It performs cryptographic operations for supporting secure and privacy-preserving cloud services to each vehicle within RSU's 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 chapter, to performs cryptographic operations such as signature generation/verification and encryption/decryption of messages for secure and privacy-preserving navigation services.
- Cloud Service Provider(CSP) provides real-time navigation service for vehicles. In order that real-time navigation service, they collect road in-

formation from RSUs. It performs the route searching process to provide navigation services for drivers.

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

- RSUs communicate with each other, CSP and 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) [8].
- 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 [2].
- 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.

3.2 Security Requirements

We clarify our security objectives in order to provide secure and privacy-preserving navigation services in vehicular cloud environments. The concerns

of our design are summarized as follows:

- *Authentication and Authorization* : Only legitimate entities should take part in the vehicular cloud. 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 vehicular cloud 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 [11, 12], and various notions may be implemented in different application environments [19]. 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 thesis.

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 [22]. As one drawback of VSPN [7], 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.

3.3 Proposed Protocol

In this chapter, 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.

3.3.1 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

Table 3.1: 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 |
| CSK_k | ID-based private key of an CSP_k |
| $Enc_k(\cdot)$ | 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 |

random generator $P \in \mathbb{G}_1$. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ 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 $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}_1$ 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 and CSP_k 's private keys are directly derived from their identity as $RSK_i = sH_1(RSU_j)$ and $CSK_k = sH_1(CSP_k)$ 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 provider. 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).

3.3.2 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 .

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.

3.3.3 Navigation Service Request

Once obtaining a navigation credential, v_i can get navigation services for guiding routes to its destination from Cloud Service Provider.

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 CSP_k to encrypt the navigation result at a later stage.
2. For secure navigation service, v_i encrypts the navigation request message as $C = ID_Enc_{CSP_k}(M)$ and requests navigation service by sending $navi_req : \{C, \sigma\}$ to CSP_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, CSP_k decrypts the request message as $M = ID_Dec_{CSK_k}(C)$ 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, CSP_k can be convinced that the requesting vehicle of PID_i has a valid token to access navigation service. Then, CSP_k stores (PID_i, κ) until v_i arrive to $DEST$ for urgent route change. Because, road condition vary abruptly. A road which is initially in good condition may become blocked in a second.

4. CSP_k initiates route searching process to find optimal driving route to the $DEST$. CSP_K collects road information from RSUs to decide 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 .

