프라이버시를 보호하며 안전하고 효율적인 차량간 통신 프로토콜

(Secure and Efficient Protocol for Vehicular Communication with Privacy Preservation)

김 인 환 † 최 형 기 †† 김 정 윤 †††
(In-Hwan Kim) (Hyoung-Kee Choi) (Jung-Yoon Kim)

요 약 Vehicular Ad Hoc Network(VANET)은 차량과 차량, 차량과 네트워크 기반 구조 간에 통신을 지원하는 네트워크로서, 다양한 서비스를 제공할 수 있어 학문적으로나 상업적으로 많은 관심을 받고 있다. 그러나 VANET이 널리 사용되기 위해서는 보안과 프라이버시 관련 문제들이 선행적으로 해결되어야 한다. VANET은 무선 통신과 ad hoc network의 성질을 그대로 이어받아, 다양한 보안 취약점이 존재하며 이에 따라 다양한 공격이 가능하다. 또한, 프라이버시 요구사항을 만족시키지 못하는 경우, 공격자는 특정 차량에 대해서 추적할 수 있으며, 운전자의 민감한 개인정보들이 노출될 수 있다.

VANET에서 프라이버시와 보안을 제공하기 위해 많은 연구들이 진행되었지만, 대부분이 차량 간의 통신 혹은 차량과 네트워크 기반 구조 간의 통신 중 하나에만 집중하고 있으며, 차량의 폐지목록(Revocation List)으로 인해 많은 네트워크 자원을 소비하고 있다. 본 논문에서는 차량과 네트워크 기반구조간의 효율적인 상호 인증을 제공하고, 상호인증 시 네트워크 기반 구조가 차량에게 짧은 시간 동안 차량과 차량 간의 통신에서 사용할 익명 인증서를 생성해주는 프로토콜을 제안한다. 보안 분석을 통해 제안한 프로토콜이 차량과 차량, 차량과 네트워크 기반 구조간의 안전한 통신을 보장하고, 차량의 프라이버시를 보호할 수 있음을 확인 하였으며, 성능 분석을 통해 제안한 프로토콜이 기존의 연구들 보다 높은 효율성을 지니고 있음을 검증하였다.

키워드 : 차량 간 네트워크, VANET, 보안, 프라이버시, 인증

Abstract Due to increasing demand for improving road safety and optimizing road traffic, Vehicular Ad-Hoc Networks (VANET) have been subject to extensive attentions from all aspects of commercial industry and academic community. Security and user privacy are fundamental issues for all possible promising applications in VANET. Most of the existing security proposals for secure VANET concentrate authentication with privacy preservation in vehicle-to-vehicle (V2V) and vehicle-to-roadside infrastructure (V2I) communications and require huge storage and network capacity for management of revocation list. Motivated by the fact, we propose a new scheme with security and privacy preservation which combines V2V and V2I communication. With our proposed scheme, the communication and computational delay for authentication and overhead for management of revocation list can be significantly reduced due to mutual authentication between a vehicle and a Roadside Unit (RSU) requires only two messages, and the RSU issues the anonymous certificate for the vehicle on behalf of the Trust Authority (TA). We demonstrate that the proposed protocol cannot only guarantee the requirements of security and privacy but can also provide efficiency of authentication and management of revocation list.

Key words : Vehicular network, VANET, security, privacy, authentication

† 비 회 원 : LG전자 CTO부문 연구소
playkih@ece.skku.ac.kr
†† 비 회 원 : 성균관대학교 정보통신공학부 교수
hkchoi@ece.skku.ac.kr
(Corresponding author임)
††† 학생회원 : 성균관대학교 휴대폰학과
steal83@ece.skku.ac.kr
논문접수 : 2010년 1월 20일
심사완료 : 2010년 8월 10일

정보과학회논문지: 정보통신 제37권 제6호(2010.12)

1. 서 론

무선 통신 기술의 발달과 보급에 따라 가까운 미래에 차량과 차량, 차량과 네트워크 기반 구조 간의 통신이 가능해질 것이다. 이렇게 차량과 차량, 차량과 RSU (Road Side Unit)가 네트워크를 구성하고 통신하는 형태의 네트워크를 VANET(Vehicular Ad Hoc Network)이라고 부른다. 교통 안전과 교통 관리 같은 요구가 증가되고 있고, 다양한 서비스가 VANET을 통해서 제공될 수 있기 때문에 학문적으로나 상업적으로 VANET에 대한 관심이 크게 증가하고 있다.

VANET은 크게 차량과 차량이 통신하는 V2V (Vehicle-to-Vehicle) 통신과 차량과 RSU가 통신하는 V2I (Vehicle-to-Infrastructure) 통신으로 구분할 수 있다. V2V 통신에서 각 차량은 위치정보, 현재시간, 방향, 속도, 가속/감속, 교통 상황 등을 담은 교통 관련 메시지를 주기적으로 브로드캐스트한다. 이 메시지들은 다른 차량들이 현재 도로 상황을 파악할 수 있게 하고 중앙의 교통제어센터를 통해 전체 교통상황의 원활한 통제 및 관리를 가능하게 한다. V2I 통신에서, 각 차량들은 RSU와의 연결을 통해 외부 네트워크와 연결하여 각종 서비스를 제공받을 수 있다.

VANET은 무선 통신의 속성을 그대로 이어받아 도청, 서비스 거부 공격(DoS attack), 위장공격(impersonation attack), 재생 공격(replay attack)과 같은 다양한 공격들이 가능하다. 따라서 VANET이 성공적으로 배포되고, 널리 이용되기 위해서는 보안 문제점이 해결되어야 한다.

또한, 여러 서비스를 사용하는데 있어 사용자의 프라이버시 보호에 대한 요구가 증가하고 있다. 사용자는 VANET에서 서비스를 이용하는데 있어, 현재 자신이 어디에 있는지, 무엇을 하고 있는지, 어디로 가고 있는지 등의 프라이버시에 관련된 정보들이 노출되지 않기를 원한다. 이에 따라 프라이버시에 대한 보호도 이루어져야 한다.

안전한 VANET을 구성하기 위해 V2I 통신에서 요구되는 보안과 프라이버시 요구사항들은 다음과 같다.

- 상호 인증 및 소스(source) 인증 - 악의적인 공격자가 다른 차량 혹은 RSU로 가장해 잘못된 정보를 다른 차량들에게 전송할 수 있다. V2I 통신에서 오직 권한을 부여 받은 개체만이 다른 개체와 통신할 수 있어야 한다. V2V 통신에서 각 차량은 전달받은 메시지의 송신자의 정당성을 확인할 수 있어야 한다.
- 기밀성과 무결성의 제공 - 차량과 RSU의 통신을 위해 전달되는 모든 메시지는 기밀성과 무결성이 보장되어야 한다. 기밀성은 전달되는 메시지의 암호화를 통하여 제공될 수 있으며, 무결성은 메시지에 MAC (Message Authentication Code)를 첨부함으로써 제공될 수 있다.
- RSU 재위치 공격(RSU replication attack) 방지 - RSU가 공격자로부터 탈취되어 다른 위치로 옮겨가 각종 문제를 발생시킬 수 있는 상황이 발생할 수 있다. Network의 보안을 유지하기 위해 이러한 공격을 막을 수 있는 방법이 필요하다.
- 재생 공격(replay attack) 방지 - 공격자는 전송되는 정상적인 메시지를 탈취하고 해당 메시지를 재전송하여 네트워크에 혼란을 가져올 수 있다. 따라서 이를 방지할 수 있는 방법이 필요하다.
- 익명성 - 차량의 실제 ID가 공격자 및 다른 차량에 노출되어서는 안 된다.
- 비연결성 - 차량의 익명성이 보장된다 하더라도 동일한 정보가 계속 통신에 사용된다면 특정 차량의 이동경로가 노출될 수 있다. 비연결성을 제공하여 특정 차량의 이동경로가 노출되는 것을 막고, 사용자의 프라이버시를 보호할 수 있어야 한다.
- 추적성 - 교통사고와 같은 문제가 발생했을 때 분쟁을 해결하기 위해 문제를 일으킨 메시지의 소스(source)가 되는 차량의 실제 ID를 추적할 수 있어야 한다.

