情報保護學會論文誌
第 21 卷 第 6 號, 2011. 12

VANET에서 RSU의 의존성을 줄이고 차량의 프라이버시를 강화한 인증 프로토콜*

임 원 우,[1†] 김 종 식,[2] 김 상 진,[3] 오 희 국[1‡]
[1]한양대학교, [2](주)그래텍, [3]한국기술교육대학교

Reduced RSU-dependency Authentication Protocol to Enhance Vehicle Privacy in VANET*

Wonwoo Rhim,[1†] Jongsik Kim,[2] Sangjin Kim,[3] Heekuck Oh[1‡]
[1]Hanyang University, [2]Gretech, [3]Korea University of Technology and Education

요 약

VANET은 차량이 안전하고 쾌적한 운행을 할 수 있도록 V2V, V2I 통신을 통해 다양한 서비스를 제공한다. 다양한 서비스를 이용하기 위해 안전하고 신뢰성 있는 V2V, V2I 통신이 보장되어야 하며, 이를 위해 RSU를 기반으로 하는 많은 연구들이 진행되었다. RSU를 기반으로 하는 환경에서는 차량과 RSU 간의 빈번한 통신으로 인한 효율성 문제, RSU가 불능이 됨으로써 발생하는 문제, RSU 내의 정보가 노출되었을 때 발생하는 차량의 프라이버시 침해 문제 등이 발생할 수 있다. 본 논문에서는 RSU의 의존성을 줄이고, 차량의 프라이버시를 강화한 그룹서명 기반의 인증 프로토콜을 제안한다. 제안하는 프로토콜은 그룹서명을 사용하는 기존의 프로토콜보다 효율적이고, VANET의 보안 요구사항을 모두 만족한다.

ABSTRACT

VANET offers variety of services to allow safe and comfortable driving through V2V and V2I communications in transportation systems. To use these services, safe and reliable V2V and V2I communications must be guaranteed. In this regards, many RSU-based studies have been carried out to meet certain issues such as: efficiency of frequent communication between RSU and vehicles, security of stored information in RSU, and invasion on vehicle's privacy. In this paper, a scheme is proposed to reduce the dependency on RSU and to enhance the vehicle privacy by using signature-based authentication protocol. The proposed protocol is more efficient than existing protocol with group signature, and satisfies all the requirements of VANET.

Keywords: VANET, Privacy, Group Signature

접수일(2011년 3월 2일), 수정일(2011년 8월 1일), 게재확정일(2011년 8월 8일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2011-C1090-1111-0010).
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No. 2011-0000189).
† 주저자, wonwoo@infosec.hanyang.ac.kr
‡ 교신저자, hkoh@hanyang.ac.kr

I. 서 론

통신기술과 컴퓨팅 능력의 비약적인 발전으로 인하여 GPS(Global Positioning System)를 이용한 내비게이션 시스템, 하이패스와 같은 자동 비용 징수 시스템 등 다양한 정보기술이 각종 차량에 적용되고 있다. 가까운 미래에는 다양한 응용을 위한 통합된 정보시스템이 차량에 장착될 것이며, 이와 같은 정보시스템들은 무선 통신 기능을 지원할 것이다. 이를 통해 차량과 인프라 간 통신은 물론 차량 간에 통신이 가능해지고, 매우 큰 규모의 애드혹 망이 형성되어 사용될 수 있다. 이와 같은 애드혹 망을 차량 애드혹 네트워크(VANET, Vehicular Ad hoc NETwork)라 한다.

VANET은 차량과 RSU(Road-Side infrastructure Units)로 구성되어 있다. 차량은 VANET에 참여하고 있는 각 차량을 말하며, RSU는 도로 주변에 설치된 통신을 지원하는 장비를 말한다. VANET의 통신 형태는 차량 간 통신(V2V, Vehicular to Vehicular)과 차량과 기반 시설 간 통신(V2I, Vehicular to Infrastructure) 두 종류가 있다. VANET를 위한 미국 통신 표준을 DSRC (Dedicated Short Range Communication)라 하며, DSRC에 의하면 각 차량은 100-300ms 마다 자신의 상태(위치, 방향, 속도 등) 정보를 방송해야 한다[1]. DSRC의 전송반경은 최대 1km 정도이며, 차량에서 방송하는 일반 운행 메시지는 400m의 전송반경을 가진다. DSRC의 전송반경은 짧지만 VANET은 다중 홉 방식의 통신을 사용하기 때문에 차량에서 방송하는 메시지는 더 멀리까지 전송된다.

VANET은 V2V, V2I 통신을 통하여 지역정보, 교통정보, 사고정보 등과 같은 다양한 정보를 수집하고 전송하여 차량의 운행에 도움이 되는 다양한 서비스를 제공한다. VANET에 참여하는 차량들은 V2V, V2I 통신을 통해 여러 가지 서비스를 제공받아 안전하고 효율적인 운행을 할 수 있다. 그러나 한 번의 사고가 큰 피해로 이어지는 VANET의 환경의 특성상, 정보가 조작 및 악용되지 않도록 하는 것이 매우 중요하다. 다양한 서비스를 이용하기 위해서는 안전하고 신뢰성 있는 V2V, V2I 통신이 보장되어야 하며, 이를 위해 RSU를 기반으로 하는 많은 연구들이 진행되었다.

차량이 빠르게 이동하는 VANET의 특성상, 차량은 운행 중 많은 RSU를 통과하게 된다. 차량과 RSU 간에 빈번한 통신이 요구되면 연산량, 통신량 등 네트워크의 효율성 측면에서 영향을 미친다. 또한 안전한 통신을 위해 RSU를 기반으로 인증, 메시지 확인 등이 요구되는 환경에서는 RSU가 불능이 되는 상황이 발생하면, 차량은 인증, 메시지 확인 등을 할 수 없게 되고 운행에 큰 지장을 초래한다. 그리고 차량이 운행 중에 통과하는 많은 RSU 중 하나의 RSU만 공격자에게 피해를 입게 되더라도 차량의 신원정보가 노출이 되는 문제가 발생할 수 있다. 따라서 본 논문에서는 보안 요구사항을 모두 만족하면서, 차량의 프라이버시를 강화한 인증 프로토콜을 제안한다. 제안하는 프로토콜에서는 RSU의 의존도를 줄여 차량의 프라이버시를 강화하였으며, 그룹 서명을 적용하여 보안 요구사항을 만족하였다.

본 논문은 다음과 같이 구성된다. 2장에서는 보안 요구사항을 정의하고, 그룹 서명과 수학적 배경에 대해 살펴본다. 3장에서 관련 연구를 소개하고, 문제점을 살펴본 뒤, 4장에서 본 논문에서 제안하는 프로토콜에 대해 자세히 기술한다. 5장에서는 제안하는 프로토콜을 비교분석하고, 6장에서 결론과 향후 연구방향을 제시한다.

II. 연구 배경

이 장에서는 수학적 배경이 되는 겹선형 사상(bilinear map)에 대해서 설명하고, 제안하는 프로토콜에서 사용한 그룹 서명에 대해서 설명한다.

