http://dx.doi.org/10.3745/KTCCS.2013.2.11.495

A Secure Protocol for Location-Aware Services in VANETs

Chul Sur[†] · Youngho Park[††] · Kyung Hyune Rhee[†††]

ABSTRACT

In this paper, we present an anonymous authentication and location assurance protocol for secure location-aware services over vehicular ad hoc networks (VANETs). In other to achieve our goal, we propose the notion of a location-aware signing key so as to strongly bind geographic location information to cryptographic function while providing conditional privacy preservation which is a desirable property for secure vehicular communications. Furthermore, the proposed protocol provides an efficient procedure based on hash chain technique for revocation checking to effectively alleviate communication and computational costs on vehicles in VANETs. Finally, we demonstrate comprehensive analysis to confirm the fulfillment of the security objectives, and the efficiency and effectiveness of the proposed protocol.

Keywords : Vehicular Ad Hoc Networks, Location-Aware Services, Anonymous Authentication, Location Information Assurance, Identity-Based Cryptography, Certificateless Aggregate Signature, Hash Chain

VANET에서 안전한 위치인지 서비스를 위한 보안 프로토콜

서 철[†] · 박 영 호[††] · 이 경 현[†††]

요 약

본 논문에서는 VANET 환경에서 핵심요소 기술로 각광받고 있는 위치인지 서비스의 안전성 및 신뢰성을 보장하기 위한 익명 인증 및 위치 정보 보증 프로토콜을 제안한다. 이를 위하여, 본 논문에서는 안전한 VANET 환경 구축을 위해 기 제안되었던 익명 인증 기술들과 차별화된 기술로써 위치정보를 암호학적 기법과 결합시켜 암호 기술의 기능과 특정 위치에 대한 연관성을 부여하고 이러한 관계를 암호학적으로 검증함으로써 위치정보에 대한 보증을 제공할 뿐만 아니라 운전자 및 차량에 대한 프라이버시 보호를 제공할 수 있는 위치인지 서명키와 이를 이용한 위치인지 서명 기술을 제안한다. 또한 제안 프로토콜은 VANET에서 차량들에 대한 통신 및 계산상 오버헤드를 경감시키기 위한 해쉬 체인에 기반한 효율적인 상태 검증 절차를 제공한다. 마지막으로, 시뮬레이션을 통하여 제안 프로토콜의 효율성 및 유효성을 검증한다.

키워드 : 차량 네트워크, 위치인지 서비스, 익명 인증, 위치정보 보증, 신원기반 암호, 무인증서기반 집합 서명, 해쉬 체인

1. 서 론

오늘날 IT 신기술을 이용한 다양한 IT융합 기술과 서비스가 등장하고 있으며, IT와 자동차 기술 또는 IT와 도로 교통 기술이 융합된 대표적인 서비스로 텔레매틱스와 지능형교통정보시스템이 생활 속에서 이용되고 있다. 이는 차량 네트워크로 알려진 VANETs(Vehicular ad hoc networks)을 근간으로 하고 있으며, DSRC(Dedicated short range communication)[1]라 불리는 근거리 무선 통신 방식을 이용하여 차량 탑재장치(On-board unit, OBU)를 장착한 차량 간(Vehicle-to-vehicle, V2V) 통신과 차량과 노변 인프라 개체(Roadsid unit, RSU) 간(Vehicle-to-infrastructure, V2I) 통신을 제공한다[2].

이러한 VANET 환경에서의 위치인지 서비스란 운전자 또는 차량의 요구에 따라 특정 도로 또는 지리적 영역에 대한 교통정보, 날씨, 주유소, 편의시설 등의 주요 시설물 정보와 같이 유용한 정보를 차량 통신을 기반으로 하여 수집하고 제공하기 위한 차량 협업 애플리케이션 서비스를 의미한다[3,4]. 이러한 차량 통신을 이용한 위치인지 서비스의 성공적인 구축을 위해서는 위치정보에 대한 신뢰성 보장이 핵심 요소로 사료되지만, 기존의 VANET 환경 하의 차량 통신을 위한 보안 기술에 대한 연구들은 운전자 및 차량에 대한 프라이버시 보호 및 차량 통신 메시지의 인증 서비스에 초점을 맞추고 있으며, 이러한 보안 서비스를 제공하기 위해 가명(Pseudonym) 식별자 및 그룹 서명 등의 전자서명 기법을 이용한 익명 인증 기술에 관한 연구가 활발히 진행되어지고

※ 이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.NRF-2013R1A1A4A01009848).
† 준 회 원 : 부경대학교 전자정보통신연구소 전임연구원
†† 정 회 원 : 부경대학교 전자정보통신연구소 전임연구원
††† 종신회원 : 부경대학교 IT융합응용공학과 교수
논문접수 : 2013년 10월 7일
심사완료 : 2013년 11월 7일
* Corresponding Author : Kyung Hyune Rhee(khrhee@pknu.ac.kr)

있다[5-7]. 그러나 일반적인 전자서명은 위치정보와는 무관하게 생성되므로 위치인지 서비스 메시지에 포함된 지리적 위치에 대한 신뢰성 보증을 제공하기에는 한계를 가진다. 한편, VANET에서 안전한 위치기반 라우팅 프로토콜을 이용한 이동 노드의 위치 검증 기법[8,9]이 소개되었지만, 이는 무선 통신에 참여하는 주변 노드들의 물리적 위치를 파악하기 위한 기법으로써 위치인지 서비스 관점에서의 위치정보 보증 기법과는 구별된다.