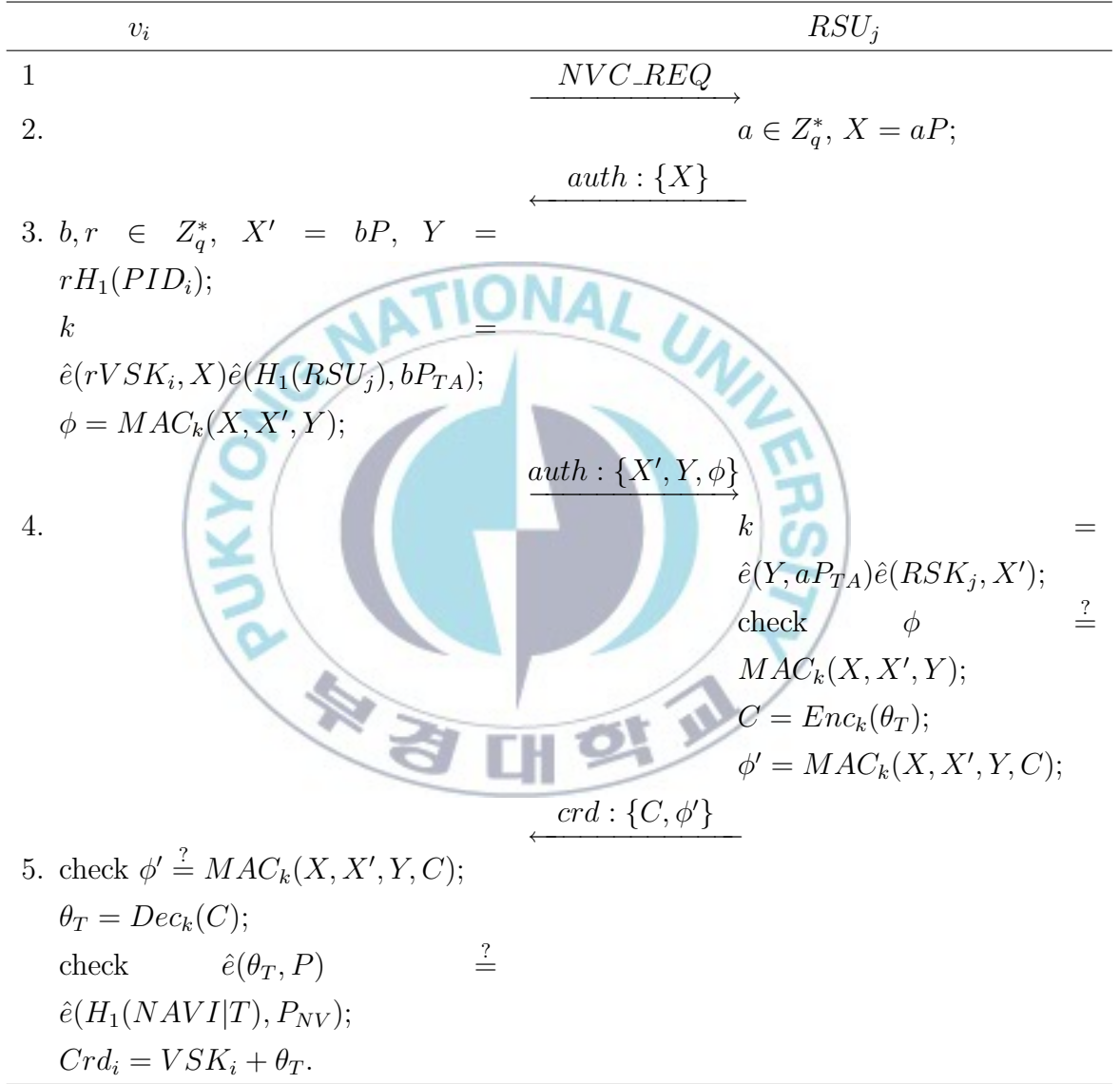


Figure 3.2: Navigation credential request protocol.

Chapter 4. Analysis

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

4.1 Security

We analyze and discuss the security of the proposed protocol with respect to the security requirements stated in chapter 3.2.

1. *Authentication* : The authentication of vehicles, RSUs and CSPs can be assured by the identity-based private keys, VSK_i for a vehicle and RSK_i for a road side unit and CSK_i for a cloud service provider issued by the TA through the initial setup. We adopted the identity-based authenticated key agreement protocol [6] for mutual authentication between a vehicle v_i and a road side unit RSU_j in navigation token request. In addition, navigation result is encrypted under the κ randomly selected in navigation service request protocol by v_i . 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 [3] 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 [9], 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 signed 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 chapter, we evaluate and compare the computational costs of the proposed protocol with VSPN [7]. 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 [1] 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.

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 [15]. 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

Table 4.1: Computational costs of VSPN and the proposed protocol.

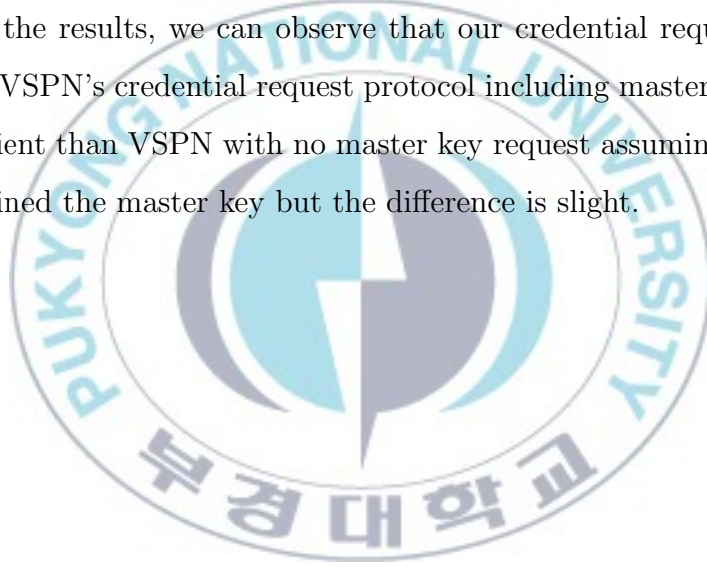
| | VSPN | | Proposed | |
|-------------------------------------|-------------------------------------|---|-------------------------|--------------------------|
| | OBU | RSU | OBU | RSU |
| Generating navigation service token | T_{mul} (by TA) | | T_{mul} (by TA) | |
| Master key request | $T_{sig}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