사용자의 프라이버시를 보호하고 안전한 통신을 지원하기 위해 여러 연구가 진행되었지만, 대부분의 논문들은 인증서에 대한 폐지목록을 배포하기 때문에 많은 네트워크 자원을 소모하고 있으며, 인증서가 커질수록 차량의 많은 저장용량을 소모한다. 또한 인증에 많은 메시지와 연산이 필요하여 효율적이지 않다.

이에 따라 IBE(ID-Based Encryption)[1]와 은닉서명[2,3]을 활용하여 RSU와 차량의 상호인증 시 RSU가 네트워크 내의 모든 개체들이 신뢰하는 기관인 Trusted Authority(TA)를 대신하여 다음 RSU까지의 구간에서 사용할 익명 인증서를 생성해주는 프로토콜을 제안한다. 즉 주기적으로 발생하는 RSU와 차량 사이의 상호인증을 통해 차량이 V2V 통신에서 사용할 인증서 역시 주기적으로 생성하도록 한다. 보안 분석을 통해 제안한 프로토콜이 보안 및 프라이버시 요구사항을 만족시키는지 분석하였으며, 다른 프로토콜들과 성능 비교를 통해 효율성을 검증하였다.

본 논문은 7장으로 구성되며 2장에서는 관련 연구를 분석한다. 3장에서는 제안하는 프로토콜의 네트워크 구조를 다루고 있고 4장에서는 제안한 프로토콜의 상세한 과정을 기술한다. 5장에서는 제안한 프로토콜의 보안 및 프라이버시 측면을 하고 6장에서는 다른 프로토콜들과 비교분석을 통해 성능 평가를 한다. 끝으로 7장에서는 논문의 결론에 대해 기술한다.

2. 관련 연구

VANET에 대한 관심이 증가함에 따라, VANET에서 보안과 프라이버시 요구사항 모두를 만족하여 안전한 네트워크를 구성하기 위한 많은 연구들이 수행되었다. 이러한 연구들은 크게 (1) 암호학 기반, (2) 그룹화(grouping) 기반, (3) 비연결성(unlinkability) 기반 3가지로 분류할 수 있다.

암호학 기반의 프로토콜들은 메시지 송신자의 익명성을 보장할 수 있는 그룹 서명(group signature)[4]와 은닉 서명(blind signature)[5]을 이용하고 있다. X. Lin등은 그룹 서명에 기반한 GSIS(Group Signature and Identity-based Signature) 프로토콜을 제안하였다[6]. 메시지의 수신 차량은 메시지의 서명의 정당성을 그룹의 공개키로 확인할 수 있으나 실제 메시지를 보낸 차량이 실제 ID는 알 수 없다. 다만 메시지를 보낸 차량이 그룹 멤버에 속해 있음만을 확인할 수 있다. GSIS는 인증서를 전송하지 않아도 된다는 장점을 지니고 있지만, 송신차량이 폐지목록에 포함되어 있는지 확인하기 위해 방대한 연산이 요구된다. C. Zhang 등은 은닉서명을 적용한 LPPAS(Location Privacy Preserving Authentication Scheme) 프로토콜을 제안하였다[7]. 각 차량은 TA로부터 받은 은닉서명 정보를 사용하여, RSU와 인증을 한다. 핸드오버 시 다음 RSU로부터 미리 받은 은닉서명 정보로 인증을 하기 때문에 차량의 이동경로가 추적되지 않는다. 그러나 초기 인증 시에 TA까지 차량의 정보를 전달해야 하기 때문에 전송되어야 하는 메시지의 수가 많아졌으며 네트워크에 문제를 일으킨 차량을 추적할 수 없다.

그룹화 기반의 프로토콜들의 키 아이디어는 차량들을 그룹으로 묶어 각 차량의 정확한 ID와 위치를 숨기는 것이다. C. Zhang 등은 k개의 차량이 그룹을 이루고 모두 동일한 ID를 사용하는 기법을 제안하였다[8]. 각 차량들은 자신 근처의 차량들이 실제 ID를 알 수 없으며 그룹 ID만 확인할 수 있다. K. Sampigethaya 등은 그룹 리더를 선출하여 RSU와 통신할 때 리더를 통해하는 방법을 제안하였다[9]. C. Zhang 등과 K. Sampigethaya 등이 제안한 방법은 차량의 프라이버시를 보호하지만 폐지목록관리를 위해 차량과 네트워크에 많은 부하가 발생한다. K. Sha 등은 Group ID-Tree를 이용한 인증 알고리즘을 제안하였다[10]. 차량은 자신의 그룹 멤버쉽을 증명한 후 RSU와 연결될 수 있다. 그러나 이 기법은 그룹 멤버쉽 관리를 위해 Group ID-Tree를 갱신하려 할 때 큰 부하가 발생한다.

기존 연구 중에 3번째 방법들은 메시지 간의 연결성(linkability)을 끊는 것이 기본 아이디어이다. 같은 인증서를 반복적으로 사용하여 방생하는 연결성으로 인해 이러한 방법들은 거대한 양의 ID와 인증서를 사용한다. M. Raya등은 차량이 사전에 43800개의 인증서를 미리 실어놓고, V2V 통신 메시지를 전송할 때 43,800개의 인증서 중 무작위로 하나를 선택하여 해당 인증서의 개인키로 전송하는 메시지를 서명하는 HAP(Huge Anonymous Certificate)을 제안하였다[11]. [12]의 방식 역시 이와 유사하게 다수의 익명 인증서를 사전에 실어놓고, 이중 하나의 인증서를 사용하여 메시지간의 연결성을 제거하였다. 그러나 이 방식은 [11]의 방법과는 다르게 한번 사용한 인증서는 폐기(discard)하여 인증서를 모두 사용한 경우, 새로이 인증서들을 전달받아야 한다. 사전에 다수의 인증서를 미리 실어놓고 사용하는 프로토콜들은 메시지간의 비연결성을 제공하여 차량의 프라이버시를 효과적으로 보호할 수 있지만, 각 차량마다 다수의 인증서를 저장하고 있어야 하기 때문에 인증서 폐지 목록이 기하급수적으로 커지게 되며, 이를 각 차량들은 저장하고 있어야 한다. 또한, 이런 거대한 인증서 폐지 목록을 각 차량에게 전달하기 위해서는 네트워크에 큰 부하가 걸리게 되어 효율성이 떨어지는 단점을 지니고 있다. R. Lu 등은 RSU가 차량의 인증서를 대신 관리하여 차량의 부하를 줄인 ECPP(Efficient Privacy Preservation Protocol) 프로토콜을 제안하였다[13]. 차량과 RSU가 인증 시 RSU는 인증된 차량에 한하여 익명 인증서를 전달한다. RSU와 차량의 인증 시 RSU는 차량의 인증서를 생성하고 이를 전달해야 하므로 많은 연산이 필요하여 오랜 시간이 소요된다.