따라서, 본 논문에서는 차량 통신을 이용한 위치인지 서비스의 안전성 및 신뢰성을 보장하기 위한 새로운 익명 인증 및 위치정보 보증 프로토콜을 제안한다. 제안 프로토콜은 위치정보를 암호학적 기법과 결합시켜 암호 기술의 기능과 특정 위치에 대한 연관성을 부여하고 이러한 관계를 암호학적으로 검증함으로써 위치정보에 대한 보증을 제공할 뿐만 아니라 운전자 및 차량의 프라이버시 보호를 제공한다. 또한, 제안 프로토콜은 차량들에 대한 통신 및 계산상 오버헤드를 경감시키기 위한 해쉬 체인에 기반한 효율적인 상태 검증 절차를 제공한다. 이를 위하여, 기존의 차량 통신을 위한 보안 프로토콜들의 한계를 지적하고 안전한 위치인지 서비스를 위한 프라이버시 및 위치정보 보호 레벨을 새로이 정의한다. 이후 본 논문에서 제시한 안전한 위치인지 서비스를 위한 보안 요구사항에 따른 안전성 분석을 기술한다. 마지막으로, 제안 프로토콜의 효율성 및 유효성을 검증하기 위하여 유효 서비스율과 메시지 인증 처리율에 대한 시뮬레이션을 통한 성능 분석을 기술한다.

본 논문의 구성은 다음과 같다. 2장에서는 안전한 위치인지 서비스를 위한 보안 요구사항을 정의한 후, 3장에서 제안 시스템 모델과 익명 인증 및 위치정보 보증 프로토콜에 대하여 기술한다. 제안 프로토콜에 대한 안전성 및 성능 분석은 4장과 5장에서 각각 기술하며, 마지막으로 6장에서 결론을 맺는다.

2. 보안 요구사항

VANET 환경에서 차량의 이동경로 추적과 같은 프라이버시와 관련된 위협으로부터 안전하기 위해서는 OBU간 인증 단계 및 RSU와의 인증 단계에서 사용자의 신원정보 및 위치정보에 대한 익명성(Anonymity)이 만족되어야 한다. 또한, VANET 환경에서 통신 메시지에 대한 분쟁이 발생하였을 경우, 사법권 집행 등에 대해 신뢰기관을 통한 추적성(Traceability)을 제공하여야 한다. 이러한 이유로 인하여, VANET에서 통신 메시지의 신뢰성 보장 및 사용자의 프라이버시 보호를 위한 다수의 익명 인증 프로토콜들이 소개되었다[5-7].

그러나, 기 제안된 익명 인증 프로토콜들은 위치인지 서비스의 안전성과 신뢰성을 제공할 수 있는 위치정보에 대한 보증 기술을 고려하지 않고 있다. 따라서, 본 논문에서는 VANET 환경에서 핵심적인 요소기술인 위치인지 서비스의 안전성 및 신뢰성을 지원하기 위한 보안 요구사항으로써 위치정보 보증을 새로이 정의하고 이에 따른 프라이버시 및 위치정보 보호를 위한 보안 레벨을 아래 Table 1과 같이 정의한다.

Table 1. Security level for location-aware services

	Authentication	Privacy Protection	Traceability	Location Assurance
Level 1	○	○	X	X
Level 2	○	○	○	X
Level 3	○	○	○	○

- 인증 : 악의적인 공격자의 위장 공격(Impersonation attack) 등으로 발생 가능한 위협을 제거하기 위하여, 차량에 탑재되어 있는 OBU 및 RSU의 통신 메시지에 대한 인증이 가능해야 한다. 또한, OBU 및 RSU들은 임의의 OBU가 생성한 메시지를 위·변조 할 수 없어야 한다.
- 프라이버시 보호 : 사용자의 식별정보는 네트워크 내부의 메시지로부터 노출되지 않아야 한다. 이는 식별정보 노출로 인한 사용자의 프라이버시 위협을 보호하기 위해 기본적으로 제공되어야 하는 특성이다. 또한, 주변 차량들뿐만 아니라 RSU나 광범위한 도청자가 특정 메시지들로부터 특정 차량의 이동경로를 파악할 수 없어야 한다. 이는 사용자의 위치정보에 대한 프라이버시를 보호하기 위한 필수적인 특성이다.
- 추적성 : 통신 메시지에 대한 분쟁이 발생했을 경우, 신뢰기관은 분쟁 발생 근원지를 추적할 수 있어야 하며 분쟁 발생 차량의 실제 식별정보를 알 수 있어야한다. 이를 위하여 익명 인증 기법으로부터 차량의 실제 식별정보를 추적할 수 있는 메커니즘이 제공되어져야 한다.
- 위치정보 보증 : 위치인지 서비스의 신뢰성을 보장하기 위해서는 위치정보 서비스를 통해 교환되는 메시지에 명시된 실제 지리적 목표 지역을 통과하는 정당한 차량들에 의해 응답 메시지가 생성되었음을 보장해야 한다. 즉, 메시지 수신 차량에 대하여 수신 메시지가 실제 목표 지역에서 생성되었음을 검증할 수 있는 메커니즘을 제공해야 한다.