2.1 겹선형 사상

겹선형 사상은 타원곡선상의 이산대수 문제를 유한체상의 이산대수 문제로 축소시켜 그 어려움을 줄여 타원곡선 암호시스템을 공격하는 도구로 사용되었다. 그러나 2000년에 Joux는 겹선형 사상이 공격 도구가 아닌 정보보호를 위한 암호학적 도구로 사용될 수 있음을 보였고, 이후 겹선형 사상을 이용한 여러 암호학적 기법들이 활발히 연구되고 있다.

본 논문에서는 앞으로 다음과 같이 정의된 표기법을 사용한다. p는 매우 큰 소수이고, G_1, G_2, G_T는 위수가 p인 곱셈 순환군(multiplicative cyclic group)이다. g_1은 G_1의 생성자이고, g_2는 G_2의 생성자이다. ψ는 G_2로부터 G_1으로 계산가능한 동형사상이며, $\psi(g_2)=g_1$이다. 다음과 같은 조건들을 만족하는 함수 $\hat{e}: G_1 \times G_2 \rightarrow G_T$를 사용가능 겹선형 사상

(admissible bilinear map)이라 한다.

- Bilinear: 모든 $u \in G_1$, $v \in G_2$와 $a, b \in Z_p^*$에 대해 $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$가 성립해야 한다.
- Non-degenerate: g_1과 g_2에 대해 $\hat{e}(g_1, g_2) \neq 1$이 성립해야 한다.
- Computable: 임의의 $u \in G_1$, $v \in G_2$에 대해 $\hat{e}(u, v)$를 계산할 수 있는 효율적인 알고리즘이 존재해야 한다.

Bilinear 특성에 의해 $\hat{e}(u^a, v^b) = \hat{e}(u, v^b)^a = \hat{e}(u^a, v)^b = \hat{e}(u, v)^{ab} = \hat{e}(u^{ab}, v) = \hat{e}(u, v^{ab})$와 같은 특성을 추가적으로 유도할 수 있다.

겹선형 사상은 다음과 같은 CDHP (Computational Diffie-Hellman Problem), DLP(Discrete Logarithm Problem), BDHP(Bilinear Diffie-Hellman Problem) 문제의 어려움에 기반하고 있다. 현재까지 CDHP, DLP, BDHP를 다항시간 내에 계산하는 것은 계산적으로 어렵다고 알려져 있다. 본 논문에서 사용된 겹선형 사상의 안전성은 위의 문제들을 다항시간 내에 계산하는 것이 어렵다는 가정에 기반하고 있다.

- CDHP: 어떠한 $a, b \in Z_p^*$에 대해 $g_1^a, g_1^b \in G_1$이 주어졌을 때, $g_1^{ab} \in G_1$을 계산하는 문제이다.
- DLP: $g_1^a \in G_1$이 주어졌을 때, 어떠한 $a \in Z_q^*$를 계산하는 문제이다.
- BDHP: 어떠한 $a, b, c \in Z_p^*$에 대해 $g_1^a, g_1^b, g_1^c \in G_1$이 주어졌을 때, $\hat{e}(g_1, g_1)^{abc} \in G_T$를 계산하는 문제이다.

2.2 그룹 서명

그룹 서명은 그룹 멤버가 신원을 노출하지 않고 그룹의 구성원임을 확인하는 기법이다. 그룹의 멤버는 키 발급 기관으로부터 서명용 비밀키를 발급받아 서명을 생성하고, 검증자는 그룹의 공개키로 서명을 검증한다. 그룹 서명에 사용되는 키는 그룹 멤버의 서명용 비밀키, 서명 검증용 그룹 공개키, 키 발급 기관이 가지는 마스터 비밀키와 같이 세 부분으로 구성된다. 그룹 서명이 일반적으로 제공하는 성질은 다음과 같다[2][3].

- 정확성(Correctness): 그룹 멤버의 유효한 서명은 검증되어야 하고, 유효하지 않은 서명은 검증에 실패하여야 한다.
- 위조불가능성(Unforgeability): 그룹 멤버만이 유효한 서명을 생성할 수 있어야 한다.
- 익명성(Anonymity): 그룹 관리자를 제외한 누구도 서명으로부터 서명자의 신원을 알 수 없어야 한다.
- 불연결성(Unlinkability): 다른 두 메시지와 각 메시지에 대한 서명이 주어졌을 때, 그 서명들이 같은 서명자의 서명인지 여부를 판단할 수 없어야 한다.
- 불결탁성(Exculpability): 그룹 멤버와 그룹 관리자가 결탁하더라도 참여하지 않은 다른 그룹 멤버의 서명을 생성할 수 없어야 한다.
- 추적가능성(Traceability): 그룹 멤버의 서명으로부터 그룹 관리자 비밀키에 의해 서명자의 신원을 확인할 수 있어야 한다.

본 논문에서는 안전한 V2V, V2I 통신을 위해 위의 성질을 만족하는 그룹 서명 기법을 사용하여, VANET의 정당한 사용자임을 확인하는 인증과 차량의 프라이버시를 보호하기 위한 익명성, 불연결성을 제공하였다. 본 논문에서 사용한 그룹 서명 기법은 boneh 등이 제안한 그룹 서명 기법[4]으로, 이 그룹 서명 기법의 안전성은 q-SDH(q-Strong Diffie-Hellman)과 DLDH(Decisional Linear Diffie-Hellman) 문제의 어려움에 기반하고 있다.

- q-SDH: 주어진 $(q+2)$개의 $(g_1, g_2, g_2^{\gamma}, g_2^{(\gamma^2)}, \cdots, g_2^{(\gamma^q)})$로부터 어떠한 $x \in Z_p^*$에 대해서 $(g_1^{1/(x+\gamma)}, x)$를 계산하는 문제이다.
- DLDH: 주어진 (u, v, h, u^a, v^b, h^c)로부터 $c = a + b$를 계산하는 문제이다.

III. 관련 연구

이 장에서는 지금까지 메시지 인증과 차량의 프라이버시를 보장하기 위해 제안되었던 방법들을 설명한다. 그리고 제안되었던 방법들이 가지는 문제점에 대해서 분석한다.

3.1 관련 연구

VANET에서 주된 요구사항은 메시지의 인증과 차량의 프라이버시를 보장하기 위한 조건부 익명성이라고 할 수 있다. 따라서 현재까지 VANET에서 메시지의 송신차량을 인증하고 프라이버시를 보호하기 위한 많은 연구가 진행되었다.

2007년 Raya와 Hubaux는 차량의 프라이버시를

보호하기 위해 신뢰기관으로부터 익명 인증서를 발급받아서 사용하는 방법을 제안하였다[6]. 하나의 익명인증서를 발급받아서 사용하게 되면 차량의 실제 ID는 보호하게 되지만 추적이 가능하기 때문에 프라이버시를 보호하지 못한다. 따라서 Raya와 Hubaux는 인증기관으로부터 다량의 익명인증서를 발급받는 방법을 사용하였다. Raya와 Hubaux의 방법에서 각 차량은 다량의 익명인증서를 유지하기 위한 저장 공간이 필요하며, 익명 철회를 위해 신뢰기관은 매우 많은 정보를 유지해야 한다. 또한, 각 차량은 주기적으로 다량의 익명인증서를 재발급 받아야 하며, VANET에서 필요한 요구사항인 부인방지를 제공하지 못한다. Raya와 Hubaux의 방법은 도로를 셀 단위로 나누고 하나의 셀을 한 그룹으로 사용하며, 셀의 중심에 가까운 차량을 그룹 관리자로 결정하였다. 따라서 도로에 차량이 존재하면 그룹은 항상 유지가 되지만, 셀의 중심에 가까운 차량을 그룹 관리자로 결정하기 때문에 차량이 빠르게 이동하는 VANET 환경의 특성상 그룹 관리자가 빈번하게 바뀌게 된다. 그룹 관리자가 바뀜에 따라 그룹키 또한 빈번하게 바뀌게 되며, 한 차량이 그룹을 통과하는데 여러 번 그룹키를 바꿔야 하는 상황이 발생할 수 있다.