이와 같이 VANET에서의 프라이버시 보호를 위해 많은 연구가 있었지만, 기존의 연구들은 폐지목록 관리로 인해 많은 부하가 발생한다. 또한, V2I 통신 혹은 V2V 통신 하나에만 집중하고 있으며 차량과 RSU간의 인증 시 많은 오버헤드가 발생한다. 이에 따라, 효율적으로 차량의 프라이버시를 보호할 수 있는 통합 통신 프로토콜이 요구된다.

3. 네트워크 구조

제안하는 프로토콜은 TA(Trust Authority), RSU, 차량 3가지 개체로 구성되어 있으며 구조는 그림 1과 같다.

TA는 차량과 RSU의 등록을 책임지고 있으며, 등록 과정에서 차량과 RSU가 안전한 통신을 수행하기 위한 각 파라미터들을 전달하는 역할을 한다. 또한, 차량에 대한 폐지 목록(revocation list)를 관리하며, 이를 주기적으로 업데이트하고 네트워크에 배포한다. 또한, 문제가 발생했을 시, TA는 분쟁을 해결하기 위해 차량의 실제 ID를 추적하는 책임을 지고 있다. TA는 모든 차

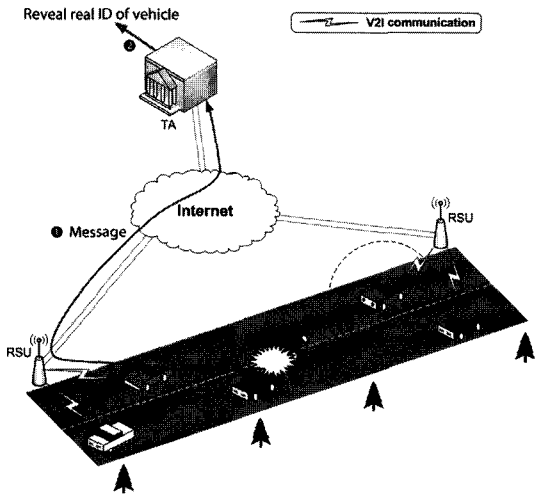

그림 1 네트워크 구조

량과 RSU가 신뢰하는 개체로서 공격자로부터 공격이 불가능하고 탈취 되지 않는다고 가정한다. RSU와 TA의 사이의 연결은 유선 혹은 무선으로 연결되어 있으며, TLS(Transport Layer Security)와 같은 보안 프로토콜로 보호된다.

RSU는 TA의 종속적인 개체로서 차량이 전달하는 정보를 TA에게 전달하거나, TA가 전달하는 정보를 차량에게 전달하는 게이트웨이(gateway) 역할을 한다. 또한, 각 차량들과 외부 네트워크를 연결하여, 차량들이 인터넷 및 각종 서비스를 제공받을 수 있도록 한다.

차량은 RSU와의 상호인증을 통해 세션키를 설정하고 인증절차가 정상적으로 통과되면 외부 네트워크 및 TA와 연결이 가능하다. 또한, 현재 위치 및 시간, 방향, 속도, 가속/감속과 교통상황 등이 포함된 교통관련 메시지를 주기적으로 브로드캐스트(broadcast)하여, 해당 차량의 주변에 있는 차량들이 현재 교통 상황을 파악할 수 있게 하며 사고 발생 시 신속한 대처가 가능하도록 돕는다.

본 논문에서는, 대리서명[2,3]과 IBE[1]를 사용한다. 대리서명은 RSU가 TA를 대신하여 인증된 차량에게 현재 RSU부터 다음 RSU까지 구간에서 사용할 인증서를 생성하는데 사용된다. 차량은 대리서명을 사용하여 RSU로 부터 인증 받는다. 차량의 RSU에 대한 인증은 IBE를 사용하여 차량과 RSU의 상호인증에 필요한 메시지 수를 줄였다.

4. 제안하는 프로토콜

제안하는 프로토콜은 설정 단계, 등록 단계, V2I 인증 단계 그리고 V2V 통신 단계 총 4개의 단계로 구성된다. 설정 단계에서, TA는 제안하는 프로토콜에서 사용

표 1 논문에서 사용하는 용어

표기	설명
G_1, G_2	타원곡선상의 덧셈 군
G_T	유한체 상의 곱셈군
P_1, P_2	G_1, G_2 군의 생성자
s	TA의 마스터키
$Y_1 = sP_1, Y_2 = sP_2$	TA의 공개키
e	bilinear map $e : G_2 \times G_2 \rightarrow G_T$
W_i	차량 혹은 RSU i에 대한 warrant
$CERT_i$	차량 i에 대한 익명 인증서
d_i / Q_i	RSU i의 IBE 개인키/공개키 쌍
x_i / Y_i	차량 i의 개인키/공개키 쌍
σ_i / U_i	RSU 혹은 차량 i의 대리서명 개인키/공개키 쌍
SK_{ij}	차량 i와 RSU j 사이의 세션키

되는 공개 파라미터들을 생성한 후 이를 배포한다. 등록 단계에서, 각 차량과 RSU는 TA로부터 개인정보들을 안전하게 전달받는다. V2I 인증 단계에서, RSU와 각 차량은 상호인증을 하고 비밀통신을 위한 세션키를 생성하며, RSU는 TA로부터 권한을 부여 받은 차량에게 익명 인증서를 생성해준다. V2V 통신 단계에서, 각 차량들은 RSU로부터 받은 익명 인증서를 이용하여 교통 관련 메시지를 서명하고, 이 메시지와 서명 값을 브로드캐스트 함으로써 차량 간의 교통 정보를 공유한다. 표 1은 제안하는 시스템을 설명하기 위해 본 논문에서 공통적으로 사용하는 용어에 대한 정의를 보여주고 있다.

4.1 설정 단계

TA는 먼저 기본 파라미터 $(q, G_1, G_2, G_T, e, P_1, P_2)$를 생성한다. 그 후, 마스터키 $s \in Z_q^*$를 선택하고 이에 따른 2개의 공개키 $Y_1 = sP_1 \in G_1$와 $Y_2 = sP_2 \in G_2$를 계산하고 3개의 해쉬 함수 $H_1 : (0,1)^* \rightarrow Z_q^*$, $H_2 : (0,1)^* \rightarrow G_2^*$, $H_3 : G_T^* \rightarrow (0,1)^*$를 선정한다. TA는 공개 파라미터$(q, G_1, G_2, G_T, e, P_1, P_2, Y_1, Y_2, H_1, H_2, H_3)$를 배포한다.

4.2 등록 단계

차량과 RSU는 인증 및 통신을 위한 개인 정보를 받기 위해 TA에 등록해야 한다. 차량은 TA로부터 임의의 ID와 RSU로부터 인증을 받기 위한 대리서명 키를 전달 받는다. RSU는 차량에게 인증서를 생성하기 위한 대리서명 키와 IBE키를 전달받는다. TA로부터 전달받은 키로 다른 개체로 위장하는 것을 막기 위해 차량과 RSU 각각은 타원곡선상의 다른 군을 사용한다.

