DOI: 10.3745/KIPSTC.2009.16C.5.589

VANET에서 다중 익명 인증서 기반 효율적인 익명 인증 프로토콜

정 채 덕[†] · 서 철[††] · 박 영 호[†††] · 이 경 현[††††]

요 약

최근까지 VANET 환경에서 차량의 익명성과 비연결성을 제공하기 위하여 제안된 익명 인증 프로토콜들은 신뢰기관이 차량에게 다수의 익명 인증서를 발급하거나, 차량과 RSU (Road-Side Unit)간의 상호인증 이후에 RSU가 차량에게 단기 (Short-time) 익명 인증서를 발급하였다. 하지만, 이러한 프로토콜들은 익명 인증서 생성 단계에서 신뢰기관을 비롯하여 차량 및 RSU의 높은 오버헤드를 발생시킨다. 따라서, 본 논문에서는 차량 및 RSU간의 한 번의 상호인증으로 RSU가 차량에게 다중 단기 익명 인증서를 발급하는 효율적인 익명 인증 프로토콜을 제안한다. 시뮬레이션을 통하여, RSU 서비스율 및 차량의 계산량 관점에서 기 제안되었던 가장 효율적인 익명 인증 프로토콜보다 효율적임을 보인다. 또한, 기 제안된 프로토콜들은 다수의 RSU들이 손상될 경우, 차량에 대한 비연결성과 추적성을 제공하지 못하는 반면 제안 프로토콜은 다수의 RSU가 손상되더라도 차량의 비연결성과 추적성을 제공한다.

키워드 : VANET (Vehicular Ad-hoc Network), 프라이버시 보호, 익명 인증, 다중 익명 인증서

An Efficient Anonymous Authentication Protocol Based on Multiple Anonymous Certificates in VANET

Chae Duk Jung[†] · Chul Sur[††] · Youngho Park[†††] · Kyung-Hyune Rhee[††††]

ABSTRACT

Until now, some protocols have been presented to provide vehicle's anonymity and unlinkability in VANET by means of issuing multiple anonymous certificates to each vehicle from the trust authority, or shot-time anonymous certificate to a vehicle after mutual authentication between a Roadside Unit (RSU) and the vehicle. However, these protocols have high overheads of the trust authority, RSUs and vehicles for generating anonymous certificate. In this paper, we propose an efficient anonymous authentication protocol, in which RSUs can issue multiple shot-time anonymous certificates to a vehicle to alleviate system overheads for mutual authentication between vehicles and RSUs. Several simulations are conducted to verify the efficiency of the proposed protocol in terms of RSU valid serve ratio and vehicle's computational costs. Moreover, the proposed protocol provides unlinkability and traceability when multiple RSUs are compromised, whereas previous protocols do not provide unlinkability and traceability.

Keywords : VANET(Vehicular Ad-hoc Network), Privacy Protection, Anonymous Authentication, Multiple Anonymous Certificates

1. 서 론

최근 전자제품의 급격한 가격하락과 함께 안전한 운전을 요구하는 사용자들이 증가하면서 자동차도로는 이동 Ad-hoc 네트워크 (MANET, Mobile Ad-hoc Network) 형태로 발전되었고 이러한 네트워크를 Vehicular Ad-hoc Network (VANET)라고 한다. 더불어, 안전한 VANET을 구성하기 위하여 VANET의 보안 구조에 관한 연구도 활발히 진행되고 있다 [5, 7, 12-15, 17, 18]. 최근에는 사용자의 프라이버시 보호에 관한 관심이 높아짐으로 인하여, 광범위한 도청 자료부터 차량의 이동경로 추척을 막기 위한 익명 인증 프로토콜들이 소개되었다 [3, 4, 8, 9, 16]. 하지만, 기 제안된 대부분의 익명 인증 메커니즘들은 RSU (Road Side Unit)의 인증 과정에서 많은 계산량을 요구하거나 차량에 부착된 OBU (On-Board Unit)가 손상되었을 시, 인증서 취소 문제 등으로 인하여 시스템 관리자 및 OBU의 높은 오버헤드를 요구한다.

※ 이 논문은 2008년도 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 연구되었음(KRF-2008-521-D00454).
† 준 회 원 : 부경대학교 정보보호학과 박사과정
†† 준 회 원 : 부경대학교 전자계산학과 박사과정
††† 준 회 원 : 부경대학교 정보보호학과 공학박사
†††† 종신회원 : 부경대학교 전자컴퓨터정보통신공학부 교수(교신저자)
논문접수 : 2009년 6월 22일
수 정 일 : 1차 2009년 7월 20일
심사완료 : 2009년 7월 28일

이러한 오버헤드를 줄이기 위해, R. Lu외 저자들은 VANET에서 효율적인 익명 인증서 관리를 위해 신원기반 암호 기법과 그룹 서명 기법을 기반한 익명 인증 프로토콜(ECPP, Efficient Conditional Privacy Preservation Protocol)을 제안하였다[9]. ECPP에서는 차량의 요청에 따라 주변 RSU와의 상호인증 절차를 수행한 이후에 RSU가 차량에게 단기(Short-time) 익명 인증서를 발급한다. 이러한, 단기 익명 인증서 검증 과정에서는 인증서 발급 개체인 RSU의 유효성 검증은 반드시 수행하여야 하지만, ECPP는 RSU가 손상되더라도 내부 정보를 알 수 없다는 가정을 설정함으로서 OBU와의 상호인증으로 RSU에 대한 유효성 검증을 생략하였다. ECPP의 익명 인증서 발급 절차는 다음과 같이 요약할 수 있다.