차량이 신뢰기관으로부터 다량의 익명인증서를 사전에 발급받고 저장해야한다는 문제점을 개선하기 위해, 2007년 Lin 등은 차량 간의 통신에 그룹 서명을 기반으로 차량에 조건부 익명성을 제공하는 시스템인 GSIS를 제안하였다[7]. GSIS는 차량 간의 통신(V2V)을 위해 Boneh 등이 제안한 그룹 서명 기법을 사용하며, 차량과 기반시설 간의 통신(V2I)은 일반 신원기반 서명을 사용한다. 그룹 서명 기법을 사용하면 서명의 검증자는 그룹 멤버 중 누가 서명하였는지 알 수 없기 때문에, 그룹의 멤버는 익명성을 보장받으면서 서명을 할 수 있다. 하지만 연산량 측면에서 그룹 서명 자체가 비효율적이며, GSIS에서 제안된 철회 방법 역시 효과적이지 못하다. 또한 Lin 등이 제안한 방법은 RSU와의 인증과정을 필요로 한다. 차량은 통신 반경이 1km정도인 RSU는 짧은 시간에 통과하게 되며, 차량의 이동에 많은 RSU을 거치게 된다. 따라서 차량과 RSU 간의 빈번한 통신은 연산량과 통신량 등 효율성 측면에서 영향을 미친다.

2008년 Lu 등은 차량이 신뢰기관으로부터 다량의 익명인증서를 사전에 발급받고 저장해야하는 문제를 해결하기 위해, RSU가 RSU의 범위를 통과하는 차량에 단기간 익명인증서를 발급해주는 방법인 ECPP를 제안하였다[8]. ECPP는 차량이 다량의 익명인증서를 유지해야 하는 기존 방법에 비해 유지해야 하는 정보가 적으며, RSU가 익명인증서의 발급을 거부함으로써 차량 철회가 비교적 쉽다. 하지만 차량은 프라이버시를 보호하기 위한 메시지의 불연결성을 보장하기 위해 RSU로부터 발급받은 익명인증서를 지속적으로 변경하여야 하며, 따라서 RSU와의 통신이 자주 발생한다. 차량과 RSU 간의 빈번한 통신은 효율성 측면에서 영향을 미치게 된다. 또한 RSU가 충분히 설치되어 있는 환경이 제공되어야 하며, RSU가 조밀하게 설치되어 있지 않는 환경에서는 다음 RSU까지 이전 RSU로부터 발급받은 단기간 익명인증서를 반복해서 사용하게 되므로 인증서의 유효기간에 따라 인증받지 못하거나, 익명인증서의 반복사용으로 메시지의 불연결성을 제공하지 못한다.

2008년 C. Zhang 등은 낮은 통신비용을 위해 MAC을 사용하는 방법인 RAISE를 제안하였다[9]. RAISE는 먼저 차량이 RSU와 Diffie-Hellman 기반 키 확립 프로토콜을 수행한 후, 확립된 세션키로 메시지의 MAC을 계산하여 전송한다. RSU는 여러 차량으로부터 수신한 메시지들을 검증한 후 메시지들을 통합하여 다시 차량들에게 메시지들의 유효성을 알려주는 방식이다. RAISE에서 차량은 익명성을 위해 RSU로부터 발급받은 세션키와 익명 ID를 사용한다. 차량이 이 익명 ID를 다음 RSU를 만날 때까지 사용하게 되면 메시지의 불연결성을 제공할 수 없기 때문에, RSU는 Sweeney의 K-ANONYMITY[10] 방법으로 같은 익명 ID를 k개의 차량에 중복해서 발급하여 차량의 프라이버시를 보호한다. RAISE는 차량에서 수신한 메시지가 VANET 시스템에 등록된 차량인지 제 3의 공격자에 의한 메시지인지에 대한 인증을 제공하지 못한다. 또한 차량과 RSU 간에 키 확립 프로토콜을 수행하여야 하고 모든 메시지는 RSU로 전달되어야 하며, RSU는 이 메시지들을 검증하고 차량들에게 메시지의 유효성을 알려주어야 한다. 따라서 차량은 RSU가 불능이거나 존재하지 않는 환경에서는 인증과 메시지 확인을 하지 못하며, RSU가 충분히 설치되어 있는 환경이 제공되어야 한다.

2008년 C. Zhang 등은 복잡한 인증서 관리 문제를 해결하기 위해 신원기반 암호시스템을 적용한 방법을 제안하였다[11]. Zhang 등이 제안한 방법은 신원기반 시스템 PKG(Public Key Generator)의 마스터키를 조작 불가능한 장비인 차량 TRH(Tamper Resistant Hardware)에 유지하며, 각 차량은 마

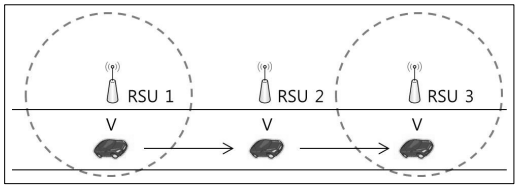
스터키를 이용하여 익명의 공개키 쌍을 자체적으로 생성한다. 조건부 익명성을 제공하기 위해 차량의 실제 신원을 PKG의 공개키로 암호화하여 익명 ID를 생성하고, 이 ID를 이용하여 신원기반 공개키 쌍을 생성한다. 따라서 PKG의 마스터키를 알고 있는 신뢰기관은 익명 ID를 복호화 하여 메시지의 익명성을 철회할 수 있다. C. Zhang 등이 제안한 방법에서 메시지의 불연결성을 제공하기 위해서는 각 공개키 쌍마다 하나의 메시지만 서명하여야 한다. 따라서 각 차량은 매우 많은 공개키를 지속적으로 생성하여야 하며, 공개키 생성비용이 많이 들게 된다. 또한 C. Zhang 등의 방법은 V2V 통신보다는 V2I 통신을 중점으로 한 방법으로 차량은 RSU에게 메시지를 보내고 RSU는 메시지를 확인한다. 서명 확인 비용을 줄이기 위해 일괄확인 기법을 사용하고 있지만 일괄확인이 실패하였을 경우 어떤 서명 때문에 실패하였는지 판단하기 어렵다. 그리고 C. Zhang 등의 방법은 VANET에서 필요한 차량 철회 방법을 제공하지 않는다.