Table 1의 정의에 따라 VANET에서 안전한 위치인지 서비스 제공을 위해서는 프라이버시 및 위치정보 보호를 위한 보안 레벨 3을 만족해야 하지만, 기 제안된 연구들은 보안 레벨 1 혹은 레벨 2만을 제공한다. 따라서, 본 논문에서는 프라이버시 및 위치정보 보호를 위한 보안 레벨 3을 제공하는 익명 인증 및 위치정보 보증 프로토콜을 제안한다.

3. 제안 프로토콜

3.1 시스템 모델 및 표기법

제안 시스템 모델은 Trusted Authority(TA), RSU, OBU

로 구성되며, 각각의 구성요소는 다음과 같은 역할을 수행한다.

- TA : 광범위한 신뢰기관으로써 제안 시스템에 등록되는 모든 RSU와 OBU에 대하여 암호학적 비밀키를 발급하며, 초기등록과정에서 제공된 비밀키는 VANET에서 RSU와 OBU의 상호인증 및 위치인지 서명키 발급 프로토콜에 사용된다. 또한 논쟁이 발생 했을 경우, TA는 위치인지 서비스 메시지에 포함된 익명으로부터 서명문 생성자를 추적할 수 있다.
- RSU : 각 RSU는 노변 상에 고정된 인프라 개체로써 TA의 통제를 받으며, 안전한 위치인지 서비스에 참여를 원하는 차량들에게 위치인지 서명키를 발급한다. 이때, 각 위치정보는 유일한 도로 식별자로 구분될 수 있으므로, 위치인지 서명키는 각 도로의 도로 식별자로부터 생성된다. 또한, 각 RSU는 논쟁이 발생하였을 경우 논쟁상황 해결을 위하여 TA에게 자신이 저장하고 있는 정보를 제공한다.
- OBU : 차량에 장착된 단말 장치로써, 위치인지 서명키가 필요할 경우에 현재 위치에 있는 RSU에게 위치인지 서명키 요청 메시지를 전송한다. 만약 OBU가 유효한 차량에 부착된 장치라면, RSU로부터 위치인지 서명키를 발급받게 된다. OBU는 컴퓨팅과 통신기능, GPS 및 내비게이션 기능을 갖추고 있다.

본 논문에서 제안하는 프로토콜의 기술을 위하여 사용되어지는 표기들은 아래 Table 2와 같다.

Table 2. Notations

Notation	Description
$params$	public parameters
sk_i, pk_i	private/public key pair of entity i
ok_i, rk_j	identity-based secret keys for OBU_i and RSU_j, respectively
vk_j^n	root validation key for RSU_j
h	collision resistant one-way hash function
H_1, H_2, H_3	cryptographic hash functions
L_j	location information of RSU_j
$GK_{i,j}$	location-aware signing key of OBU_i issued from RSU_j
MAC_k	MAC function under the key k
Enc, Dec	symmetric encryption/decryption functions
PE, PD	public key encryption/decryption functions

본 논문에서 제안하는 안전한 위치인지 서비스를 위한 익명 인증 및 위치정보 보증 프로토콜은 “시스템 설정, OBU 및 RSU 등록, 위치인지 서명키 발급, 위치인지 서명 생성 및 검증” 단계들로 구성되며, 이를 위하여 무인증서 암호기반 집합 서명 기법[10], 신원기반 키 교환 기법[11], 해쉬 체인 기술[12,13]을 기반으로 하여 설계되었다. 제안 프로토콜의 각 단계에 대한 자세한 설명은 아래와 같다.

3.2 시스템 설정

TA는 제안 프로토콜에서 사용되는 공개 파라미터를 생성하기 위하여 아래와 같은 절차를 수행한다.

1. 보안 매개변수 ℓ를 입력 값으로 ℓ비트 소수 q를 선택하고, 위수 q를 갖는 군 (G_1, G_2)과 겹선형 페어링(Bilinear pairing) $e : G_1 \times G_1 \rightarrow G_2$을 생성한 후 임의의 생성자 $P \in G_1$를 선택한다.
2. 시스템 마스터 키로 임의의 $\alpha \in Z_q^*$를 선택하고, 공개키 $P_o = \alpha P$를 계산한다.
3. 암호학적 해쉬 함수들 $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : \{0,1\}^* \rightarrow G_1$, $H_3 : \{0,1\}^* \rightarrow G_1$과 충돌 회피 해쉬 함수 h를 선택하고, 키 유도 함수 KDF를 정의한다.
4. 암호학적으로 안전한 대칭키 암호화 알고리즘 Enc과 공개키 암호화 알고리즘 PE을 선택한 후, TA의 개인키/공개키 쌍 $< sk_T, pk_T >$을 생성한다.
4. 공개 파라미터는 아래와 같이 구성한다.
$params = \{G_1, G_2, e, P, P_0, pk_T, h, H_1, H_2, H_3, Enc, PE, KDF\}$

3.3 OBU 및 RSU 등록

시스템에 참여하는 모든 RSU와 OBU는 초기등록과정을 통하여 TA로부터 암호학적 키를 발급받는다. 이때, RSU의 신원기반 비밀키는 위치정보로부터 유도되며, OBU의 비밀키는 유효성 검증을 통과한 식별정보로부터 유도된다.

- OBU 등록 : 만약 등록 개체가 OBU_i라면 TA는 아래와 같은 절차를 수행한다.

1. OBU_i의 식별정보 ID_i에 대한 유효성 검증을 수행한 후, 유효성 검증을 통과한 식별정보 ID_i를 유효한 식별정보로써 안전한 저장소에 등록한다.
2. OBU_i의 암호학적 키로 $ok_i = \alpha H_1(ID_i)$를 계산하고 $< params, ok_i >$을 OBU_i에게 안전한 채널을 통하여 전송한다.