① OBU 익명 (RID) 및 RSU의 위치정보 기반의 상호 인증 수행
② OBU는 자신의 단기 서명키/검증키 쌍 (x / xP)을 생성하고, RSU에게 검증키 전송
③ RSU는 그룹 서명 기법을 이용하여 수신된 검증키에 대한 서명 값 (σ_{xP})을 생성하고, OBU에게 전송
④ 이후, OBU는 서명 값 (σ_{xP})을 검증키의 인증서로 사용

그러나, 공격자에 의해 손상된 장치의 내부 정보는 일반적으로 공격자가 획득할 수 있기 때문에, ECPP는 CRL (Certificate Revocation List) 등을 이용하여 발급된 익명 인증서를 검증하기 이전에 RSU의 유효성 검증 과정을 수행하여야 한다. 이로 인하여, ECPP는 손상된 RSU가 증가할수록 익명 인증서 검증과정에서 OBU의 계산상 오버헤드는 증가할 것으로 예상된다. 따라서, 단기 익명 인증서 생성 과정에서 효율적으로 RSU의 유효성을 검증할 수 있는 방법에 관한 연구가 필요하다.

한편, ECPP는 다수의 RSU들이 훼손될 경우에 OBU의 비연결성을 제공하지 못함으로서 OBU에 대한 이동경로 추적 공격이 가능하다. 더불어, ECPP는 분쟁상황에서 익명 인증서로부터 OBU의 식별정보를 추적하기 위하여 인증서를 발급해준 RSU와의 협력이 반드시 필요하다. 따라서, 인증서를 발급해준 RSU가 손상될 경우에는 OBU의 추적성을 제공하지 못한다. 따라서, 다수의 RSU들이 훼손되더라도 OBU의 비연결성 및 추적성을 제공하는 효율적인 익명 인증 프로토콜에 관한 연구가 필요하다.

따라서, 본 논문에서는 Universal 재암호화 기법[6], 그룹 서명 기법[2] 및 신원기반 키 일치 기법[19]을 이용하여 VANET에서 프라이버시 보호를 위한 효율적인 익명 인증 프로토콜을 제안한다. 제안 프로토콜은 다수의 RSU가 손상되더라도 차량의 비연결성과 추적성을 제공하며, 익명 인증서 검증단계에서 RSU의 유효성 검증 절차를 제거하였다. 또한, RSU 서비스율 및 OBU의 계산량 관점에서 제안 프로토콜이 기 제안된 가장 효율적인 익명 인증 프로토콜인 ECPP보다 효율적임을 증명한다. 비록 ECPP와 달리 그룹 관리자가 익명 인증서 발급 단계에서 관여하지만 현실성 있는 그룹 관리자의 오버헤드가 발생한다.

본 논문의 구성은 다음과 같다. 2장에서는 VANET에서 익명 인증 프로토콜의 보안 요구사항을 정의하고, 효율적인 익명 인증 프로토콜을 3장에서 제안한다. 또한, 4장에서는 제안 프로토콜의 안전성 및 효율성을 분석하며, 마지막으로 5장에서 결론을 맺는다.

2. 보안 요구사항

VANET에서 차량의 이동경로 추적과 같은 프라이버시와 관련된 위협으로부터 안전하기 위해서는 차량간 인증 단계 및 RSU와의 인증 단계에서 사용자의 익명성 (Anonymity) 및 비연결성 (Unlinkability)이 만족되어야 한다. 또한, VANET에서 통신 메시지에 대한 분쟁이 발생하였을 경우, 사법권 집행 등에 대해 신뢰기관을 통한 추적성 (Traceability)을 제공하여야 한다. 이러한 이유로 인하여, R. Lu외 저자들은 VANET에서 프라이버시 보호 레벨을 정의하였지만 [9], 다수의 RSU 손상을 고려하지 않았다. 따라서, 본 논문에서 다수의 RSU의 손상을 고려한 VANET에서 새로운 프라이버시 보호 레벨을 아래 <표 1>과 같이 정의한다.

- **인증** : 악의적인 공격자의 위장 공격 (Impersonation attack)등으로 발생 가능한 위협을 제거하기 위하여, OBU 및 RSU의 통신 메시지에 대한 인증이 가능해야 한다. 또한, 다수의 RSU가 손상되더라도 OBU 및 RSU들은 임의의 OBU가 생성한 메시지를 위·변조 할 수 없어야 한다.
- **익명성** : 사용자의 식별정보는 네트워크 내부의 메시지로부터 노출되지 않아야 한다. 이는 식별정보 노출로 인한 사용자의 프라이버시 위협을 보호하기 위해 기본적으로 제공되어야 하는 특성이다. 또한, 익명 인증서를 발급한 RSU 또는 다수의 RSU들이 손상되더라도 익명 인증서로부터 사용자의 식별정보를 추출할 수 없어야 한다.
- **비연결성** : 주변 차량들뿐만 아니라 RSU나 광범위한 도청자가 특정 메시지들로부터 특정 차량의 이동경로를 파악할 수 없어야 한다. 이는 사용자의 위치에 대한 프라이버시를 보호하기 위한 특성으로, 비연결성을 만족하기 위하여 각 차량들은 주기적으로 익명 인증서를 바꿔야 한다. 또한, 익명 인증서를 발급한 다수의 RSU들

〈표 1〉 프라이버시 보호 레벨

	인증	익명성	비연결성	추적성
레벨 1	○	○	X	X
레벨 2	○	○	○	X
레벨 3	○	○	○	○

이 손상되더라도 각 익명 인증서들 간의 연결성을 추적할 수 없어야 한다.