2010년 L. Zhang 등은 인증서의 분배 및 철회를 효율적으로 처리하고, TRH에 의존하는 환경을 줄이기 위해 Ferrara 등이 제안한 그룹 서명 기법[12]을 사용하는 방법을 제안하였다[13]. RSU들은 각각 그룹을 유지하며 그룹을 지나는 차량에 인증과정을 거친 후 그룹키를 발급한다. 그리고 RSU에 유지되는 그룹은 그룹 서명을 사용하여 메시지 인증을 제공한다. 그룹 서명에 겹선형 사상(bilinear pairing)이 사용되기 때문에 서명 확인 비용을 줄이기 위해 일괄확인 기법이 사용되지만 앞서 C. Zhang 등의 연구[11]에서와 같이 일괄확인이 실패하였을 경우 어떤 서명 때문에 실패하였는지 판단하기 어렵고, 이 특성 때문에 DoS 공격에 취약해질 수 있다. 또한 RSU를 기반으로 유지되는 그룹을 기반으로 인증과정을 거치고 그룹 서명을 사용하는 방법이기 때문에 RSU가 충분히 설치되어 있는 환경이 제공되어야 한다.

3.2 기존 연구들에 대한 고찰

기존 연구들을 살펴보면 초기에 다량의 익명인증서를 사용하는 방법이 제안되었고, 이후에는 그 방법이 가지는 문제점을 해결하기 위해 RSU를 기반으로 한 그룹을 사용하거나, 인증, 메시지 확인 등의 이유로 RSU와의 통신이 요구되는 환경이 많이 사용되었다.

RSU를 기반으로 한 그룹을 통해 그룹 서명을 사용하는 기법, RSU로부터 익명인증서를 발급받는 기법



〔그림 1〕 RSU 2가 불능이 되는 예

등 차량과 RSU 간에 인증 및 통신이 요구되는 환경은 RSU에 차량의 신원정보 저장을 필요로 한다. 차량은 많은 RSU를 통과하게 되고, 차량의 신원정보는 통과한 많은 RSU에 중복되어 저장이 된다. 많은 RSU 중 하나의 RSU만 공격자에게 피해를 입게 되더라도 차량의 신원정보가 노출이 되는 문제가 발생할 수 있다.

앞서 1장에서 언급한 것과 같이 RSU는 통신에 DSRC 프로토콜을 사용하기 때문에 전송반경이 크지 않으며 1km 정도이다. 따라서 RSU가 그룹 관리자가 되어 그룹을 유지하는 환경에서 RSU는 도로상에 매우 조밀하게 설치되어 있어야한다. 그리고 〔그림 1〕과 같이 어떤 RSU가 불능이 되는 상황이 발생하게 되면, 차량은 RSU와 인증과정을 거치지 못하여 그룹에 가입하지 못하거나 그룹키를 발급받지 못하게 되어 차량 간에 통신 및 메시지 인증에 문제가 발생하게 된다.

인증, 메시지 확인 등에 RSU와의 통신이 요구되는 환경 또한 위와 비슷한 문제가 발생할 수 있다. 어떤 RSU가 불능이 되는 상황이 발생하면, 그 RSU를 지나는 차량은 인증, 메시지 확인 등을 할 수 없게 되고 VANET에 큰 지장을 초래하게 된다. 그리고 인증, 메시지 확인 등의 이유로 발생하는 차량과 RSU 간에 빈번한 통신은 연산량, 통신량 등 네트워크 효율성 측면에서 효율을 떨어뜨리게 된다.

본 논문에서는 위의 문제들을 바탕으로, 신뢰기관만 차량의 신원을 확인할 수 있도록 차량의 익명성을 RSU까지 확대하였다. 그리고 VANET을 이용하는 전체 차량을 하나의 그룹으로 그룹 서명을 사용하여 메시지 인증과 익명성을 제공하였다. 따라서 차량과 RSU의 요구되는 통신이 줄어들고, 어떤 RSU가 불능이 되더라도 VANET에 미치는 영향이 적다. 이와 같이 본 논문에서 역할이나 권한이 적은 RSU를 가정하고 있으며, 가정하는 RSU는 다음과 같은 기능을 한다.

- 차량이 방송한 메시지를 중계 한다.
- 차량이 방송한 메시지를 수집하고 거짓 여부를

판단하여 신뢰기관에 전달한다.
- 신뢰기관으로부터 받은 철회메시지, 알림메시지 등을 방송한다.
- 다양한 콘텐츠를 활용한 서비스를 제공한다.

IV. 제안하는 프로토콜

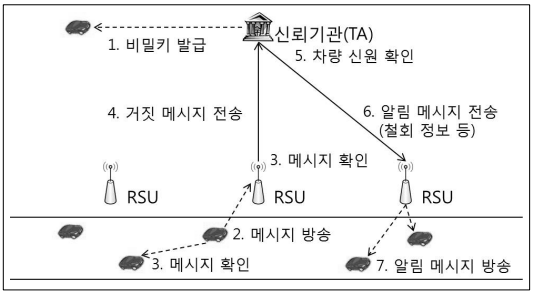
이 장에서는 제안하는 프로토콜에 대해서 설명한다. 차량의 신원정보를 신뢰기관(TA, Trusted Authority)만 확인할 수 있도록 차량의 익명성을 RSU까지 확대하였으며, VANET의 전체 차량을 하나의 그룹으로 그룹서명을 사용하는 방법이다.

제안하는 프로토콜은 시스템 설정 단계, 차량 등록 단계, 메시지 서명 단계, 메시지 확인 단계, 신원 확인 단계, 차량 철회 단계의 6단계에 걸쳐 진행한다. 시스템 설정 단계는 TA가 필요한 인자들을 설정하고 시스템을 구성한다. 차량 등록 단계는 차량이 VANET을 이용하기 전에 TA를 통해서 차량을 등록하고, TA로부터 그룹서명에 사용할 비밀키를 발급받는다. TA는 차량의 신원정보를 저장하며, 저장한 신원정보는 차량 철회 등에 사용한다. 메시지 서명 단계에서는 차량이 TA로부터 발급받은 개인키로 메시지에 서명을 하여 메시지를 방송한다. 메시지 확인 단계는 메시지를 수신한 후 서명을 확인하는 단계로, 차량과 RSU에서 각각 일어난다. 신원 확인 단계는 TA에서 수행하는 단계로 어떤 차량이 거짓 메시지를 방송할 경우, 거짓 메시지의 서명을 통해 차량의 신원을 확인한다. 차량 철회 단계는 차량에서 철회 대상 차량을 구분하기 위한 과정을 수행하는 단계로, TA가 어떤 철회 대상 차량을 구분하여 RSU에 전달하면, RSU는 TA로부터 받은 메시지를 방송한다.

4.1 시스템 모델

VANET의 노드들인 차량과 도로에 설치된 RSU는 무선 통신 표준으로 DSRC를 사용하며, RSU와 TA는 유선 또는 무선 통신을 사용한다고 가정한다. 그리고 다중 홉 방식의 통신을 통해 메시지가 전파된다고 가정한다.