- RSU 등록 : 만약 등록 개체가 RSU_j라면 TA는 아래와 같은 절차를 수행한다.

1. RSU_j에 대한 상태 검증을 위한 임의의 비밀 값 vk_j을 선택하고 루트 검증키로 $vk_j^n = h^n(vk_j)$을 계산한다.
2. 위치정보 L_j를 이용하여 RSU_j의 암호학적 키 $rk_j = \alpha H_1(RSU_j \| vk_j^n \| L_j)$을 계산한다.
3. RSU_j에게 $< params, rk_j, vk_j^n >$을 발급한 후, $< RSU_j, L_j, vk_j >$을 안전한 저장소에 보관한다.

이후, RSU_j는 자신의 개인키로 $\lambda_j \in Z_q^*$를 선택하고 공개키로 $P_j = \lambda_j P$을 계산한다.

3.4 위치인지 서명키 발급

VANET에서 제공되는 안전한 위치인지 서비스에 참여하고자 하는 OBU_i는 자신이 통과하는 지리적 영역 L_j에 위치한 RSU_j로부터 상호인증 과정을 수행한 후 위치인지 서명키를 다음과 같은 절차를 통하여 발급받는다.

1. OBU_i는 임의의 $a \in Z_q^*$를 선택하고 $X = aP$와 $Q_i = H_1(ID_i)$을 계산한 후 $< X, Q_i >$를 RSU_j에게 위치인지 서명키 요청 메시지로 전송한다.
2. 위치인지 서명키 요청 메시지를 전송받은 RSU_j는 임의의 $b \in Z_q^*$을 선택하고 $Y = bP$를 계산한 후 메시지 인증을 위한 비밀 값 $k = e(bQ_i, P_0) \cdot e(rk_j, X)$를 계산하고 메시지 인증 코드 생성을 위한 비밀키 $k_0 = KDF(k \| 0)$을 생성한다. 이후 메시지 인증 코드 $\pi_j = MAC_{k_0}(RSU_j, Q_i, X, Y, vk_j^n, L_j)$를 생성한 후 OBU_i에게 $< RSU_j, Y, vk_j^n, L_j, \pi_j >$을 응답 메시지로 전송한다.
3. OBU_i는 메시지 인증을 위한 $k = e(ok_i, Y) \cdot e(aQ_j, P_0)$와 $k_0 = KDF(k \| 0)$을 계산한 후 $\pi_j = MAC_{k_0}(RSU_j, Q_i, X, Y, vk_j^n, L_j)$을 검증한다. 여기서, $Q_j = H_1(RSU_j \| vk_j^n \| L_j)$이다. 만약 메시지 인증 코드가 유효하다면, OBU_i는 타임스탬프 t_s를 선택하고 현 지리적 위치에 대한 위치인지 서비스에서 사용될 익명 $PID_i = PE_{pk_T}(ID_i \| t_s)$을 생성한다. 이후 메시지 인증코드 $\pi_i = MAC_{k_0}(PID_i, RSU_j, Q_i, X, Y, vk_j^n, L_j, t_s)$를 계산한 후 $< PID_i, t_s, \pi_i >$를 RSU_j에게 전송한다.
4. RSU_j는 t_s가 유효한 타임스탬프로 설정되어 있는지 확인한 후 메시지 인증코드 $\pi_i = MAC_{k_0}(ID_i, RSU_j, Q_i, X, Y, vk_j^n, L_j, t_s)$를 검증한다. 만약 모든 검증이 유효하다면, RSU_j는 OBU_i의 현재 상태 검증을 위하여 PID_i를 TA에게 전송한다. TA는 자신의 개인키를 이용하여 $ID_i \| t_s = PD_{sk_T}(PID_i)$를 계산한 후 t_s 시점에서 ID_i의 상태 검증을 수행한다. 만약 OBU_i가 유효한 차량이라면, RSU_j는 $X_{i,j} = H_1(PID_i \| L_j \| t)$를 생성하고 위치인지 서명키로 $GK_{i,j} = \lambda_j X_{i,j}$를 계산한 후 암호문 $C = Enc_{k_1}(GK_{i,j})$를 생성한다. 여기서, t는 현재 유효기간이며 $k_1 = KDF(k \| 1)$이다. 마지막으로 RSU_j는 OBU_i의 위치인지 서명키 $GK_{i,j}$와 TA로부터 전송받은 현재 검증키 vk_j^{n-t} 및 자신의 공개키 P_j에 대한 메시지 인증 코드 $\pi_j' = MAC_{k_0}(GK_{i,j}, vk_j^{n-t}, P_j)$를 생성한 후 $< C, vk_j^{n-t}, P_j, \pi_j' >$을 OBU_i에게 전송한다.
5. OBU_i는 $k_1 = KDF(k \| 1)$을 이용하여 C을 복호화한 후 $\pi_j' = MAC_{k_0}(GK_{i,j}, vk_j^{n-t}, P_j)$을 검증한다. 이후, 현재 유효기간 t와 검증식 $h^t(vk_j^{n-t}) = vk_j^n$을 통하여 RSU_j에 대한 상태 검증을 수행한 후 검증식을 만족하면, 임의의 $x_i \in Z_q^*$을 선택하여 자신의 서명키를 $sk_i = < GK_{i,j}, x_i >$로 설정하고 이에 대응하는 공개키로 $pk_i = x_i P$를 설정한다.