이 등록과정은 차량과 RSU가 네트워크에 배포되기 전에 이루어져야 한다. 등록과정의 절차는 다음과 같다.

차량은 TA와 적절한 유효기간 T_{Exp}를 협상한 후, 차량 자신의 ID와 T_{Exp}를 TA에게 보낸다. 이를 받은 TA는 알고리즘 A1을 수행하여 차량을 위한 각 종 파라미터를 생성한다. 이후 TA는 차량에게 $(PID_V, U_V,$

Algorithm 1: [A1] Registration

Data: With system parameters and master key s, the TA inputs an identity ID of the registration request

Result: Generate registration information

begin
  if ID is a vehicle **then**
    Choose random ID PID_V
    Set $W_V = (PID_V, T_{Exp})$
    Compute $U_V = H_1(W_V)P_1 + a_1P_1 \in G_1$ and $\sigma_V = -sH_1(U_V) - a_1 \in Z_q^*$
    Store the duplet $(ID_V, U_V, W_V, \sigma_V)$
    return $(PID_V, U_V, W_V, \sigma_V)$
  else if ID is a RSU **then**
    Set $W_R = (ID_R, T_{Exp})$ and $LID_R = (ID_R, L_R)$
    Compute $U_R = H_1(W_R)P_2 + a_2P_2 \in G_2$, $\sigma_R = -sH_1(U_R) - a_2 \in Z_q^*$, $Q_R = H_2(LID_R) \in G_2$ and $d_R = sQ_R \in G_2$
    Store $(d_R, W_R, U_R, \sigma_R)$
    return $(d_R, W_R, U_R, \sigma_R)$
  end
end

W_V, σ_V)를 안전하게 전달한다. 이를 받은 차량은 TA의 공개키 $Y_1 = sP_1$를 사용하여 다음 식 (1)이 성립할 때에만 대리서명 키 (σ_V, U_V)를 받아들인다.

$$H_1(W_V)P_1 = \sigma_V P_1 + H_1(U_V)Y_1 + U_V \quad (1)$$

RSU 또한 차량과 비슷한 등록과정을 수행하게 된다. 자신의 ID ID_R과 위치정보 L_R을 TA에게 보낸다. TA는 차량의 알고리즘 A1을 수행하여 RSU가 대리서명과 IBE를 사용하기 위한 정보들을 생성한다. 이후 TA는 RSU에게 (d_R, W_R, U_R, σ_R)를 안전하게 전달한다. RSU 역시 TA의 공개키 $Y_2 = sP_2$를 사용하여 차량과 동일한 방법으로 대리서명 키 (σ_R, U_R)를 검증해 본다.

4.3 V2I 인증 단계

차량은 RSU를 통해 인터넷과 같은 외부 네트워크와 연결되기 전에 반드시 RSU로부터 인증 받아야 한다. 또한 위조 RSU를 막기 위해 차량은 RSU를 인증해야 한다. 차량과 RSU의 상호인증이 수행되면 차량과 RSU는 세션키 SK_{VR}을 고유하고, 차량은 익명 인증서를 소유하게 된다. 세션키는 차량과 RSU 사이에 교환되는 메시지의 정보가 외부로 노출되는 것을 막는다. 차량의 익명 인증서는 V2V 통신에서 차량이 메시지에 대한 서명에 사용하는 키에 대한 공증하는 역할을 한다. 그림 2가 V2I 통신에서 인증을 위한 메시지의 교환과 익명 인증서의 생성 과정을 보여주고 있다.

1단계

차량 V가 RSU R의 통신범위로 이동하면, V는 R이 주기적으로 보내는 Beacon 메시지를 통해 RSU의 ID ID_R를 획득하게 된다. 그 후 차량은 GPS(Global Positioning System)를 사용하여 RSU R의 위치 정보 L_R을 측정하고 RSU R의 IBE 공개키 $Q_R = H_2(LID_R) \in G_2$를 계산한다. 차량 V는 다음 RSU까지 구간 동안 V2V통신에서 교통관련 메시지를 서명할 개인키 x_V를 설정하고 이에 대한 공개키 $Y_V = x_VP_1 \in G_1$를 생성한다. V는 세션키를 생성하기 위해 이후, 임의 랜덤 값 $r_1 \in Z_q^*$을 선택하고 $r_1P_1 \in G_1$를 계산한다. 생성한 각 정보가 담긴 메시지 M을 다음 식 (2)와 같이 설정한다. TS_V는 차량이 V가 생성하는 타임스탬프(timestamp)이다.

$$M = (W_V, U_V, PID_V, r_1P_1, Y_V, TS_V) \quad (2)$$

V는 자신의 대리서명 기반의 키 (U_V, σ_V)를 사용하여 서명 (K, w)을 식 (3)과 같이 생성한다.

$$K = k_1P_1 \in G_1$$
$$w = \sigma_V - k_1H_1(K \| M) \in Z_q^* \quad (3)$$

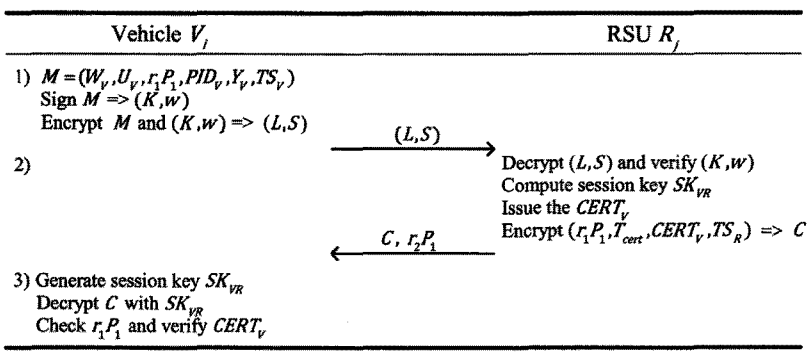

그림 2 V2I 통신에서 인증 및 익명 인증서의 생성 2단계

생성된 서명과 메시지를 평문으로 전송하게 되면 차량의 개인정보들이 쉽게 외부에 노출되므로 V는 RSU R의 IBE 공개키 $Q_R = H_2(ID_R, L_R) \in G_2$를 사용하여 메시지 M과 서명 (K, w)를 다음 식 (4)와 같이 암호화한다.

$$L = k_2 P_2 \in G_2$$
$$S = (M \| K \| w) \oplus H_3(e(Q_R, Y_2)^{k_2}) \quad (4)$$

V는 (L, s)를 R에게 전송한다.

2단계

(L, S)를 받은 R은 IBE 개인키 $d_R = sQ_R \in G_2$를 사용하여 (L, S)를 식 (5)와 같이 복호화한다.

$$S \oplus H_3(e(d_R, L)) = (M \| K \| w) \quad (5)$$

R은 복호화를 통해 메시지 M을 획득하고 TS_V를 확인하여 재생 공격이 발생했는지 확인한다. 해당 차량이 TA가 보낸 폐지 목록에 포함되어 있는지 확인하고 차량 V가 보낸 서명 (K, w)을 TA의 공개키 Y_1를 사용하여 식 (6)과 같이 검증해본다.

$$wP_1 + U_V + H_1(U_V)Y_1 + H_1(K \| M)K = H_1(W_V)P_1 \quad (6)$$

식 (6)의 검증과정이 정상적으로 통과되면 R은 V를 인증하게 된다. R은 랜덤 값 $r_2 \in Zq^*$을 선택하고, 차량과의 세션키 $SK_{VR} = r_2 r_1 P_1 \in G_1$를 계산한다. 그 후, R은 다음 RSU까지 거리와 해당 구간에서의 평균 속도 등을 고려하여 차량이 사용할 익명 인증서에 대한 적절한 유효기간 T_{Cert}를 설정하고 랜덤 값 n를 선택한다.