- **추적성** : 통신 메시지에 대한 분쟁이 발생했을 경우, 신뢰기관은 분쟁 발생 근원지를 추적할 수 있어야 하며, 분쟁 발생 차량의 실제 식별정보를 알 수 있어야한다. 또한, 분쟁의 원인이 된 익명 인증서 발급자인 RSU가 손상되더라도 인증서로부터 차량 또는 운전자의 식별정보를 추적할 수 있어야 한다.

차량의 추적성을 제공하기 위하여, ECPP는 각 RSU들이 차량의 장기 (Long-term) 익명을 저장한다. 이로 인하여, 다수의 RSU들이 손상될 경우에 각 RSU들이 저장하고 있는 장기 익명을 이용하여 익명 차량에 대한 이동경로를 추적할 수 있다. 비록, 익명 차량에 대한 이동경로 추적이지만, 프라이버시 보호 관점에서는 이것 또한 위협 요소로 분류된다. 한편, 분쟁 상황에서 ECPP는 인증서 발급자인 RSU를 통하여 차량의 식별정보를 추적하기 때문에, 손상된 RSU가 발급한 인증서에 대한 추적은 불가능하다. 따라서, (표 1)의 프라이버시 보호 레벨 정의에 의하면, ECPP는 *레벨 1 프라이버시*를 제공한다.

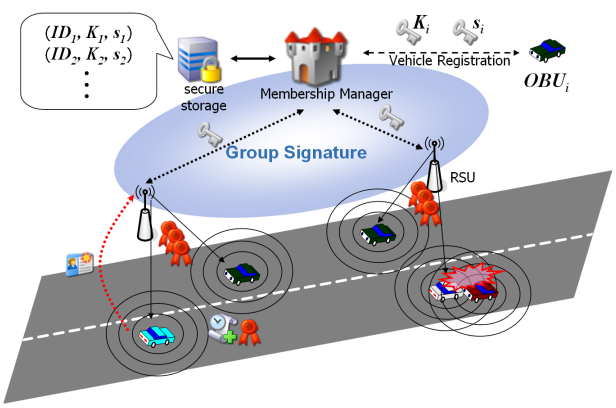
본 논문에서는, 단기 익명 인증서 생성 단계에서 기 제안된 가장 효율적인 프로토콜인 ECPP 보다 RSU 서비스율 및 차량의 계산량 관점에서 효율적며, *레벨 3 프라이버시*를 제공하는 익명 인증 프로토콜을 제안한다.

3. 다중 익명 인증서 기반 효율적인 익명 인증 프로토콜

3.1 시스템 모델 및 표기법

제안 시스템 모델은 (그림 1)과 같으며, 각 객체들의 기능 및 역할은 아래와 같다.

- **그룹 관리자** : 광범위한 신뢰기관으로서 합법적인 RSU에 대하여 그룹 서명키 및 비밀키를 발급하고, 정당한 OBU에게 MAC 키 및 비밀키를 발급한다. 이후, 논쟁이 발생 했을 경우에 그룹 관리자는 인증서에 포함된 익명으로부터 서명문 생성자를 추적한다.
- **RSU** : 각 RSU는 그룹 관리자에 소속되며, OBU로부터 익명 인증서 발급 요청 메시지를 수신했을 경우에 그룹 관리자와 협력하여 OBU의 유효성을 검증한다. OBU가 정당한 사용자라면, RSU는 Universal 재암호화 기법 및 그룹 서명 기법을 이용하여 OBU에게 다중 익명 인증서를 발급하다.
- **OBU** : 차량에 부착된 장치로서, 익명 인증서가 필요할 경우에 인증서 발급에 필요한 메시지를 생성하여, 가장 가까이에 있는 RSU에게 생성한 메시지를 전송한다. 만약 OBU가 유효한 차량에 부착된 장치라면, RSU로부터 다중 익명 인증서를 발급받게 된다. OBU는 발급받은 익명 인증서를 이용하여 주기적으로 안전 메시지 (Safety Message)를 생성하여 브로드캐스트 형태로 전송한다.



(그림 1) 시스템 모델

제안 프로토콜의 가정사항은 다음과 같다.

- 각 OBU는 유일한 식별정보 (ELP, Electronic License Plate)를 가지고 있다.
- 각 OBU는 0.3초마다 안전 메시지를 브로드캐스트 형태로 전송한다.
- 각 OBU는 익명 인증서를 대략 1분마다 갱신한다 [13].

제안 프로토콜의 표기법은 <표 2>와 같다.