3.5 위치인지 서명 생성 및 검증

• 위치인지 서명 생성 : OBU_i는 안전한 위치인지 서비스를 위하여 사용되어지는 위치인지 서명을 자신의 서명키 $sk_i = < GK_{i,j}, x_i >$을 사용하여 아래와 같이 생성한다.

1. 위치인지 서명에 사용될 상태정보 $\Delta = \{L_j, t\}$를 생성하고 임의의 $r \in Z_q^*$을 선택한 후 $U = rP$을 계산한다.
2. $W = H_2(\Delta)$와 $S = H_3(\Delta \| m \| PID_i \| pk_i \| U)$를 생성한 후 $V = GK_{i,j} + x_i W + rS$를 계산한다. 여기서 m은 위치인지 서비스에서 사용되는 메시지이다.
3. 위치인지 서명으로 $\Sigma = (U, V)$을 설정한 후 메시지 수신자에게 전송한다.

• 위치인지 서명 검증 : 위치인지 메시지/서명 쌍 (m_i, Σ_i)을 전송받은 수신자는 아래와 같은 집합 검증 기법을 사용하여 위치인지 서명들을 검증한다.

1. $W = H_2(\Delta)$를 생성한 후 $X_{i,j} = H_1(PID_i \| L_j \| t)$와 $S_i = H_3(\Delta \| m_i \| PID_i \| pk_i \| U_i)$를 계산한다.
2. 아래의 검증식을 통하여 수신 받은 위치인지 서명들에 대한 집합 검증을 수행한다.

$$e(\sum_{i=1}^{n} V_i, P) = e(P_j, \sum_{i=1}^{n} X_{i,j}) e(W, \sum_{i=1}^{n} pk_i) \prod_{i=1}^{n} e(S_i, U_i)$$

4. 안전성 분석

본 장에서는 2장에서 정의한 보안 요구사항들에 대한 제안 프로토콜의 안전성을 분석한다.

• 인증 : 시스템에 참가하는 모든 개체들의 인증은 초기 등록과정에서 발급되는 신원기반 비밀키에 의하여 보장되어질 수 있다. 즉, 단지 유효한 rk을 소요하고 있는 RSU와 ok을 소유하고 있는 OBU만이 상호 인증을 과정을 수행할 수 있다. 또한 제안 프로토콜에서 각 위치인지 서명은 암호학적 증명 가능한 무인증서 암호기반 집합 서명 기법 [10]을 이용하여 생성되므로, 악의적인 공격자는 OBU가 생성한 위치인지 서비스 메시지를 위·변조할 수 없다.

• 프라이버시 보호 : 제안 프로토콜에서 위치인지 서비스 메시지의 송신자들과 수신자들은 각자가 소유하고 있는 익명 PID으로 식별되어진다. 그러나, $PID = PE_{pk_T}(ID \| t_s)$는 TA의 공개키로 암호화된 암호문이므로 TA를 제외한 누구도 차량의 실제 식별정보를 확인할 수 없다. 또한, 제안 프로토콜에서는 차량이 새로운 지리적 위치를 통과할 시 새로운 PID를 생성하여 사용되어지므로 이러한 PID들의 비연결성은 광범위한 도청

자가 다른 지역에서 수집한 메시지를 이용한 이동경로 추적 공격에 대한 안전성을 보장한다.

- 추적성 : 위치인지 서비스 메시지에 대한 분쟁이 발생했을 경우, 제안 프로토콜에서는 위치인지 서비스 메시지에 포함된 *PID*를 이용하여 이를 해결할 수 있다. 즉, $PID = PE_{pk_T}(ID \| t_s)$는 TA의 공개키로 암호화된 암호문이므로 분쟁의 소지가 있는 메시지로부터 *PID*를 추출하여 TA에게 제시하면, *PID*를 수신 받은 TA는 자신의 개인키로 *PID*를 복호화하여 분쟁상황에 대한 책임소재를 해결할 수 있다.
- 위치정보 보증 : 제안 프로토콜에서 위치인지 서비스의 신뢰성은 위치인지 서명키를 이용한 위치인지 서명에 의해서 보증된다. 각 차량이 소유하고 있는 위치인지 서명키는 발급받은 위치정보 L와 익명 *PID*을 유효기간 t에서 암호학적 바인딩을 이용하여 생성된다. 따라서, 제안 프로토콜은 위치정보 서비스를 통해 교환되는 메시지에 명시된 실제 지리적 목표 지역을 통과하는 정당한 차량들에 의해 응답 메시지가 생성되었음을 보장한다.

따라서, Table 1의 안전한 위치인지 서비스를 위한 보안 레벨 정의에 의해, 제안 프로토콜은 레벨 3 프라이버시 및 위치정보 보호를 제공한다.

또한, 각 RSU에 대한 해쉬 체인기반 상태 검증 메커니즘의 안전성은 다음과 같이 보증되어질 수 있다. 공격자가 유효기간 t 시점에 대응하는 RSU의 현재 검증키 vk^{n-t}를 위조하기 위해서는 RSU의 루트 검증키 vk^n의 $(n-t)$번째 해쉬 함수 $h()$의 역원을 계산해야 하지만 이는 현재 컴퓨팅 환경에서 계산상 실행 불가능하다.