제안하는 프로토콜의 기본적인 구성과 과정은 〔그림 2〕와 같다. 시스템은 기본적으로 차량, RSU, TA로 구성된다. 기본적인 과정은 1) 차량은 차량 등록 단계를 거쳐 비밀키를 발급 받는다. 2) 차량이 운행 중에 메시지 서명 단계를 통해 메시지에 서명을 하여



〔그림 2〕 제안하는 프로토콜의 기본적인 구성과 과정

방송하면, 3) 주변 차량과 RSU는 메시지 확인 단계를 통해 메시지의 서명을 확인한다. 4) 메시지 중 한 메시지가 공격자에 의한 거짓 메시지로 확인되면 RSU는 TA에 거짓 메시지를 전송한다. 5) TA는 메시지의 서명을 통해 개인키를 확인하고, 차량의 신원을 확인한다. 6) TA는 철회 메시지 등 방송이 필요한 알림 메시지를 RSU에 전송하고, 7) RSU는 TA로부터 받은 메시지를 차량이 수신할 수 있도록 방송한다.

제안하는 프로토콜은 〔표 1〕과 같은 표기법을 사용한다. 그리고 차량에서 전송되는 안전한 메시지 형식은 〔표 2〕와 같다. 〔표 2〕의 그룹 ID *GID*는 차량이 속한 하위 그룹으로 지역적인 그룹의 ID가 아닌, TA에서 관리하는 차량 정보의 하나로 존재한다. 철회 대상 차량이 발생하였을 때 사용되는 정보이다. M으로 표기되는 Payload는 차량의 위치, 방향, 속도, 시간 등 교통관련 정보가 포함이 되며, 사고 등과 같이 이벤트가 발생하면 이벤트 정보가 추가된다. M에 포함이 되어있는 시간정보는 교통관련 정보의 시간을 나타내주면서, 재전송 공격을 방지하는 역할도 한다. 〔표 2〕의 마지막에 위치한 TTL(time to live)은 메시지의 재송신 범위를 지정해준다.

〔표 1〕 제안하는 프로토콜에서 사용하는 표기법

표기법	내용
Q_G	그룹의 공개키
q_S	TA의 개인키
Q_{V_i}	차량 i의 공개키
q_{V_i}	차량 i의 개인키
GID	철회를 위한 하위그룹
$E_K\{\ \}$	키 K를 이용한 암호화
$D_K\{\ \}$	키 K를 이용한 복호화
$H_1 : \{0,1\}^* \rightarrow G_1$	일방향 해쉬 함수
$H_2 : \{0,1\}^* \rightarrow \{0,1\}^f$	일방향 해쉬 함수
$H_3 : \{0,1\}^* \rightarrow Z_p^*$	일방향 해쉬 함수

〔표 2〕 안전한 메시지의 형식과 길이

Group ID	Payload	Signature	TTL
2 bytes	100 bytes	192 bytes	1 byte

차량이 메시지를 방송할 때 메시지에 대한 서명이 없이 방송한다면, 여러 공격에 노출이 될 수 있고 인증, 무결성 등 안전한 통신을 위해 위에서 정의하였던 보안 요구사항들을 만족하지 못하게 된다. 즉, 메시지를 수신한 차량에서는 수신한 메시지가 정당한 사용자로부터 발송된 것인지 또는 중간에 위/변조 되지 않았는지 등을 확인할 수 없다. 따라서 메시지에 서명을 추가하여, 인증, 무결성 등 안전한 통신을 위한 요구사항을 만족할 수 있도록 해야 한다. 본 논문에서는 이러한 요구사항을 만족하기 위해 그룹 서명 기법을 사용하였다.

4.2 제안하는 프로토콜

4.2.1 시스템 설정 단계

TA가 시스템에 필요한 인자들을 생성하고, 그룹의 공개키와 TA의 개인키를 설정한다. 그리고 TA는 시스템에 등록하는 각 차량에 발급할 차량의 비밀키를 만들기 위한 인자를 생성한다.

1) TA는 $G_1, G_2, g_1, g_2, \psi, \hat{e}$와 $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : \{0,1\}^* \rightarrow \{0,1\}^f$, $H_3 : \{0,1\}^* \rightarrow Z_p^*$를 선택한다.
2) TA는 임의의 $h \in G_1^*$, $\xi_1, \xi_2 \in Z_p^*$를 선택하고 $u^{\xi_1} = v^{\xi_2} = h$가 되는 $u, v \in G_1$을 설정한다.
3) TA는 임의의 $r \in Z_p^*$를 선택하고, $w = g_2^r$을 생성한다. 그리고 $W = g_2^w$를 생성한다.
4) 그룹의 공개키 $Q_G = (h, u, v, W)$이고, TA의 개인키 $q_S = (\xi_1, \xi_2)$이다.

4.2.2 차량 등록 단계

차량이 TA에 신원을 등록하고, TA로부터 서명에 사용할 비밀키를 발급받는 단계이다. TA는 차량의 신원정보를 저장하기 위해 〔표 3〕과 같은 차량리스트를 관리한다.

〔표 3〕 TA에서 관리하는 차량리스트

그룹	차량 ID	차량 인증서	대칭키	랜덤값
GID_1	A_1	C_1	K_1	r_1
GID_1	A_2	C_2	K_2	r_2
GID_1	A_3	C_3	K_3	r_3
GID_2	A_4	C_4	K_4	r_4
GID_2	A_5	C_5	K_5	r_5
⋮	⋮	⋮	⋮	⋮

1) 차량 V_i는 개인키 ζ_i를 선택하고, 공개키 $g_2^{\zeta_i}$를 생성한다. 그리고 TA로부터 발급받는 비밀키의 암호화에 사용할 세션키 K_i와 타임스탬프 T, 차량의 인증서 C_{V_i}를 TA에 보낸다. 자세한 과정은 다음과 같다.
   a) V_i는 임의의 $\zeta_i \in Z_p^*$를 선택하고, $g_2^{\zeta_i}$를 생성한다. V_i의 개인키 $q_{V_i} = \zeta_i$이고, 공개키 $Q_{V_i} = g_2^{\zeta_i}$이다. 그리고 세션키 K_i를 선택한다.
   b) V_i는 $\rho = u^{\zeta_i}$, $\sigma = H_1(K_i \| C_{V_i} \| T \| \rho \| h \| h^{\zeta_i})^{\zeta_i}$, $\tau = (K_i \| C_{V_i} \| T \| \sigma) \oplus H_2(\rho \| h \| h^{\zeta_i})$를 계산한다.
   c) V_i는 (ρ, τ)를 TA에 보낸다.
1) TA는 V_i로부터 받은 (ρ, τ)로부터 K_i, C_{V_i}, T, σ를 획득하고, 인증서와 서명의 유효성을 확인한다. 그리고 유효한 서명일 경우, V_i에게 비밀키 (A_i, x_i)와 차량이 소속될 하위그룹의 ID GID를 발급한다. 자세한 과정은 다음과 같다.
   a) TA는 V_i로부터 받은 (ρ, τ)의 ρ로부터 $H_2(\rho \| h \| \rho^{\xi_1})\,(= H_2(\rho \| h \| h^{\zeta_i}))$를 계산한다. 그리고 τ로부터 $\tau \oplus H_2(\rho \| h \| \rho^{\xi_1}) = (K_i \| C_{V_i} \| T \| \sigma)$를 계산하여, K_i, C_{V_i}, T, σ를 획득한다.
   b) TA는 C_{V_i}의 유효성을 확인하고, C_{V_i}로부터 Q_{V_i}를 획득한다. C_{V_i}가 유효하지 않거나 TA가 관리하는 철회리스트에 포함되어 있을 경우, 프로토콜을 중지한다.(철회 리스트에 대해서는 차량 철회 단계에서 설명한다.)
   c) TA는 $\hat{e}(\sigma, g_2) ? = \hat{e}(H_1(K_i \| C_{V_i} \| T \| \rho \| h \| h^{\xi_1}), Q_{V_i})$를 계산하여 서명을 확인한다. 유효한 서명일 경우, $x_i = H_3(r \| Q_{V_i})$, $A_i = g_1^{1/(w + x_i)}$를 생성한다. 유효하지 않는 서명일 경우, 프로토콜을 중지한다.
   d) TA는 $\mu_i = E_{K_i}\{T \| A_i \| x_i \| GID\}$를 생성하고, μ_i를 V_i에게 보내준다. 그리고 (GID, A_i, C_{V_i})를 차량리스트에 저장한다.
3) V_i는 TA로부터 μ_i를 받으면, $D_{K_i}\{\mu_i\} =$