〈표 2〉 표기법

표 기	의 미
GS_{mk}	그룹 서명의 마스터 키
GS_{pk}	그룹 서명의 공개키
GS_{params}	그룹 서명의 시스템 변수
sk_{MM}, pk_{MM}	그룹 관리자의 개인키/공개키 쌍
H, H_0	암호학적 해쉬 함수
K_i	OBU_i의 MAC 키
ID_i	개체 i의 식별정보 (OBU: ELP, RSU: 위치정보)
ID'_i	OBU_i의 익명 (Pseudonym)
$ID'_{i,*}$	OBU_i의 단기 익명
$Cert_{i,*}$	OBU_i의 단기 익명 인증서
s_i	ID_i의 장기 비밀키
$s_{i,j}$	ID_i와 ID_j간의 세션 (Session) 키
$sk_{i,*}, pk_{i,*}$	OBU_i의 단기 개인키/공개키 쌍
t	단기 익명 인증서의 유효 기간
$H_K()$	키 K에 대한 메시지 인증 코드
$GSig()$	서명 서명 알고리즘
$E(), D()$	Universal 재암호화 기술의 암호화/복호화 알고리즘
$Re()$	Universal 재암호화 기술의 재암호화 알고리즘
$SE(), SD()$	대칭키 기반 암호화/복호화 알고리즘

3.2 제안 프로토콜

본 논문에서 제안하는 효율적인 익명 인증 프로토콜은 "설정, OBU 등록, RSU 등록, 다중 익명 인증서 생성, 메시지 인증, OBU 식별정보 추적" 단계들로 구성되며 각 단계에 대한 자세한 설명은 아래와 같다.

[설정] 그룹 관리자는 k-bit의 임의의 소수 p를 선택하고, 위수가 p인 순환군 G_1과 G_2를 설정한다. 또한, 각 순환군 G_1과 G_2에 대한 생성자 (Generator) g_1과 g_2, Bilinear pairing $e: G_1 \times G_2 \rightarrow G_T$를 선택한다. 이후, 그룹 관리자는 임의의 $GS_{mk} = \gamma \in Z_p^*$에 대한 $GS_{pk} = g_2^{\gamma}$를 계산하고, 암호학적 해쉬 함수 $H: \{0,1\}^* \rightarrow Z_p$와 $H_0: \{0,1\}^* \rightarrow G_2^2$를 선택한다. 그룹 서명의 시스템 변수 GS_{params}는 $(G_1, G_2, G_T, e, p, g_1, g_2, H, H_0, GS_{pk})$으로 설정한다.

또한, 신원기반 키 일치 프로토콜[19]을 수행하기 위하여, 그룹 관리자는 각 $(p_i - 1)/2$가 홀수이며 서로소 관계인 소수 p_1, p_2, p_3와 p_4를 선택하고 $N = p_1 \cdot p_2 \cdot p_3 \cdot p_4$를 계산한다. 이후, 임의의 비밀 곱셈요소 $\alpha \in Z_{\phi(n)}^*$을 선택한다(여기서, $\phi()$은 오일러 Totient 함수이다). 마지막으로, Universal 재암호화 기법 [6]에 기반하여 개인키 sk_{MM}와 공개키 $pk_{MM} = g_3^{sk_{MM}}$를 생성한다(여기서, g_3는 Z_q의 생성자이다).

[OBU 등록] 그룹 관리자는 OBU_i에 대하여, 임의의 MAC 키 K_i를 선택하고 장기 비밀키 $s_i = \alpha \log_{g_4}(ID_i^2) \pmod{\phi(n)}$를 계산한다(여기서, g_4는 $GF(p_j)$의 원시근이다, $1 \leq j \leq 4$). 이후, 그룹 관리자는 OBU_i에게 (K_i, s_i)를 안전한 채널을 통하여 전송하고, (ID_i, K_i, s_i)를 안전한 저장소에 보관한다.

[RSU 등록] 그룹 서명 기법[2]에 따라, 그룹 관리자는 $\gamma + x_j \neq 0$을 만족하는 임의의 $x_j \in Z_p^*$를 선택하고 $A_j = g_1^{1/\gamma + x_j}$를 생성한다. 이후, 그룹 관리자는 $s_i = \alpha \log_{g_4}(ID_j^2) \pmod{\phi(n)}$를 계산하여, RSU_j에게 $((A_j, x_j), s_j)$를 안전한 채널을 통하여 전송한다.

[다중 익명 인증서 생성] OBU_i는 익명 인증서가 필요할 경우에 다음과 같은 절차를 통하여 새로운 익명 ID'_i, 다중 서명키 쌍을 생성한다.

1) 새로운 익명 $ID'_i = E_{pk_{MM}}(ID_i)$ 계산
2) 인증서 유효기간 t 설정
3) n개의 서명키 $sk_1, ..., sk_n$ 및 각 서명키에 대응하는 공개키 $PK = \{pk_1, ..., pk_n\}$ 계산 (단, 각 서명키/공개키 쌍들은 메시지 인증 단계에서 사용하는 서명 알고리즘(예, ECDSA)에 기반하여 생성된다.)