선택한 랜덤 값을 사용하여 $c = H_1(Y_V \| T_{Cert})$, $N = nP_2$와 $z = \sigma_R - nH_1(N \| c)$를 계산하고 익명 인증서 $CERT_V = (z, N, c, W_R, U_R)$를 설정한다. 이 후 차량의 정보 $(W_R, CERT_V, SK_{VR}, PID_V)$는 추후 추적을 위해 R에 저장된다. R은 SK_{VR}를 사용하여 $(r_1 P_1, T_{Cert}, CERT_V, TS_R)$를 암호화 하고 이를 $r_2 P_1$와 함께 V에게 전송한다. TS_R은 RSU가 생성하는 타임스탬프이다.

3단계

R이 보낸 메시지를 받은 V는 $r_2 P_1$를 이용하여 RSU와 동일하게 $SK_{VR} = r_1 r_2 P_1 \in G_1$를 계산하고 받은 메시지를 복호화한다. 그 후, 복호화하여 얻은 $r_1 P_1$ 값이 자신이 1단계에서 계산했던 것과 같은지 확인하여 R을 인증한다. 마지막으로 다음 식 (7)을 계산하여 R이 생성한 인증서가 정당한지 확인한다.

$$zP_2 + U_R + H_1(U_R)Y_2 + H_1(N \| c)N = H_1(W_R)P_2 \quad (7)$$

상호인증이 종료된 후의 차량과 RSU 사이의 통신은 SK_{VR}로 보호된다. 차량은 도로를 주행하면서 RSU와 상호인증 과정을 반복적으로 수행하게 되고, 주기적으로 익명 인증서를 RSU로부터 발급받게 된다. 차량은 발급받은 익명 인증서를 사용하여 주기적으로 교통 관련 메시지를 브로드캐스트 한다.

4.4 V2V 통신 단계

차량은 교통 관련 메시지를 ECDSA(Elliptic Curve Digital Signature Architecture)[14]를 사용하여 서명하고 검증한다. 송신 차량이 교통관련 메시지를 서명 시 자신의 개인키 x_v를 사용하며, 이를 받은 다른 차량들은 해당 차량의 익명 인증서 $CERT_V$에 포함된 공개키 Y_V를 사용하여 교통관련 메시지를 검증한다.

메시지의 서명

차량은 랜덤 값 $b \in Zq^*$을 선택하고 다음 식 (8)에 따라 B, r와 t를 계산한다.

$$B = bP_1 = (x_A, y_A)P \in G_1$$
$$r = x_A \bmod q$$
$$t = b^{-1}H_1(INFO) + x_V \cdot r) \bmod q \quad (8)$$

$INFO$는 교통관련 정보이며 ECDSA방식으로 생성된 서명은 (r, t)이다. 차량은 메시지를 다음 식 (9)와 같이 형성하고 이를 브로드캐스트한다. 메시지에 포함된 정보는 교통관련정보, 이에 대한 서명과, 차량의 공개키와 익명인증서이다.

$$M = [INFO \| (r,t) \| (Y_V, T_{Cert}) \| CERT_V] \quad (9)$$

메시지의 검증

차량들이 브로드캐스트된 메시지를 받았을 때 차량들은 다음과 같이 메시지를 검증한다. 먼저 익명 인증서 $CERT_V$의 유효기간 T_{Cert}을 검증하고, 유효기간이 지났을 경우 해당 메시지를 버린다. 그 후, 익명 인증서 $CERT_V$를 TA의 공개키 Y_2를 사용하여 식 (7)과 동일하게 검증한다. 마지막으로 다음 식 (10)과 같이 검증한다. 만약 $x_A' \bmod q == r$이 성립한다면 해당 교통관련 정보를 받아들인다.

$$u_1 = H_1(M) \cdot t^{-1} \bmod q$$
$$u_2 = r \cdot t^{-1} \bmod q$$
$$K = u_1 P_1 + u_2 Y_V = (x_A', y_A') \quad (10)$$

2장에서 설명한 ECPP 및 GSIS와 비교하였을 때, 제안하는 프로토콜은 차량 네트워크에 더욱 적합한 암호기법(대리서명, proxy signature)을 적용함으로써 효율성을 향상시켰다.

5. 보안 및 프라이버시 분석

이번 장에서 제안한 프로토콜이 안전한 VANET을 구현하기 위해 필요되는 요구사항들을 어떻게 만족시키는지 분석할 것이다.

• 상호 인증

차량의 소유하고 있는 대리서명 기반 키 σ_V는 TA의

개인키로 생성되고 차량은 이 키를 이용해서 인증 요청 메시지에 서명을 하고 이를 RSU의 IBE 공개키 $Q_R = H_2(LID_R)$ 를 사용하여 암호화한다. 이를 받은 RSU는 자신의 개인키 $d_R = sQ_R$ 로 이를 복호화 하고 TA의 공개키 Y_1 를 사용하여 서명 검증을 통해 차량을 인증한다. RSU는 자신이 차량이 보낸 r_1P_1 을 알고 있음을 증명함으로써 차량으로부터 인증 받는다. 이 증명은 4장에서 설명했듯이, RSU가 차량과 공유하고 있는 세션키인 SK_{VR} 을 이용하여 r_1P_1 을 암호화하여 차량에게 전송함으로써 가능하다. 차량이 보낸 인증 요청 메시지는 RSU의 공개키 $Q_R = H_2(LID_R)$로 암호화 되어있으므로 이에 대응되는 개인키 $d_R = sQ_R$ 를 가지고 있어야만 해당 메시지를 정상적으로 복호화 할 수 있기 때문이다.

• 소스 인증

차량은 식 (9)와 같이 교통 관련 정보에 자신의 공개키, 서명, 인증서를 첨부하여 브로드캐스트한다. 이를 받은 주변의 차량들은 식 (7)과 같이 인증서의 유효성을 확인하고 서명을 송신차량의 공개키 Y_V 로 검증한다. 익명인증서는 TA가 서명한 것과 동일하므로 이 과정들이 정상적으로 통과된다면 주변 차량들은 송신차량의 정당성을 확인할 수 있다. 이는 RSU가 TA를 대신하여 대리서명을 기반으로 하여 인증서를 생성하였기 때문이다. 또한 RSU는 인증서를 생성해주기전에 각 차량들이 폐지목록에 포함되어 있는지 확인하므로 주변 차량들은 송신차량이 폐지목록에 포함되어있지 않은지 확신할 수 있다. 차량의 인증서가 폐지목록에 포함되는 것은 언제나 가능하지만 이 인증서는 짧은 유효시간을 가지고 있어 새로운 RSU의 지역으로 옮겨 갈 때마다 갱신된다.