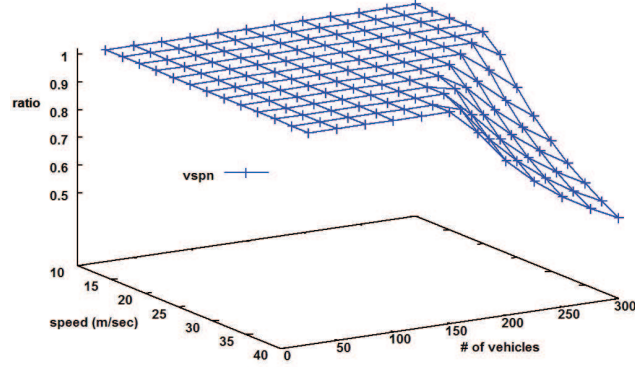
measured by the following formula where ρ is the probability for each vehicle in RSU's range to request navigation credential, and T_{crd} is the computational time to perform navigation credential request of Table 2. We estimated cryptographic overhead by using the pairing-based cryptography library of [23] on Pentium-III 1GHz machine to measure the processing time. The following results are obtained: $T_{mul} = 0.6ms$, $T_{par} = 4.5ms$, $T_{as-enc} = 1.2ms$.

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

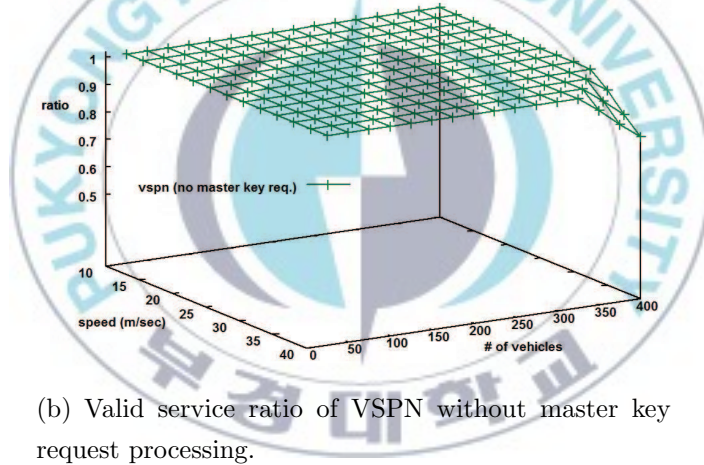
Figure 4.1 shows valid RSU's serving ratio for processing credential request

under VSPN and our protocol with different vehicle density and speed within $R_{rng}=1,000\text{m}$ and $\rho=0.8$. 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 4.1-(a) and 4.1-(b) respectively show the results for those cases, and 4.1-(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.

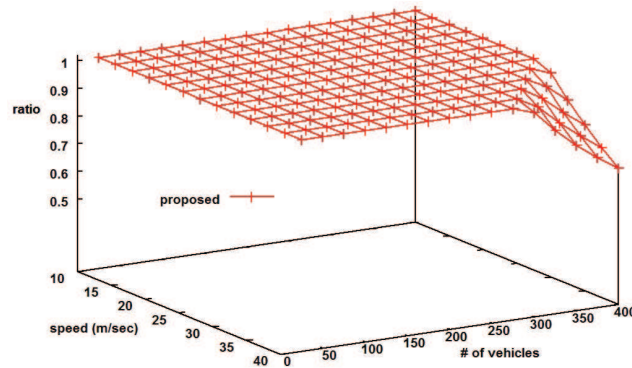




(a) Valid service ratio of VSPN including master key request processing.



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



(c) Valid service ratio of the proposed protocol

Figure 4.1: RSU's valid service ratio for processing navigation credential request.

Chapter 5. Conclusion

In this thesis, we proposed a secure and privacy-preserving vehicular cloud service that overcome the problems of previous works. It first address privacy preserving by designing anonymous credential based on concept of two person multisignature and identity based cryptographic schemes for mutual authentication between a vehicle and road side unit. We have provided the analysis to confirm the fulfillment of the security objectives and the efficiency of the proposed protocol. We evaluate the computational costs of the proposed protocol and show that it performs better than other protocol.