또한, RSU_j에 대한 세션키 $s_{i,j} = (ID_j^2)^{s_i h(t \| K_i)}$를 설정하고, 공개키 목록에 대한 암호문 $PK' = SE_{s_{i,j}}(PK)$을 계산한다(여기서, $h()$는 임의의 암호학적 해쉬 함수이다). 마지막으로 $MAC_{ID'_i} = H_{K_i}(ID'_i \| PK' \| t)$을 생성하고, RSU_j에게 $(ID'_i, PK', t, MAC_{ID'_i})$를 전송한다.

$$OBU_i \rightarrow RSU_j: \ ID'_i, PK', t, MAC_{ID'_i}$$

이후, RSU_j는 수신된 메시지의 t가 유효한 단기 기간으로 설정되어 있는지 확인한 후, OBU_i를 인증하기 위하여 $(ID'_i, PK', t, MAC_{ID'_i})$를 그룹 관리자에게 전송한다. 그룹 관리자는 RSU_j가 유효한 RSU라면 개인키를 이용하여 ID'_i를 복호화하여 OBU_i의 식별정보를 추출하고, 저장소에 보관된 K_i를 이용하여 $MAC_{ID'_i}$를 검증한다. $MAC_{ID'_i}$이 유효하고 OBU_i가 정당한 차량이면, 그룹 관리자는 RSU에게 부분 세션키 $g_4^{v \cdot s_i \cdot h(t \| K_i)}$를 계산하여 RSU_j에게 발급한다 (여기서, $v \equiv \alpha^{-1} (\bmod \phi(N))$). RSU_j는 부분 세션키와 자신의 장기 비밀키 s_j를 이용하여 세션키 $s_{i,j} = (g_4^{v \cdot s_i \cdot h(t \| K_i)})^{s_j}$를 계산하여, 암호화된 공개키 목록을 복호화한다. 또한, 아래와 같이 Universal 재암호화 기법을 이용하여 다중 익명 $ID'_{i,1}, ..., ID'_{i,n}$을 생성한다.

$$ID'_{i,1} = Re(ID'_i), ..., ID'_{i,n} = Re(ID'_i)$$

RSU_j는 각 익명 $ID'_{i,*}$과 공개키 $pk_{i,*}$에 대하여 그룹 서명 알고리즘 [2]를 이용하여 그룹 서명문 $\sigma_{i,*} = GSig(ID'_{i,*} \| pk_{i,*} \| t)$를 계산하고, 각 공개키에 대한 익명 인증서 $Cert_{i,*} = [ID'_{i,*}, pk_{i,*}, t, \sigma_{i,*}]$를 생성한다. 이후, 다중 익명 인증서를 세션키 $s_{i,j}$로 암호화하여 OBU_i에게 전송한다.

$$RSU_j \rightarrow OBU_i: \ CERT = SE_{s_{i,j}}(Cert_{i,1}, ..., Cert_{i,n})$$

OBU_i는 수신된 메시지를 복호화하여 다중 익명 인증서를 획득한다. 이후, 각 인증서에 포함된 공개키들이 자신이 생성한 공개키 목록과 동일한지 확인하고, 각 인증서에 포함된 서명들을 그룹 공개키 GS_{pk}를 이용하여 검증한다. 만약, 동일한 공개키 목록을 가지는 유효한 인증서들이면, OBU_i는 발급받은 다중 인증서들을 채택한다.

[메시지 인증] OBU_i는 주기적으로 수집한 교통정보 M과 공개키기반 서명 기술 (예, ECDSA)과 서명키 sk_i를 이용하여 교통정보에 대한 서명문 σ_M을 생성한다. 이후, 메시지, 익명, 인증서 및 서명문을 브로드캐스트 형태로 전송한다.

$$OBU_i \rightarrow * : M, Cert_{i,*}, \sigma_M$$

수신자들은 $Cert_{i,*}$를 검증하고, 유효한 인증서라면 $Cert_{i,*}$에 포함된 공개키를 이용하여 서명문 σ_M을 검증한다. 서명문이 유효하면, 수신자는 교통정보 M을 채택한다.

[OBU 식별정보 추적] 분쟁상황이 발생했을 경우, 그룹 관리자는 분쟁의 원인이 된 메시지에 포함된 익명 인증서의 익명 $ID'_{i,l}$을 그룹 관리자 개인키로 복호화하여 메시지 생성자의 식별정보 ID_i를 출력한다.

4. 분 석

4.1 안전성

2장에서 소개한 보안 요구사항들에 대한 제안 프로토콜의 분석은 다음과 같다.

- **인증** : 제안 프로토콜에서 각 교통정보에 대한 메시지는 디지털 서명 기법(예, ECDSA)에 기반한 서명문을 포함하기 때문에, 악의적인 공격자는 OBU가 발급한 교통정보 메시지를 위·변조 할 수 없다.
- **익명성** : Universal 재암호화 기법은 암호화에 사용된 공개키 및 암호문의 특성을 유지하면서 새로운 암호문을 생성한다. 따라서, 각 익명들은 OBU의 식별정보를 그룹 관리자의 공개키로 암호화한 형태로 구성되기 때문에, 그룹 관리자외의 개체들은 익명으로부터 실제 식별정보를 추출할 수 없다.
- **비연결성** : Universal 재암호화 기법의 주요 특징은 암호문 및 재암호문들 간의 비연결성을 제공한다는 것이다. 따라서, 제안 프로토콜에서 OBU들은 자신들의 인증을 위한 익명들을 Universal 재암호화 기법의 재암호화 알고리즘으로 생성하기 때문에, 다수의 RSU가 훼손되더라도 OBU의 비연결성을 제공한다.
- **추적성** : 다중 익명 인증서에 포함된 익명들은 OBU의 식별정보를 그룹 관리자의 공개키로 암호화된 암호문이다 (Universal 재암호문은 입력된 암호문의 평문 및 암호화 키 속성을 유지함). 따라서, 그룹 관리자는 익명 인증서 발급자인 RSU의 도움 없이 익명 인증서에서 실제 식별정보를 추출할 수 있다. 따라서, 제안 프로토콜은 RSU가 손상되더라도 OBU에 대한 추적성을 제공한다.