5. 성능 분석

본 장에서는 RSU의 유효 서비스율 및 OBU의 메시지 인증 처리율 관점에서 제안 프로토콜과 기존의 효율적인 익명 인증 프로토콜인 ECPP[5]을 비교한다. 현실적인 비교를 위하여, 차수 $k=6$과 $|q|=160$ 비트의 MNT 타원곡선[14]을 고려하여 제안 프로토콜과 ECPP의 성능을 평가하였다. 제안 프로토콜과 ECPP에 대한 주요 암호 연산량은 아래 Table 3와 같다. 여기서, t_p는 겹선형 페어링 연산, t_m은 포인트 곱셈 연산, t_e는 공개키 암호 연산을 나타내며 암호학적 해쉬 함수와 같은 수행시간이 미미한 연산은 고려하지 않았다.

Table 3. Cryptographic operations for performance measures

	Description	ECPP	Proposed
T_{gen}	key generation	$6t_p+13t_m$	$2t_p+6t_m+1t_e$
T_{sig}	signature generation	$2t_m$	$4t_m$
T_{vrf}	signature verification	$3t_p+11t_m$	$4t_p$
T^n_{vrf}	n signature verification	$n(3t_p+11t_m)$	$(n+3)t_p$

5.1 RSU 유효 서비스율

RSU의 주요 연산은 통신 범위 R_{rng}내의 차량들에 대한 위치인지 서명키를 발급하는 것이므로, RSU의 성능은 차량 밀도(Density) d와 속도 v에 의존한다. 따라서, RSU의 유효 서비스율을 측정하기 위하여 본 논문에서는 [5]에서 소개한 분석 방법을 사용하였다: RSU의 유효 서비스율 S_{RSU}은 아래의 식과 같이 서비스 요청 횟수에 대한 실제 발급된 서명키의 비율로 측정될 수 있으며, ρ는 각각의 OBU가 위치인지 서명키 요청을 수행할 확률을 나타낸다.

$$S_{RSU} = \begin{cases} 1, & if \ \dfrac{R_{rng}}{T_{gen} \cdot \rho \cdot v \cdot d} \geq 1; \\ \dfrac{R_{rng}}{T_{gen} \cdot \rho \cdot v \cdot d}, & otherwise. \end{cases}$$

아래 Fig. 1은 통신 범위 $R_{rng}=300m$와 $\rho=0.8$ 환경에서 다양한 차량 밀도 및 속도에 따른 제안 프로토콜과 ECPP의 서명키 발급을 위한 RSU의 유효 서비스율을 보여주고 있으며, 성능 분석 결과 대부분의 현실적인 시나리오 상에서 위치인지 서명키 요청에 대하여 제안 프로토콜이 ECPP 보다 효율적임을 알 수 있다.

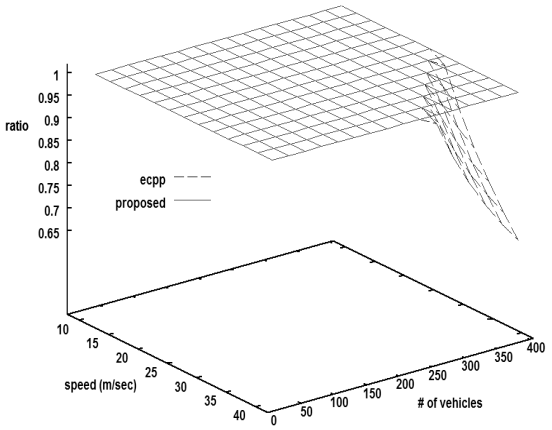


Fig. 1. RSU valid serving ratio for $\rho=0.8$

5.2 메시지 인증 처리율

VANET 환경 하에서 위치인지 서비스를 위한 시스템 성능은 각 차량들의 수신 메시지에 대한 인증 처리율로 평가되어질 수 있으며, 이는 각 수신 메시지에 포함된 서명을 검증하는데 소요되는 시간과 차량 간의 통신에 참여하는 주변 송신 차량의 수에 따라 결정될 수 있다. 만약 동일한 통신 범위내의 k(msg./second)의 메시지 처리율을 가진 n대의 차량들이 있다고 가정하자. 최악의 경우, 초당 $n_{msg}=n\times k$ 메시지들이 수신된다고 볼 수 있으며, 메시지 인증 처리율은 $1/(T_{vrf}\times n_{msg})$으로 측정되어질 수 있다.

아래 Fig. 2와 Fig. 3은 제안 프로토콜과 ECPP의 n_{msg}에 대한 서명 검증 시간과 다양한 차량 밀도 하에서의 유효 메

시지 처리율을 비교하여 각각 보여주고 있다. 또한, 제안 프로토콜은 다중 메시지들에 대한 집합 서명 검증을 사용하므로 본 논문에서는 집합 서명 검증과 개별 n_{msg} 메시지 검증의 비교를 수행하였다.