$(T'\|A_i\|x_i\|GID)$를 계산한다. V_i가 TA로 보냈던 T와 μ_i를 복호화 하여 획득한 T'가 같으면 $(T?=T')$, 비밀키 (A_i, x_i)와 그룹 ID GID를 저장한다.

4.2.3 메시지 서명 단계

차량이 서버로부터 받은 비밀키를 사용하여 메시지에 대한 서명을 생성하고, 메시지를 방송하는 단계이다. 차량 V_i에서 메시지 M에 대한 자세한 서명 방법은 다음과 같다.

1) V_i는 임의의 $\alpha, \beta \in Z_p^*$를 선택하고 다음 $T_1, T_2, T_3, \delta_1, \delta_2$를 계산한다.

$$T_1 = u^{\alpha}$$
$$T_2 = v^{\beta}$$
$$T_3 = A_i h^{\alpha+\beta}$$
$$\delta_1 = x_i \alpha$$
$$\delta_2 = x_i \beta$$

2) V_i는 임의의 $r_{\alpha}, r_{\beta}, r_{x_i}, r_{\delta_1}, r_{\delta_2} \in Z_p^*$를 선택하고 다음 $R_1 . R_2 . R_3 . R_4 . R_5$을 계산한다.

$$R_1 = u^{r_{\alpha}}$$
$$R_2 = v^{r_{\beta}}$$
$$R_3 = \hat{e}(T_3, g_2)^{r_{x_i}} \cdot \hat{e}(h, W)^{-r_{\alpha}-r_{\beta}} \cdot \hat{e}(h, g_2)^{-r_{\delta_1}-r_{\delta_2}}$$
$$R_4 = T_1^{r_{x_i}} \cdot u^{-r_{\delta_1}}$$
$$R_5 = T_2^{r_{x_i}} \cdot u^{-r_{\delta_2}}$$

3) 위 과정에서 계산된 값 $T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5$와 메시지 M, 그룹 ID GID를 사용하여, $c = H_3(M, GID, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$를 계산한다.

4) 다음의 $s_{\alpha}, s_{\beta}, s_{x_i}, s_{\delta_1}, s_{\delta_2}$를 계산한다.

$$s_{\alpha} = r_{\alpha} + c\alpha$$
$$s_{\beta} = r_{\beta} + c\beta$$
$$s_{x_i} = r_{x_i} + cx_i$$
$$s_{\delta_1} = r_{\delta_1} + c\delta_1$$
$$s_{\delta_2} = r_{\delta_2} + c\delta_2$$

5) M에 대한 서명은 $\pi = (T_1, T_2, T_3, c, s_{\alpha}, s_{\beta}, s_{x_i}, s_{\delta_1}, s_{\delta_1})$이다.

6) V_i는 GID, M, π를 방송한다.

4.2.4 메시지 확인 단계

메시지의 서명을 확인하여 유효성을 검증하는 단계이다. 한 차량에서 방송한 메시지를 주변 차량과 RSU가 메시지를 수신하면, 먼저 M에 포함된 시간 정보로 유효한 시간 내의 메시지인지 여부를 확인한다. 그리고 그룹 공개키를 사용하여 유효한 서명인지 확인한다.

1) 수신한 메시지의 서명 π를 이용하여 다음 $\overline{R_1}, \overline{R_2}, \overline{R_3}, \overline{R_4}, \overline{R_5}$를 계산한다.

$$\overline{R_1} = u^{s_{\alpha}} / T_1^c$$
$$\overline{R_2} = v^{s_{\beta}} / T_2^c$$
$$\overline{R_3} = \hat{e}(T_3, g_2)^{s_{x_i}} \cdot \hat{e}(h, W)^{-s_{\alpha}-s_{\beta}} \cdot \hat{e}(h, g_2)^{-s_{\delta_1}-s_{\delta_2}} \cdot (\hat{e}(T_3, W)/\hat{e}(g_1, g_2))^c$$
$$\overline{R_4} = T_1^{s_{x_i}} \cdot u^{-s_{\delta_1}}$$
$$\overline{R_5} = T_2^{s_{x_i}} \cdot v^{-s_{\delta_2}}$$

2) 위 과정에서 계산된 값들$(\overline{R_1}, \overline{R_2}, \overline{R_3}, \overline{R_4}, \overline{R_5})$과 메시지의 서명 π에 포함된 값들(T_1, T_2, T_3), GID, M을 이용하여 $\bar{c}$를 계산한다.
$\bar{c} = H_3(M, GID, T_1, T_2, T_3, \overline{R_1}, \overline{R_2}, \overline{R_3}, \overline{R_4}, \overline{R_5})$

3) 메시지의 서명 π에 포함된 c와 위 과정에서 계산된 $\bar{c}$를 비교하여 유효한 서명인지 확인하고, 유효한 서명이 아닐 경우 메시지를 무시한다.

4.2.5 신원 확인 단계

메시지의 서명으로부터 TA의 개인키에 의해 서명한 차량의 신원을 확인하는 단계이다. 문제를 일으킨 차량이나 사고 책임자는 TA에 의해 메시지의 익명성을 철회하여 차량의 신원을 확인할 수 있어야 하며,

TA는 다음 과정을 통해 차량의 신원을 확인한다.

1) $A_i = T_3/(T_1^{\xi_1} \bullet T_2^{\xi_2})$를 계산한다.
2) TA는 차량리스트에서 A_i를 검색하여 차량의 신원을 확인한다.

4.2.6 차량 철회 단계

TA에 의해 철회 차량의 신원이 확인되면, 그 차량을 VANET으로부터 철회하는 단계이다. TA가 철회 대상 차량을 확인하면, TA는 철회를 위한 메시지를 RSU에 전송한다. RSU는 TA로부터 받은 메시지를 차량에 전달하기 위해 방송한다. TA는 철회 대상 차량을 저장하기 위해 〔표 4〕와 같은 철회리스트를 관리한다.

일반적으로 어떤 특정 차량을 철회하기 위해서는 다른 차량에서 특정 차량을 구분하기 위한 인자가 필요하다. 하지만 차량의 익명성과 프라이버시를 위한 불연결성을 보장하기 위해서는 특정 차량을 구분할 수 있는 특정 인자가 메시지에 포함되면 안 된다. 따라서 각 차량에 하위 그룹의 ID *GID*를 사용하여 철회를 한다. 즉, 어떤 차량이 철회 대상 차량일 경우, 그 차량만 철회할 수 없기 때문에 그 차량이 소속된 그룹을 철회한다. *GID*를 통해 특정 차량을 구분할 수 없도록 하기 위해 여러 차량에 *GID*를 중복해서 발급한다.