따라서, <표 1>의 프라이버시 보호 레벨 정의에 의해, 제안 프로토콜은 *레벨 3 프라이버시*를 제공한다.

4.2 효율성

본 장에서는 단기 익명 인증서 생성 단계에서 RSU 서비스율 및 OBU 계산량 관점에서 제안 프로토콜과 가장 효율적인 익명 인증 프로토콜인 ECPP을 비교한다. 현실적인 비교를 위하여, 80-bit 보안 레벨을 고려하였다. 즉, 타원곡선의 차수(Degree) $k=6$, $|G_1|=160$ bits 및 $|q|=1024$ bits로 설정하였으며, Pentium IV 3.0 기반 주요 암호 연산에 대한 소요되는 시간은 아래 <표 3>과 같다.

위의 <표 3>에 의하여, 제안 프로토콜과 ECPP의 각 단계에서 소요되는 연산 시간은 <표 4>와 같다.

제안 프로토콜과 ECPP의 RSU 서비스율의 정의는 아래와 같이 [9]에서 소개한 RSU 서비스율 측정 방법에 기반하였다.

$$RSU \text{ 서비스율} = \begin{cases} 1 & \text{만약 } \dfrac{R_{range}}{T_K \cdot \rho_n \cdot v \cdot d} \geq 1; \\ \dfrac{R_{range}}{T_K \cdot \rho_n \cdot v \cdot d} & \text{그 외.} \end{cases}$$

여기서, R_{range}는 RSU의 통신범위, T_K는 n개의 인증서를 생성하는데 소요되는 시간, ρ_n은 n개의 인증서를 요청할 최대 확률, v는 차량의 평균 속도이며, d는 RSU 통신범위에 있는 차량의 수이다.

위의 RSU 서비스율 식에 기반하여 제안 프로토콜 및 ECPP의 RSU 서비스율은 아래 (그림 2)와 같다.

위 그림에서 보듯이, RSU 서비스율 관점에서 가장 효율적인 익명 인증 프로토콜인 ECPP 보다 본 논문에서 제안한 다중 익명 인증서 발급 프로토콜이 효율적임을 알 수 있다.

또한, ECPP 및 제안 프로토콜에서 n개의 단기 익명 인증서를 생성하기 위한 OUB 계산량 정의는 및 OBU의 계산량 비교는 (그림 3)과 같으며, 제안 프로토콜은 RSU 유효성 검증을 요구하지 않기 때문에 N_R을 고려하지 않았다.

OBU 계산량 = n개의 인증서 발급 시간 + n개의 인증서 검증 시간 + RSU 유효성 검사 시간

(그림 3)과 같이, 단기 익명 인증서 생성 과정에서 손상된 RSU가 증가 할수록 제안 프로토콜이 ECPP 보다 OBU 계산량 관점에서 효율적임을 알 수 있다.

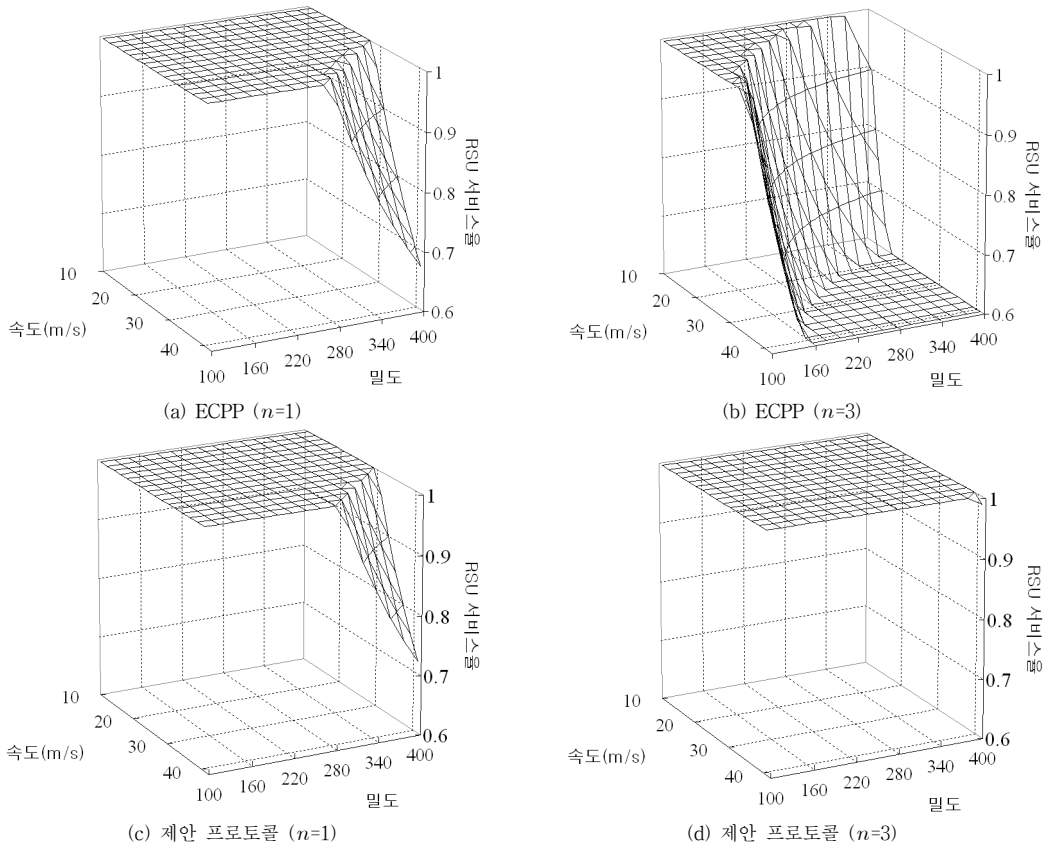
마지막으로, 제안 프로토콜은 ECPP와 달리 그룹 관리자의 참여를 요구한다. 하지만 아래 (그림 4)와 같이 n이 증