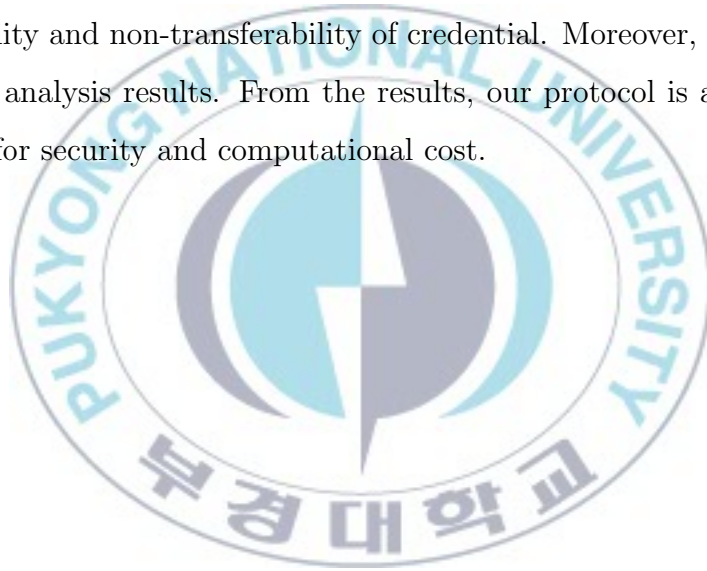
We conclude this thesis as summarizing and discussing the contents of each chapter.

In chapter 2, we briefly introduced a new concept, Vehicular cloud computing. The vehicular cloud computing concept is a further step to assemble the computational and situational consciousness of driver in public and the greater portion of the population. The focus of the vehicular cloud is to offer on demand solutions for unpredictable events in a proactive fashion. However, a more careful analysis reveals that many of the classic security challenges are exacerbated by the characteristic features of vehicular cloud computing to the point where they can be construed as vehicular cloud computing specific. Moreover, we discuss related work for privacy preserving navigation protocol for vehicular networks.

In chapter 3, we proposed a privacy-preserving vehicular cloud navigation service based on concept of two person multisignature and identity based cryp-

tographic schemes for mutual authentication between a vehicle and road side unit. The proposed protocol consist of three parts which are system setup, navigation credential request and navigation service request. In this chapter, we give a detailed explanation of the each operations.

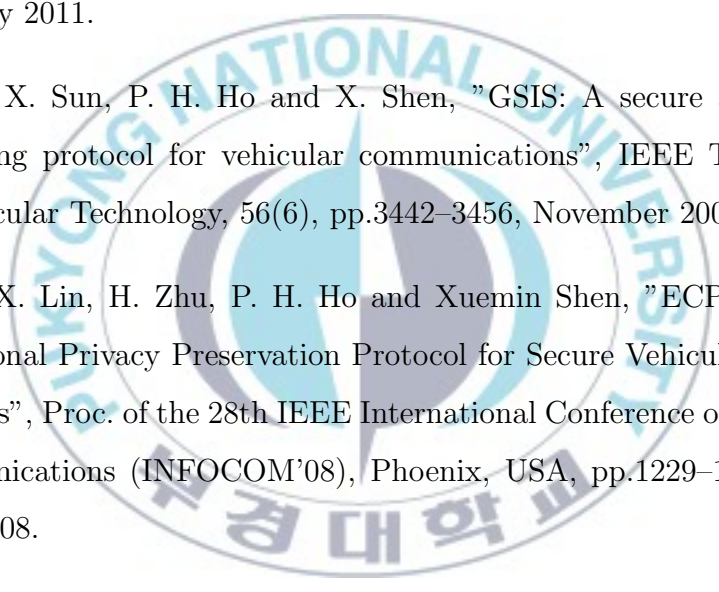
In chapter 4, we analyzed how the proposed protocol achieves the security requirements described in section 3.2. As mentioned before, our protocol can provide authentication, authorization, confidentiality, identity privacy preserving, traceability and non-transferability of credential. Moreover, we presented performance analysis results. From the results, our protocol is advantageous than VSPN for security and computational cost.