• 무결성과 기밀성 제공

V2I 통신에서 차량과 RSU는 상호인증 이후 세션키를 공유한다. 상호인증 이후의 모든 메시지는 이 세션키를 이용하여 암호화되고 MAC을 첨부하여 기밀성과 무결성을 보장받는다. V2V 통신에서 차량이 전송하는 교통 관련 메시지는 모두가 공유하는 정보이기에 기밀성을 필요로 하지 않지만, 메시지의 조작 및 위조로 인한 운전자의 안전이 위험한 상황을 방지하기 위해 메시지의 무결성은 반드시 제공되어야 한다. 차량은 메시지를 자신의 개인키 x_V 를 사용하여 식 (8)과 같이 서명한다. 이 서명은 익명 인증서 $CERT_V$ 로 확인된 공개키 Y_V 로만 검증할 수 있다. 이에 따라 RSU로부터 서명된 익명 인증서 $CERT_V$ 에 포함된 공개키 Y_V 에 대응되는 개인키 x_V 를 소유하고 있지 않으면 메시지를 위조하거나 조작할 수 없다.

• RSU 재위치 공격 방지

차량은 RSU와의 인증과정에서 RSU의 위치정보를 직접 측정하고 Beacon메시지로부터 획득한 RSU의 ID를 결합하여 RSU의 IBE 공개키 $Q_R = H_2(LID_R)$ 를 생성한다. 이후 이 공개키로 메시지를 암호화하여 전송하게 된다. RSU가 공격자로부터 탈취되어 다른 위치로 옮겨가게 되면, 차량이 메시지를 암호화 할 때 사용하는 RSU의 공개키가 변경된다. 변경된 공개키에 대응되는 개인키는 TA만이 생성할 수 있다. RSU를 탈취된 공격자는 TA의 개인키를 알 수 없으므로 차량이 전송하는 메시지를 복호화 할 수 없게 되어 정상적으로 인증과정이 수행되지 않는다. 따라서 재위치 공격이 발생한 RSU를 발견할 수 있게 된다.

• 재생(replay) 공격 방지

V2I 통신에서 교환되는 메시지들에는 타임스탬프 값들인 TS_V 와 TS_R 가 포함되어있다. 만약 메시지에 포함된 타임스탬프 값이 유효범위를 벗어난 경우 차량과 RSU는 해당메시지를 버리게 된다. 이와 동일하게 V2V 통신에서 차량이 브로드캐스트하는 교통 관련 메시지에도 현재 시간 정보가 포함되어 있다. 허용 가능한 시간 내에 메시지가 들어왔는지 확인하고 그렇지 않을 경우 재생 공격이 발생한 것으로 간주하고 메시지를 버리게 된다.

• 익명성

차량과 RSU의 상호 인증 과정에서 차량이 사용하는 ID인 PID_V는 TA가 임의로 선택된 값이다. 따라서 RSU는 차량의 실제 아이디를 알 수 없다. 차량이 RSU에게 인증 요청 메시지를 전송할 때 PID_V 는 메시지에 포함되지만 RSU의 IBE 공개키로 암호화되므로 RSU의 IBE 개인키를 소유하고 있지 않으면 복호화 할 수 없으므로 공격자 및 다른 차량들은 이를 알 수 없다. 또한, 차량이 브로드캐스팅하는 교통관련메시지에는 이 PID_V 가 포함되어 있지 않으며 주변의 다른 차량들은 공개키 Y_V 와 인증서 $CERT_V$ 로 각 차량을 구분한다.

• 비연결성

RSU가 생성하는 익명 인증서에는 차량의 실제 ID가 포함되어 있지 않으며, 차량은 새로운 RSU의 범위로 들어갈 때마다 새로운 익명 인증서와 공개키를 사용한다. 따라서 공격자 및 주변 차량들은 계속해서 변경되는 인증서와 공개키가 어떤 차량의 것인지 알 수 없으므로 차량의 이동경로를 추적할 수 없다.

• 추적성

분쟁상황 발생시 TA는 문제가 된 메시지의 $CERT_V$ 에 포함된 $W_R = (ID_R, T_{Exp})$ 를 통해 차량에게 $CERT_V$ 를 발급한 RSU를 찾을 수 있다. RSU는 차량과의 상호인증 과정에서 차량의 정보(W_R, $Cert_V$, SK_{VR}, PID_V)를 일정시간 저장하고 있기 때문에 $CERT_V$ 를 발급받은 차량의 PID_V 를 알 수 있으며, 이 PID_V 를 TA에게 전달한다. TA는 자신의 데이터베이스(database)를 검색하여 PID_V 에 해당하는 차량의 실제 ID를 찾을 수 있게 된

표 2 5개 프로토콜의 보안 및 프라이버시 요구사항 만족 여부 비교

요구사항		GSIS [6]	LPPAS [7]	HAP [11]	ECPP [13]	제안하는 프로토콜
V2I	상호 인증	X	O	X	O	O
	기밀성 및 무결성	X	O	X	X	O
	프라이버시	X	O	X	O	O
V2V	소스 인증	O	X	O	O	O
	무결성	O	X	O	O	O
	프라이버시	O	X	O	O	O
추적성		O	X	O	O	O
효율적인 폐지 목록 관리		X	X	X	O	O

다. 또한, 차량이 사용하는 PID_V는 TA가 설정하였으며, TA와 해당 차량만이 알고 있기 때문에 TA를 제외한 다른 개체들은 차량의 실제 ID를 알 수 없다.

표 2가 5개 프로토콜이 VANET에서 필요한 보안과 프라이버시 요구사항들의 만족 여부를 비교하여 보여주고 있다. 오직 제안한 프로토콜만이 V2I 통신 및 V2V 통신 모두의 요구사항을 만족시키고 있다.

6. 성능평가

본 장에서는 제안한 프로토콜을 널리 알려진 다른 프로토콜들과 비교 분석한다. V2I 통신에서 상호인증에 소요되는 시간, V2V 통신에서 교통관련 메시지를 서명 및 검증하는 시간 및 폐지목록 관리로 발생하는 차량의 저장공간 오버헤드 3가지 측면에서 비교 분석하였다.

6.1 V2I 통신 상호인증 시간 비교

V2I 통신에서 상호인증에 소요되는 시간은 연산 시간과 통신 시간으로 구분된다. 통신 시간은 각 통신 개체간에 RTT(round-trip time)로 정의될 수 있다. 연산 시간은 차량이 인증 요청 메시지를 송신하고 RSU로부터 익명 인증서를 받을 때까지 필요한 각 연산에 소요되는 시간을 말한다. 우리는 연산 시간을 측정하는데 있어 타원 곡선상의 곱하기 연산과 paring 연상이 가장 많은 연산 오버헤드를 지니므로 2가지 연산 외의 전체 성능 에 거의 영향을 미치지 않는 one way hash등의 다른 연산은 고려하지 않을 것이다. 이 두 연산을 각각 PM과 PR로 표시한다. 우리는 Inter Pentium IV 3.0 GHZ의 컴퓨터에서 측정된 [15]의 결과를 적용하였으며, 측정된 결과는 PM은 0.6ms이며, PR은 4.5ms이다.

우리는 제안한 프로토콜의 차량과 RSU의 상호인증 과정 및 인증서 생성과정의 성능을 측정하고, 2장에서 소개한 ECPP[13], LPPAS[7]와 비교하였다.