*GID*를 사용하여 차량을 철회하는 방법은 두 가지 방법이 있다. 각 차량에서 차량 등록 단계를 다시 수행하여 *GID*를 갱신하는 방법과 TA에서 각 차량에 *GID*를 발급하는 방법이다. 두 가지 방법에 대한 과정은 다음과 같다.

1) 차량의 등록을 갱신하는 방법
   a) TA는 철회 대상 차량을 차량리스트에서 삭제하고, 철회리스트에 등록한다.
   b) 철회 대상 차량이 소속된 그룹이 GID_1이라고 하면, GID_1에 대한 철회 메시지를 RSU에 보내고, RSU는 철회 메시지를 방송한다.
   c) 철회 메시지를 수신한 차량은 소속된 그룹이 철회 대상 그룹인 GID_1일 경우, 차량 등록 단계를 다시 수행하여 새로운 *GID*를 발급 받는다. 소속된 그룹이 철회 대상 그룹인 GID_1이 아닐 경우, 철회 메시지를 무시한다.
   d) TA는 차량 등록 단계에서 등록 과정을 수행하는 차량이 철회 리스트에 포함되어 있을 경우, 비밀키와 *GID*를 발급하지 않고 프로토콜을 중지한다.
2) 새로운 *GID*를 방송하는 방법
   a) TA는 철회 대상 차량을 차량리스트에서 삭제하고, 철회리스트에 등록한다.
   b) 철회 대상 차량이 소속된 그룹이 GID_1이라고 하면, GID_1에 대한 철회 메시지를 RSU에 보내고, RSU는 철회 메시지를 방송한다. 그리고 철회 대상을 제외한 GID_1를 사용하는 차량들에게 새로운 그룹 ID를 암호화하여 철회 메시지와 함께 보낸다. 암호화에 사용하는 키는 철회 대상 차량을 제외한 GID_1를 이용하는 다른 차량들이 차량 등록 과정에서 사용한 대칭키를 사용하여 암호화한다.
   $E_{K_1}\{GID, C_{V_1}\}, \cdots, E_{K_n}\{GID, C_{V_n}\}$
   c) 철회 메시지를 수신한 차량은 소속된 그룹이 철회 대상 그룹인 GID_1일 경우, 새로 발급된 *GID*를 사용하고, 소속된 그룹이 철회 대상 그룹인 GID_1이 아닐 경우, 철회 메시지를 무시한다.
   d) 이후, 메시지에 GID_1이 포함된 메시지는 유효한 서명으로 확인되어도 무시한다.

〔표 4〕 TA에서 관리하는 철회리스트

철회 차량의 인증서	기간
C_6	T_1
C_7	T_2
C_8	T_3
⋮	⋮

V. 분석

이 장에서는 제안하는 프로토콜의 안전성과 효율성에 대해 분석한다. 분석에 앞서 VANET의 보안 요구사항들에 대해 살펴본 후, 제안하는 프로토콜이 보안 요구사항들을 만족하는지에 대한 안전성을 분석한다. 효율성 분석은 3장의 관련연구 중 그룹서명을 사용하는 기법인 Lin 등이 제안한 프로토콜, L. Zhang 등이 제안한 프로토콜과 연산량을 비교하여 분석한다.

5.1 보안 요구사항

앞서 설명한 바와 같이 VANET은 V2V와 V2I의 2가지 통신 기법을 사용한다. 본 절에서는 V2V와 V2I 통신에서 안전하고 신뢰성 있는 통신을 보장하기

위해 VANET에서 만족해야하는 보안 요구사항들을 정의한다.

- 메시지 인증(Message authentication): 메시지 수신자는 자신이 수신한 메시지가 정당한 사용자에 의한 것인지를 알 수 있어야 한다. 즉, 메시지를 수신한 차량은 차량의 프라이버시 보호를 위해 메시지를 방송한 차량의 신원은 알 수 없더라도, VANET 시스템에 등록된 차량인지 확인할 수 있어야 한다. 제안하는 프로토콜에서는 그룹서명을 사용하였기 때문에 메시지를 방송한 차량이 그룹에 소속된 차량인지 확인할 수 있어야 한다.
- 무결성(Integrity): 메시지 수신자는 자신이 수신한 메시지가 전송 중간에 위/변조 되었는지 확인할 수 있어야 한다. 메시지를 수신한 차량은 수신한 메시지의 payload, 서명 등이 공격자에 의해 위/변조 되었는지 확인할 수 있어야 한다.
- 부인방지(Non-repudiation): 사고와 같은 분쟁이 발생할 경우, 책임 회피를 방지하기 위해 자신이 보낸 메시지에 대해 부인할 수 없어야 한다. 어떤 차량에서 거짓 메시지를 방송하여 문제가 발생하면, TA는 방송한 메시지에 대해 부인할 수 없도록 그 차량에서만 생성할 수 있는 메시지임을 보여야 한다.
- 조건부 익명성(Conditional Anonymity): 일반 사용자의 프라이버시는 보호하면서 문제를 일으킨 차량이나 사고 책임자는 신뢰 기관에 의해 식별할 수 있어야 한다. 문제를 일으킨 차량에 대해서 TA는 메시지의 익명성을 철회하여 차량의 신원을 확인할 수 있어야 하며, 차량의 신원을 확인하는 과정에서 VANET에 참여하는 다른 일반 차량의 프라이버시는 보호되어야 한다.

위의 보안 요구사항을 바탕으로 VANET에서 강한 프라이버시를 지원하기 위해서는 다음 두 가지 요구사항을 만족해야 한다.

- 불관찰성(Unobservability): 개별 메시지에 대해 해당 메시지를 방송한 차량을 식별할 수 없어야 한다. 차량이 전파하는 메시지를 통해 누구나 신원을 확인할 수 있다면 프라이버시를 침해한다.
- 불연결성(Unlinkability): 같은 차량이 보낸 두 메시지를 서로 연결할 수 없어야 한다. 불연결성이 보장이 되면, 특정 메시지의 불관찰성이 깨졌을 경우 피해를 해당 메시지에 한정할 수 있다. 반대로 불연결성이 보장되지 않는다면, 하나의 메시지에 대한 불관찰성이 깨졌을 경우 해당 차량의 모든 메시지를 추적할 수 있다.

5.2 분석

5.2.1 안전성 분석

앞서 5.1절에서 살펴본 VANET의 보안 요구사항을 제안하는 프로토콜이 만족하는지에 대해 안전성을 분석한다.