References

- [1] 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, 9(1), pp.1–30, February 2006.
- [2] K. Behrendt and K. Fodero, "The Perfect Time: An Examination of Time-Synchronization Techniques", Proc. 32rd Annual Western Protective Relay Conference, Spokane, USA, pp.1–18, Washington State University, October 2005.
- [3] D. Boneh, B. Lynn and H. Shacham, "Short Signatures from the Weil Pairing", 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, LNCS 2248, pp.514–532, Springer-Verlag, December 2001.
- [4] B. J. Chang, B. J. Huang and Ying-Hsin Liang, "Wireless Sensor Network-Based Adaptive Vehicle Navigation in Multihop-Relay WiMAX Networks", Proc. of the 22nd International Conference on Advanced Information Networking and Applications (AINA'08), Okinawa, Japan, pp.56–63, IEEE, March 2008.
- [5] C. L. Philip Chen, J. Zhou and Wei Zhao, "A Real-Time Vehicle Navigation Algorithm in Sensor Network Environments", IEEE Transactions on Intelligent Transportation Systems, 13(4), pp.1657–1666, December 2012.

- [6] L. Chen, Z. Cheng and N. P. Smart, "Identity-based Key Agreement Protocols From Pairings", *International Journal of Information Security*, 6(4), pp.213–241, July 2007.
- [7] T.W. Chim, S.M. Yiu, Lucas C.K. Hui, Victor O.K. Li, "VSPN: VANET-based Secure and Privacy-preserving Navigation, *IEEE Transactions on Computers*, 63(2), pp.510–524, August 2012.
- [8] US Federal Communication Commission. (2003 December), "Dedicated Short Range Communication Report and Order" [Online] Available: http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-03-324A1.pdf, [Nov 29, 2013].
- [9] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography", *Proc. of the 8th International Conference on the Theory and Application of Cryptology and Information Security*, Queenstown, New Zealand, LNCS 2501, pp.548–566, Springer-Verlag, December 2002.
- [10] M. Gerla, J. T. Weng and G. Pau, "Pics-On-Wheels: Photo Surveillance in the Vehicular Cloud", *Proc. of the International Conference on Computing, Networking and Communications*, San Diego, USA, pp.1123–1127, IEEE, January 2013.
- [11] D. He, C. Chen, J. Bu, S. Chan and Yan Zhang, "Security and efficiency in roaming services for wireless networks: challenges, approaches, and prospects", *IEEE Communications Magazine*, 51(2), pp.142–150, February 2013.

- 
- [12] D. Hughes and V. Shmatikov, "Information hiding, anonymity and privacy: a modular approach", *Journal of Computer Security*, 12(1), pp.3–36, January 2004.
- [13] J. H. Jeong, S. Guo, Y. Gu, T. He and David H.C. Du, "Trajectory-Based Data Forwarding for Light-Traffic Vehicular Ad Hoc Networks", *IEEE Transactions on Parallel and Distributed Systems*, 22(5), pp.743–757, May 2011.
- [14] 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*, 56(6), pp.3442–3456, November 2007.
- [15] R. Lu, X. Lin, H. Zhu, P. H. Ho and Xuemin Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications", *Proc. of the 28th IEEE International Conference on Computer Communications (INFOCOM'08)*, Phoenix, USA, pp.1229–1237, IEEE, April 2008.
- [16] R. Lu, X. Lin, H. Zhu and X. Shen, "SPARK: A New VANET-Based Smart Parking Scheme for Large Parking Lots", *Proc. of the 28th IEEE International Conference on Computer Communications (INFOCOM'09)*, Rio de Janeiro, Brazil, pp.1413–1421, IEEE, April 2009.
- [17] H. Mousannif, I. Khalil and H. A. Moatassime, "Cooperation as a Service in VANETs", *Journal of Universal Computer Science*, 17(8), pp.1202–1218, April 2011.

- [18] Y. H. 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*, 26(3), pp.785–800, May 2010.
- [19] 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*, 8(2), pp.295–307, April 2011.
- [20] C. Sur, Y. H. Park, K. Sakurai and K. H. Rhee, "Providing Secure Location-Aware Services for Cooperative Vehicular Ad Hoc Networks", *Journal of Internet Technology*, 13(4), pp.631–644, July 2012.
- [21] C. Tarnovsky. (2010 February), "Deconstructing a Secure Processor", [Online] Available: <https://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html>, [Nov 29, 2013]
- [22] Y. Yang, R. H. Deng and F. Bao, "Privacy-preserving rental services using one-show anonymous credentials", *Security and Communication Networks*, 2(6), pp.531–545, December 2009.
- [23] "Pairing-Based Cryptography Library", [Online] Available: <http://crypto.stanford.edu/pbc>, [Nov 29, 2013]