그림 3이 세가지 프로토콜의 차량과 RSU간의 상호인증에 소요되는 연산 시간을 보여주고 있다. 제안한 프로토콜과 ECPP는 15ms와 34.2ms가 각각 소요된다. ECPP는 상호인증 시 차량과 RSU가 주고 받는 메시지가 4개인데 비해 제안한 프로토콜은 2개의 메시지만 필요하며

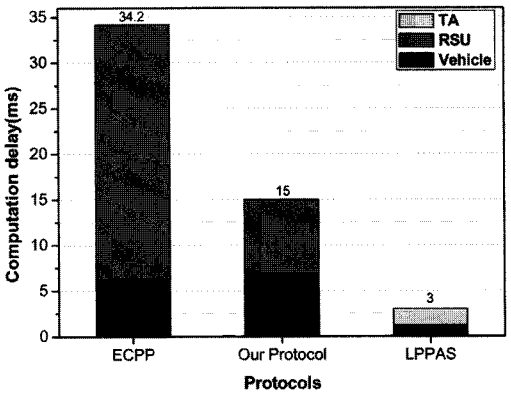

그림 3 상호인증 연산 시간 비교

더 적은 연산이 수행되어 ECPP보다 빠르게 상호인증을 수행한다. LPPAS는 3ms가 소요되어 3가지 프로토콜 중 연산시간을 비교한 경우 가장 좋은 성능을 보여주고 있다. 이러한 결과는 LPPAS에서 상호인증 시 차량과 TA사이에 주고받는 6개의 메시지의 통신 시간이 고려되지 않았으며 LPPAS는 인증서를 생성하는 일련의 과정이 포함되어 있지 않기 때문이다. 일반적으로 통신시간이 연산시간 보다 크므로 연산시간 및 통신시간 모두 고려되었을 경우 LPPAS가 가장 많은 시간을 소요할 것이다.

그림 4는 세가지 프로토콜의 상호인증 수행 시 RTT가 포함된 전체 소요 시간을 보여주고 있다. RTT는 0ms에서 15ms까지 변수로 포함되었다. RSU와 TA 사이의 RTT는 차량과 RSU 사이의 RTT의 α배로 정의하였다. RTT 값이 작을 경우 LPPAS가 가장 빠르다는 것을 알 수 있다. 그러나 RTT 값이 커지는 경우 오히려 LPPAS가 느려져 역전되는 것을 A, B 그리고 C 세 포인트를 통해 알 수 있다. 차량과 RSU사이의 일반적인 RTT 값이 10ms 이상이라면 제안한 프로토콜이 가장 적은 시간이 소요된다는 것을 알 수 있다. 차량과 RSU사이는 무선 구간으로서 일반적으로 10ms이상의 RTT값이 측정된다.

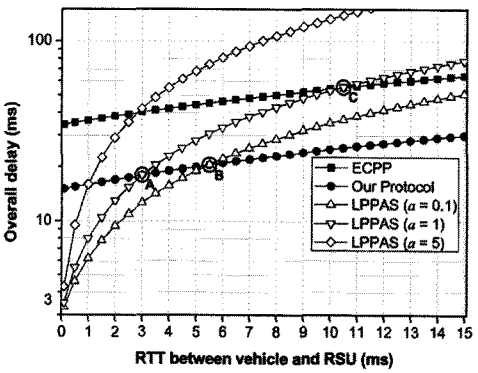

그림 4 RTT가 고려된 상호인증 시간 비교

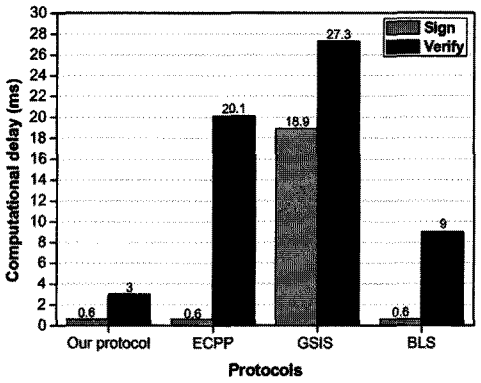

그림 5 교통 관련 메시지의 서명 및 검증 시간 비교

6.2 V2V 통신 서명 및 검증 시간 비교

이번 장에서 주로 연산 시간 위주로 V2V의 통신 시간을 비교할 것이다. 프로토콜 별로 메시지가 다른 경로를 통해 전달되어 각기 다른 통신 시간이 설정되는 V2I 통신과는 달리 V2V통신의 통신 시간은 거의 일정하다. V2V 통신에서 시간을 결정짓는 2가지 동작은 교통 관련 메시지에 대한 서명과 검증이다.

우리는 제안한 프로토콜 ECPP[13], GSIS[6]와 BLS[16, 17] 총 4가지 프로토콜의 메시지 서명과 검증에 소요되는 시간을 비교하였다. LPPAS는 V2V 통신을 정의 하고 있지 않으므로 비교 대상에서 제외한다. 그림 5가 4가지 프로토콜의 연산시간 비교 결과를 보여주고 있다. 제안한 프로토콜, ECPP 및 BLS는 메시지의 서명에 0.6ms가 소요된다. 제안한 프로토콜과 BLS는 메시지의 검증에 각각 3ms와 9ms가 소요된다. BLS가 ECPP나 GSIS보다 나은 성능을 보여주고 있지만, 제안한 프로토콜보다 3배의 시간이 소요되는 것을 알 수 있다.

차량 간 네트워크에서 많은 수의 차량이 주기적으로 교통 관련 메시지를 브로드캐스트하고 주변의 차량들은 이를 계속해서 검증하고 받아들인다. 만약 차량이 자신이 받은 메시지를 일정 시간 내에 검증하지 못한 경우, 계속 메시지가 수신되고 있으므로 해당 메시지들을 버려야 한다. 이는 네트워크 환경에 따라 일정량의 메시지가 처리되지 못할 수도 있음을 시사한다. Dedicated Short Range Communication 표준[18]에 따르면 각 차량은 100ms에서 300ms까지 시간 차를 두고 주기적으로 교통 관련 메시지를 브로드캐스트한다. 우리는 이 주기를 300ms로 정하고 차량의 서비스 비율(service rate)을 다음과 같이 정의한다.

$$\text{서비스 비율} = \frac{\text{300ms 안에 검증하는 메시지들의 수}}{\text{300ms 안에 수신되는 메시지들의 수}}$$

서비스 비율이 높을수록 더욱 더 많은 메시지를 시간 내에 처리할 수 있음을 뜻한다.

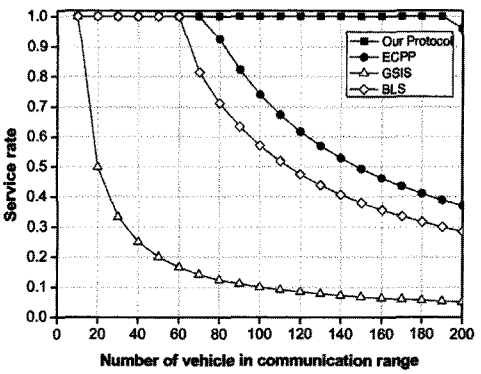

그림 6 멤버 변화율이 15%일 때 서비스 비율 비교

이 서비스 비율은 차량의 통신 범위 내에 있는 차량들의 변화율에 영향을 받는다. 특정 차량이 다른 차량의 통신 범위에 처음 들어가는 경우 인증서의 검증이 발생한다. 그러나 이후 통신 범위 내에 계속 차량이 존재하는 경우 인증서의 검증은 발생하지 않는다. 즉 통신 범위내의 차량 그룹의 멤버가 자주 변화하는 경우 거의 대부분의 메시지에 대한 인증서와 서명 모두 검증해야 하고, 변화가 거의 없는 경우 메시지의 서명에 대한 검증만이 이루어진다.