〈표 3〉 주요 암호 연산 시간

암호 연산	계산 시간(ms, millisecond)
Bilinear pairing e 연산	4.5
G_1상에서 곱셈 연산	0.6
Z_q상에서 지수승 연산	2.1

〈표 4〉 제안 프로토콜과 ECPP의 연산 시간 (N_R은 손상된 RSU 수)

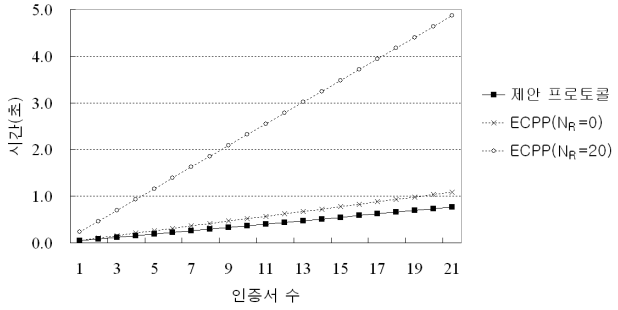
단계	ECPP	제안 프로토콜
n개의 인증서 발급 단계	$34.8n\ ms$	$12.6+18.6n\ ms$
n개의 인증서 검증 단계	$17.1n\ ms$	$17.1n\ ms$
RSU 유효성 검증 단계	$9N_R\ ms$	없음



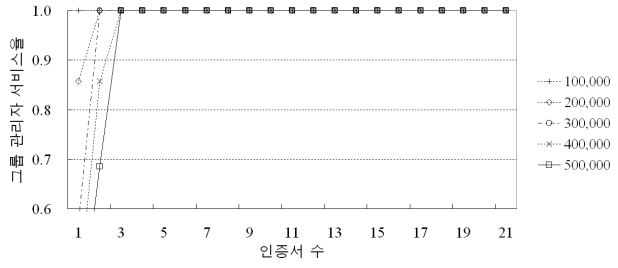
(a) ECPP (n=1) (b) ECPP (n=3)

(c) 제안 프로토콜 (n=1) (d) 제안 프로토콜 (n=3)

(그림 2) 제안 프로토콜과 ECPP의 RSU 서비스율 (여기서, n은 요청하는 인증서 수)



(그림 3) ECPP 및 제안 프로토콜의 OBU 계산량 비교



(그림 4) 차량 수에 대한 그룹 관리자의 서비스율

가 할수록 그룹 관리자는 대부분의 경우에서 100% 서비스를 제공하는 것을 알 수 있다.

결론적으로, (그림 2)와 (그림 4)를 통하여 제안 프로토콜은 충분한 현실성을 가지고 있음을 알 수 있으며, 비록 그룹 관리자가 익명 인증서 발급 단계에서 참여하지만 대부분의 교통 상황에서 충분한 서비스를 제공하는 것을 알 수 있다. 또한, 제안 프로토콜이 기 제안된 효율적인 익명 인증서 발급 프로토콜인 ECPP보다 RSU 서비스율 및 OBU 계산량 관점에서 효율적임을 입증하였다.

5. 결 론

본 논문에서는 Universal 재암호화 기법[6], 신원기반 키 일치 기법[19]과 그룹 서명 기법[2]을 이용하여 VANET에서 프라이버시 보호를 위한 효율적인 익명 인증 프로토콜을 소개하였다. 기 제안된 익명 인증서 발급 프로토콜들과는 다르게, 제안 프로토콜에서는 RSU가 OBU에게 다중 익명 인증서를 발급한다. 이로 인하여, 단기 익명 인증서 생성을 위한 RSU 및 OBU의 계산상 오버헤드를 감소시켰다. 게다가, 제안 프로토콜은 익명 인증서 발급단계에서 OBU 인증을 위한 익명이 각 RSU마다 바뀜으로서, 다수의 RSU가 손상되더라도 OBU의 비연결성을 제공한다. 더불어, 제안 프로토콜에서 그룹 관리자는 RSU와의 협력 없이 서명문 생성자의 식별정보를 추출할 수 있음으로서, RSU가 손상되더라도 분쟁상황에서 사용자 식별정보 추적이 가능하다.

참 고 문 헌

[1] J. Blum and A. Eskandarian, “The threat of intelligent collisions,” IT Professional, Vol.6, No.1, pp.22-29, 2004.

[2] D. Boneh, and H. Shacham, “Group signatures with verifier-local revocation,” CCS 2004, pp.168-177, 2004.