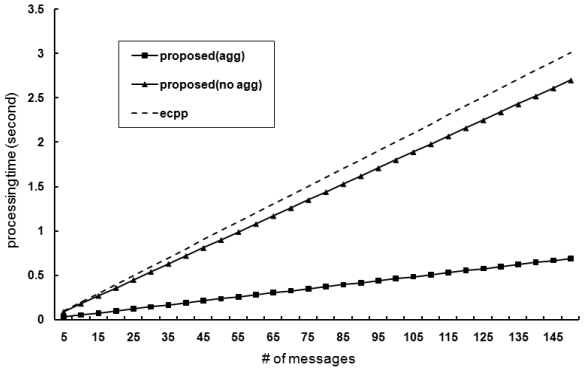


Fig. 2. Message verification time for n messages

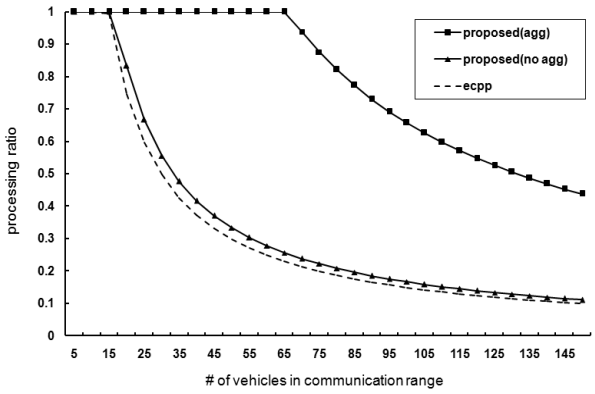


Fig. 3. Message verification ratio depending on the number of vehicles

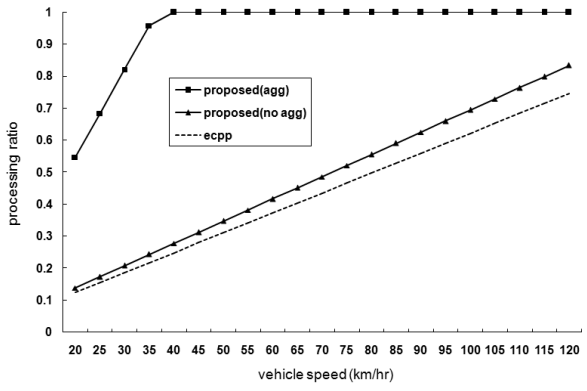


Fig. 4. Message verification ratio depending on vehicle speed in two-lane road

Fig. 4는 300m 통신 범위를 가지는 차량들이 2차선 도로상에서 균일하게 분포되어 있다고 가정하여 차량 속도에 따른 메시지 인증 처리율을 보여주고 있다. 위의 그림들의 결과와 같이 제안 프로토콜은 메시지 인증 처리율 관점에서 ECPP 보다 효율적임을 알 수 있다.

Table 4. Configuration for simulation

Parameter	Measures
road length	$4{,}600m \times 3{,}800m$ (city road) $5{,}000m$, 2-lane (highway)
vehicle density	$1-70$ in traffic flow(vehicle/km)
velocity	max. $20m/s$ (city road) max. $30m/s$ (highway)
radio range	$300m$ (nominal)
message interval	$300ms$
wireless protocol	802.11p

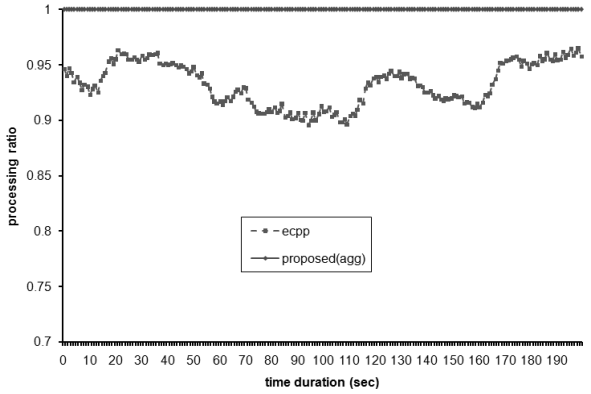


Fig. 5. Average message processing ratio in highway scenario

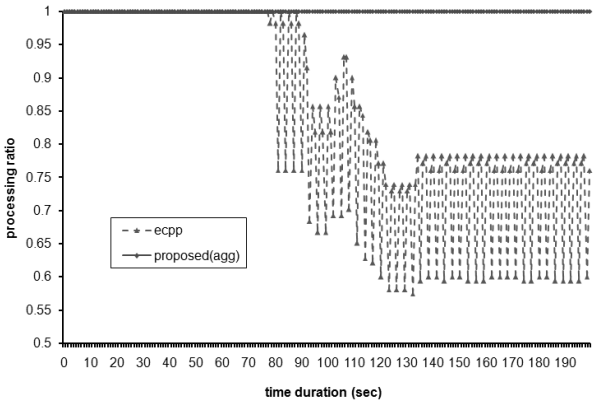


Fig. 6. Average message processing ratio in city road scenario

마지막으로, 현실적인 도로 환경에서의 제안 프로토콜의 성능 분석을 위하여, 본 논문에서는 TraNS[15]와 NS-2[16] 시뮬레이터를 이용한 시뮬레이션을 수행하였으며 시뮬레이션을 위한 구성은 Table 4와 같다. 시뮬레이션을 위한 차량의 밀도는 1에서 최대 70으로 설정하였으며, 도시도로 환경에서의 최대 속도는 20m/s, 고속도로 환경에서의 최대 속도는 30m/s로 설정하였다. 또한 각 차량은 DSRC[1]에 따라 300m 통신 범위 내에서 300ms 마다 정규적으로 위치인지 서비스를 위한 메시지를 전송한다고 가정하였다.