그림 6과 7이 통신 범위 내의 차량 그룹의 멤버 변화율이 각각 15%와 70%일 때 4가지 프로토콜의 서비스 비율을 보여주고 있다. 통신 범위 내의 차량의 수가 증가할수록 각각 포인트는 틀리지만 서비스 비율이 1에서 점점 떨어지는 것을 알 수 있다. 두 그림에서 알 수 있듯이 제안한 프로토콜이 항상 가장 높은 서비스 비율을 유지하고 있으며 통신 범위 내에 차량 그룹의 멤버 변화율이 70%이며 100대 정도의 차량이 존재하더라도 모든 메시지를 버리지 않고 처리할 수 있다.

6.3 차량의 저장공간 오버헤드

표 3은 폐지목록으로 발생하는 4개 프로토콜의 차량

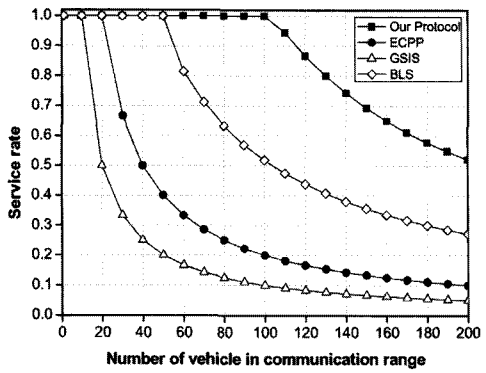

그림 7 멤버 변화율이 70%일 때 서비스 비율 비교

표 3 4개 프로토콜의 저장공간 오버헤드 비교

	제안하는 프로토콜	ECPP	GSIS	HAP
저장공간 오버헤드	-	-	n	mn

의 저장공간 오버헤드를 비교하여 보여주고 있다. ECPP와 제안한 프로토콜은 차량이 폐지목록을 저장하지 않고 RSU가 관리하므로 폐지목록으로 인한 저장공간 오버헤드가 발생하지 않는다. GSIS에서는 폐지목록에 포함된 차량의 수 n이 증가하면 저장공간의 크기도 선형적으로 증가한다. HAP에서 각 차량들은 다수의 익명 인증서를 소유하고 있다. 차량이 소유하고 있는 익명 인증서의 수를 m이라 하면 폐지목록에 포함된 차량의 수 n이 증가하면 저장공간의 사이즈는 mn으로 증가하게 된다. 게다가 폐지목록은 주기적으로 업데이트 되므로 이로 인해 추가적인 통신 오버헤드가 발생하게 된다.

7. 결 론

교통 안전과 관리에 대한 사용자의 요구가 증대되고 VANET을 통해서 다양한 서비스가 창출될 수 있어 VANET은 여러 분야에서 많은 관심을 받고 있다. VANET과 같은 네트워크의 경우 공격이 발생하는 경우 운전자의 생명이 위급한 상황이 발생될 수 있으므로 VANET이 널리 배포되기 위해서는 보안과 프라이버시 관한 이슈들이 선행적으로 해 해결해야 한다. 이를 위해 많은 연구가 진행되었지만, 대부분의 연구가 V2V와 V2I 중 하나에만 집중하고 있으며, 폐지목록 관리로 인해 많은 자원을 소모한다. 또한, 상호인증 및 메시지의 서명과 검증에 많은 시간이 소모되어 효율성이 떨어졌다.

이에 따라 본 논문은 대리서명을 사용하여 RSU가 TA를 대신하여 차량에게 익명의 인증서를 생성하고 이를 V2V 통신에 사용할 수 있는 프로토콜을 제시하여 폐지목록 관리로 인한 오버헤드를 크게 줄였다. 또한, 이 인증서는 주기적으로 변경되어 비연결성을 제공하도록 하여 높은 프라이버시를 제공할 수 있도록 하였다.

보안 분석을 통해 제안한 프로토콜의 특징을 다양한 측면에서 분석하였다. 상호인증에 소요되는 시간, 교통 관련 메시지의 서명과 검증에 소요되는 시간, 차량의 저장 공간 오버헤드와 같은 3가지 측면에서 성능평가를 통해 제안한 프로토콜이 기존 연구들보다 훨씬 나은 효율성을 지니고 있음을 증명하였다.

참 고 문 헌

[1] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *Lecture Notes in Computer Science*, vol.2139, pp.213-229, 2001.

[2] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," *Proc. of 3rd ACM CCS 1996*, pp.48-57, 1996.

[3] T. Okamoto, M. Tada, and E. Okamoto, "Extended proxy signatures for smart cards," *Lecture Notes in Computer Science*, vol.1729, pp.247-258, 1999.

[4] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," *Lecture Notes in Computer Science*, vol.3152, pp.41-55, 2004.

[5] D. Chaum, "Blind signatures for untraceable payments," *Proc. of Advances in Cryptology 1982*, pp. 191-203, 1982.

[6] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," *IEEE Trans. Vehicular Technology*, vol.56, no.6, pp.3442-3456, 2007.

[7] C. Zhang, R. Lu, P.-H. Ho, and A. Chen, "A Location Privacy Preserving Authentication Scheme in Vehicular Networks," *Proc. of IEEE WCNC 2008*, pp.2543-2548, 2008.

[8] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks," *Proc. of IEEE ICC 2008*, pp.1451-1457, 2008.

[9] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," *IEEE Journal on Selected Areas in Communication*, vol.25, no.8, pp.1569-1589, Oct. 2007.

[10] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, "Adaptive Privacy-Preserving Authentication in Vehicular Networks," *Proc. of the International Workshop on Vehicle Communication and Applications 2006*, pp.1-8, Oct. 2006.

[11] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol.15, pp.39-68, 2007.

[12] U.S. Department of Transportation, National Highway Traffic Safety Adimistrtation, Vehicle Safety Communications Project, Final Report. Apr. 2006.

[13] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen,

"ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," *Proc. of IEEE INFOCOM 2008*, pp.1229-1237, 2008.
[14] V. Kapoor, V. S. Abraham, and R. Singh, "Elliptic Curve Cryptography," *ACM Ubiquity*, vol.9, no.20, pp.1-8, 2008.
[15] M. Scott, "Efficient implementation of cryptographic pairings," [Online]. Available: http://ecrypt-ss07.Rhul.ac.uk/ Slide/Thursday/mscottsamos07.pdf
[16] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *Proc. of Asiacrypt 2001*, vol.2248, pp.514-532, 2001.
[17] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," *Lecture Notes in Computer Science*, vol.2656, pp.416-432, 2003.
[18] Dedicated Short Range Communications (DSRC), [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html

김 인 환
2008년 2월 성균관대학교 컴퓨터공학전공 졸업(학사). 2010년 2월 성균관대학교 대학원 전자전기컴퓨터공학과 졸업(석사). 2010년~현재 LG전자 CTO부문 연구소. 관심분야는 암호 프로토콜, VANET, 키 교환, 프라이버시 보호

최 형 기
정보과학회논문지 : 정보통신
제 37 권 제 1 호 참조

김 정 윤
2004년~2005년 안철수연구소 인턴사원 2006년 성균관대학교 컴퓨터공학전공 졸업(학사). 2008년 성균관대학교 대학원 전자전기컴퓨터공학과 졸업(석사). 2010년~현재 성균관대학교 대학원 휴대폰학과 박사과정. 관심분야는 차량 간 통신 보안, Pay-TV 보안, 무선통신망 보안