[3] L. Buttyan, T. Holczer, and I. Vajda, “On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs,” ESAS 2007, pp.129-141, 2007.

[4] G. Calandriello, P. Papadimitratos, and J.-P. Hubaux, “Efficient and Robust Pseudonymous Authentication in VANET,” VANET 2007, pp.19-27, 2007.

[5] M. Gerlach, A. Festag, T. Leinm¨uller, G. Goldacker, and C. Harsch. “Security architecture for vehicular communication,” WIT 2005, 2005.

[6] P. Golle, M. Jakobsson, A. Juels, and P. Syverson, “Universal Re-encryption for Mixnets,” Topics in Cryptology - CT-RSA 2004, pp.163-178, 2004.

[7] J.-P. Hubaux, S. Capkun and J. Luo, “The Security and Privacy of Smart Vehicles,” IEEE Security & Privacy Magazine, Vol. 2, No. 3, pp49-55, 2004.

[8] X. Lin, X. Sun, and X. Shen, “Secure vehicular communications based on group signature and ID-based signature,” ICC 2007, pp.1539-1545, 2007.

[9] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen,“ECPP: Efficient Conditional Privacy Preservation Protocol for secure Vehicular Communications,” IEEE INFOCOM 2008, pp. 1903-1911, 2008.

[10] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, “Securing Vehicular Communications - Assumptions, Requirements, and Principles,” ESCAR 2006, 2006.

[11] P. Papadimitratos, A. Kung, J.-P. Hubaux, and F. Kargl, “Privacy and Identity Management for Vehicular Communication Systems: A Position Paper,” Workshop on Standards for Privacy in User-Centric Identity Management, 2006.

[12] B. Parno and A. Perrig, “Challenges in securing vehicular networks,” HotNets-IV, 2005.

[13] M. Raya, and J. -P. Hubaux, “The Security of Vehicular Ad Hoc Networks,” SASN 2005, pp. 11-21, 2005.

[14] M. Raya, P. Papadimitratos, and J-P. Hubaux, “Securing Vehicular Networks,” IEEE Wireless Communications, Vol.13, Issue 5, 2006.

[15] M. Raya and J.-P. Hubaux, “Security Aspects of Inter-Vehicle Communications,” In Proceedings of STRC 2005, 2005.

[16] E. Schoch, F. Kargl, T. Leinmuller, S. Schlott, and P. Papadimitratos, “Impact of Pseudonym Changes on Geographic Routing in VANETs,” ESAS 2006, LNCS 4357, pp.43-57, 2006.

[17] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “AMOEBA: Robust Location Privacy Scheme for VAENT,” IEEE Journal on Selected Areas in Communications, Vol.25, No.8, pp.1569-1589, 2007.

[18] U. Varsheney, “Vehicular mobile commerce,” IEEE Computer Magazine Online, 2004.

[19] U.M. Maurer and Y. Tacobi, “A Non-interactive Public-key Distribution System,” Designs, Codes and Cryptography, pp. 9:305-316, 1996.

[20] 김태환, 김희철, 홍원기, “차량간 통신에서 긴급 메시지 전파를 위한 적응적 릴레이 노드 선정 기법,” 정보처리학회논문지C, 14-C권, 7호, pp.571-582, 2007.

[21] 원윤재, “지능형 자동차 시스템 및 동향 분석,” 한국정보처리학회지, 15권, 5호, pp.16-23, 2008.

[22] 이상응, “In-Vehicle Network 기술 동향,” 한국정보처리학회지, 15권, 5호, pp.76-83, 2008.

[23] 임지환, 오희국, 양대헌, 이문규, 김상진, “강화된 사용자 프라이버시를 보장하는 효율적인 RFID 검색 프로토콜,” 정보처리학회논문지C, 16-C권, 3호, pp.347-356, 2009.

정 채 덕

e-mail : jcd0205@pknu.ac.kr

2005년 동의대학교 수학과(학사)

2007년 부경대학교 정보보호학과(공학석사)

2007년~현 재 부경대학교 정보보호학과 박사과정

관심분야 : 암호 프로토콜, 공개키 암호, 신원기반 암호

서 철

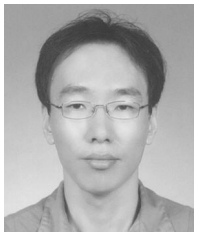
e-mail : kahlil@pknu.ac.kr

2000년 부경대학교 전자계산학과(학사)

2004년 부경대학교 전자계산학과(이학석사)

2004년~현 재 부경대학교 전자계산학과 박사과정

관심분야 : 암호 프로토콜, 공개키 암호, 신원기반 암호



박 영 호

e-mail : pyhoya@pknu.ac.kr
2000년 부경대학교 전자계산학과(학사)
2002년 부경대학교 전자계산학과(이학석사)
2006년 부경대학교 정보보호학과(공학박사)
관심분야 : 암호 프로토콜, 공개키 암호, 신원기반 암호

이 경 현

e-mail : kahlil@pknu.ac.kr
1982년 경북대학교 수학교육과(학사)
1985년 한국과학기술원 응용수학과(이학석사)
1992년 한국과학기술원 수학과(이학박사)
1993년~현 재 부경대학교 전자컴퓨터정보통신공학부 교수
관심분야 : 정보보호론, 공개키 암호, 신원기반 암호, 멀티미디어 정보보호, 그룹 키 관리