Fig. 5와 Fig. 6은 고속도로 환경과 도시도로 환경에서의 제안 프로토콜과 ECPP의 평균 메시지 처리율을 각각 보여주고 있다. 시뮬레이션의 결과를 통하여, 제안 프로토콜은 효과적으로 모든 메시지를 처리할 수 있으며 메시지 처리율 관점에서 ECPP 보다 효율적임을 알 수 있다.

6. 결 론

본 논문에서는 VANET 환경에서 위치인지 서비스의 안전성 및 신뢰성을 보장하기 위한 익명 인증 및 위치정보 보증 프로토콜을 제안하였다. 이를 위하여 안전한 위치인지 서비스를 위한 보안 레벨을 정의하고 차량의 프라이버시 보호뿐만 아니라 위치정보에 대한 암호학적 신뢰성을 보장할 수 있는 위치인지 서명 기술을 제안하였다. 또한 제안 프로토콜은 차량들에 대한 통신 및 계산상 오버헤드를 경감시키기 위한 해쉬 체인에 기반한 효율적인 상태 검증 절차를 제공한다. 결과적으로, 제안 프로토콜은 VANET 환경에서 안전한 위치인지 서비스의 구축을 위한 적절한 암호학적 도구로 활용될 수 있다.

참 고 문 헌

[1] Dedicated Short Range Communications (DSRC), Available: http://www.leearmstrong.com/dsrc/dsrchomeset.htm.

[2] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” *Journal of Computer Security*, Vol.15, No.1, pp.39-68, 2007.

[3] M. D. Dikaiakos, A. Florides, T. Nadeem, and L. Iftode, “Location-aware services over vehicular ad-hoc networks using car-to-car communication,” *IEEE Journal on Selected Areas in Communications*, Vol.25, No.8, pp.1590-1602, 2007.

[4] M. D. Dikaiakos, S. Iqbal, T. Nadeem, and L. Iftode, “VITP: An information transfer protocol for vehicular computing,” in *Proceedings of 2nd ACM Internationial Workshop on Vehicular Ad Hoc Networks*, 2005, pp.30-39.

[5] X. Lin, X. Sun, 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, 2007.

[6] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, “ECPP: Efficient conditional privacy preservation protocol for secure vehicle communications,” in *Proceedings of IEEE INFOCOM*, 2008, pp.1229-1237.

[7] C. D. Jung, C. Sur, Y. Park, and K. H. Rhee, “A robust and efficient anonymous authentication protocol in VANETs,” *Journal of Communications and Networks*, Vol.11, No.6, pp.607-614, 2009.

[8] V. Pathak, D. Yao, and L. Iftode, “Securing location aware services over VANET using geographical secure path routing,” in *Proceedings of IEEE International Conference on Vehicular Electronics and Safety*, 2008, pp.346-353.

[9] Z. Ren, W. Li, and Q. Yang, “Location verification for VANETs routing,” in *Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2009, pp.141-146.

[10] L. Zhang and F. Zhang, “A new certificateless aggregate signature scheme,” *Computer Communications*, Vol.32, Issue 6, pp.1079-1085, 2009.

[11] L. Chen, Z. Chen, and N. P. Smart, “Identity-based key agreement protocols from pairings,” *International Journal of Information Security*, Vol.6, No.4, pp.213-241, 2007.

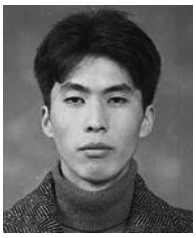
[12] S. Micali, “NOVOMODO: Scalable certificate validation and simplified PKI management,” in *Proceeding of 1st Annual PKI Research Workshop*, 2002, pp.15-25.

[13] C. Sur and K. H. Rhee, “An efficient authentication and simplified certificate status management for personal area networks,” in *Proceeding of APNOMS*, 2006, LNCS 4238, pp.273-282, 2006.

[14] Pairing-Based Cryptography Library, Available: http://crypto.stanford.edu/pbc.

[15] TraNS - Realistic Simulator for VANET, Available: http://trans.epfl.ch/.

[16] The Network Simulator - NS-2, Available: http://www.isi.edu/nsnam/ns/



서 철

e-mail : kahlil@pknu.ac.kr

2000년 부경대학교 전자계산학과(학사)

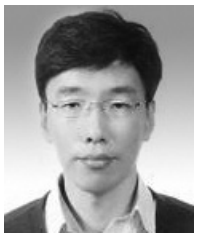
2004년 부경대학교 전자계산학과(석사)

2010년 부경대학교 전자계산학과(박사)

2010년~2011년 일본 큐슈대학 박사후 연구원

2012년~현 재 부경대학교 전자정보통신연구소 전임연구원

관심분야 : 공개키 암호, 암호 프로토콜, 애드 혹 네트워크 보안



박 영 호

e-mail : pyhoya@pknu.ac.kr

2000년 부경대학교 전자계산학과(학사)

2002년 부경대학교 전자계산학과(석사)

2006년 부경대학교 정보보호학과(박사)

2010년~현 재 부경대학교 전자정보통신연구소 전임연구원

관심분야 : 암호 프로토콜, 암호 응용, 애드 혹 네트워크 보안

이 경 현

e-mail : khrhee@pknu.ac.kr

1982년 경북대학교 수학교육과(학사)

1985년 한국과학기술원 응용수학과(석사)

1992년 한국과학기술원 수학과(박사)

1993년~현 재 부경대학교 IT융합응용 공학과 교수

관심분야 : 정보보호론, 공개키 암호, 신원기반 암호, 멀티미디어 정보보호, 그룹 키 관리