- 메시지 인증: 각 차량은 차량 등록 단계에서 비밀키 (A, x)를 발급받고, 그 비밀키를 사용하여 서명을 한다. TA가 발급한 옳은 비밀키를 사용한 서명은, 그룹 공개키 $Q_G=(h, u, v, W)$를 통해 유효한 서명으로 확인된다. 즉, 그룹서명의 특성상 메시지 송신자가 누구인지는 확인할 수는 없지만, 그룹 내의 차량에 의한 메시지임을 확인할 수 있다.
- 무결성: 차량이 방송하는 메시지의 서명 $\pi=(T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{x_i}, s_{\delta_1}, s_{\delta_1})$에 포함되는 인자인 c는 M을 포함하여 $c=H_3(M, GID, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$와 같이 계산된다. 따라서 M이 중간에 M'으로 위/변조 된다면, 서명의 확인과정에서 생성하는 $\bar{c}$가 $\bar{c}=H_3(M', GID, T_1, T_2, T_3, \overline{R_1}, \overline{R_2}, \overline{R_3}, \overline{R_4}, \overline{R_5})$와 같이 계산된다. c와 $\bar{c}$가 다른 값을 가지면 유효하지 않는 서명으로 확인되므로, 서명 확인과정을 통해 무결성을 확인할 수 있다.
- 부인방지: 메시지 서명 단계에서 과정 1)의 인자인 δ_1, δ_2는 $\delta_1=x_i\alpha$, $\delta_2=x_i\beta$와 같이 차량 V_i에 발급된 비밀키 x_i를 포함하는 연산을 한다. 그리고 과정 3)의 인자인 $s_{x_i}, s_{\delta_1}, s_{\delta_2}$는 $s_{x_i}=r_{x_i}+cx_i$, $s_{\delta_1}=r_{\delta_1}+c\delta_1$, $s_{\delta_2}=r_{\delta_2}+c\delta_2$와 같이 M_i과 차량 V_i에 발급된 비밀키 x_i를 포함하는 연산을 한다. 따라서 서명 생성과정에 M_i에 대한 x_i가 포함된 서명 $\pi=(T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{x_i}, s_{\delta_1}, s_{\delta_1})$는 비밀키 x_i를 발급받은 차량만이 생성할 수 있다. 또한 제안하는 프로토콜에서 사용한 그룹서명의 성질에 따라 다른 차량의 서명은 생성할 수 없다. x_i에 대해서는 생성과정에 $x_i=H_3(r\|Q_{V_i})$와 같이 V_i의 공개키 Q_{V_i}가 포함이 되고, r은 TA의

차량리스트에 차량의 신원정보와 같이 저장된다. 때문에 x_i가 V_i에게 발급된 비밀키임을 TA는 확인시켜 줄 수 있다.

- 조건부 익명성: 문제를 일으킨 차량의 메시지는 TA에 전송된다. TA는 그 메시지의 서명으로부터 차량의 신원을 확인한다. TA의 개인키로 차량의 신원확인 단계의 $A_i = T_3/(T_1^{\xi_1} \cdot T_2^{\xi_2})$를 계산하여 차량의 신원을 확인할 수 있다.
- 불관찰성: 제안하는 프로토콜에서 각 차량은 TA로부터 비밀키 x_i와 함께 차량 ID A_i를 발급받는다. 그리고 서명과정에서 임의의 $\alpha, \beta \in Z_p^*$를 선택하고 $T_3 = A_i h^{\alpha+\beta}$와 같은 연산과정을 거친 후 사용되기 때문에 차량이 방송하는 메시지를 통해 송신한 차량을 식별할 수 없다.
- 불연결성: 차량의 서명인 $\pi = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{x_i}, s_{\delta_1}, s_{\delta_1})$의 모든 인자는 서명생성 과정에서 선택한 랜덤값과 연산과정을 거친다. 따라서 메시지에 대한 서명을 생성할 때마다 다른 값을 가진다. 그러므로 한 차량에서 서로 다른 두 메시지를 방송했을 때, 메시지 GID, M, π에서 같은 값을 가지는 인자는 GID만 남는다. GID는 한 차량에만 발급되는 값이 아닌 여러 차량에 중복해서 발급해주는 값이기 때문에 GID로서 같은 차량을 구분할 수 없다.

5.2.2 효율성 분석

효율성에 대한 분석은 제안하는 프로토콜과 기존의 그룹서명을 사용하는 방법인 Lin 등이 제안한 프로토콜, L. Zhang 등이 제안한 프로토콜의 요구되는 계산에 대한 연산횟수를 비교하였다. 연산횟수에 대한 분석은 차량이 1개의 RSU를 통과하며 1개의 메시지를 방송할 때 차량에서 발생하는 연산과 RSU를 1대의 차량이 1개의 메시지를 방송하며 통과할 때 RSU에서 발생하는 연산을 분석하였다. 제안하는 프로토콜과 Lin 등이 제안한 프로토콜, L. Zhang 등이 제안한 프로토콜에 대해서 〔표 5〕는 차량에서 발생하는 연산횟수를 나타내고 있으며, 〔표 6〕은 RSU에서 발생하는 연산횟수 나타내고 있다.

제안하는 프로토콜과 L. Zhang 등이 제안한 프로토콜은 차량 등록 단계에서 발생하는 연산횟수에 대한 분석이 가능하고, 차량에서 발생하는 연산량에 대해서는 두 프로토콜이 같은 연산횟수 가진다. 하지만 Lin 등이 제안한 프로토콜은 차량이 등록하는 과정을 자세히 서술하고 있지 않아서 차량 등록 단계에서 발생하는 연산량에 대한 비교분석을 할 수 없다. 따라서 〔표 5〕에는 세 프로토콜 모두 차량 등록 단계에서 발생하는 차량의 연산량을 제외하고 연산횟수를 비교하였다. 효율성 분석을 위해 제안하는 프로토콜과 기존의 그룹서명을 사용하는 기법인 Lin 등이 제안한 프로토콜, L. Zhang 등이 제안한 프로토콜의 연산횟수를 비교하여 보았을 때, 〔표 5〕와 〔표 6〕을 통해 제안하는 프로토콜이 기존의 두 프로토콜보다 효율적임을 확인할 수 있다.

차량에서 요구되는 연산량에 대해 차량이 1개의 RSU를 통과할 때를 가정하여 비교하였지만, 차량이 운행될 때는 여러 개의 RSU를 통과하고, 이에 따라 요구되는 연산량이 달라질 수 있다. 제안하는 프로토콜에서는 최초 차량 등록 단계를 수행한 후, 여러 개의 RSU를 통과하더라도 RSU마다 추가적인 차량 등록 단계가 필요하지 않다. 하지만 Lin 등의 프로토콜과 L. Zhang 등의 프로토콜에서는 RSU마다 차량 등록 단계를 수행하며, 그에 따라 차량과 RSU와의 빈번한 연산이 요구된다. 차량이 n개의 RSU를 통과한다고 할 때, Lin 등의 프로토콜과 L. Zhang 등의 프로토콜에서는 제안하는 프로토콜보다 $n-1$번의 차량 등록 단계를 더 수행하게 된다. 따라서 차량이 여

〔표 5〕 차량에서 발생하는 연산횟수 비교

	Lin	L. Zhang	제안 프로토콜
덧셈 연산	6	6	6
곱셈 연산	12	10	10
해쉬 연산	3	1	1
지수 연산	11	9	9
pairing 연산	4	3	3
XOR 연산	0	0	0
대칭키 암/복호화	0	0	0

단위: 회

〔표 6〕 RSU에서 발생하는 연산횟수 비교

	Lin	L. Zhang	제안 프로토콜
덧셈 연산	1	1	0
곱셈 연산	4	7	4
해쉬 연산	2	2	1
지수 연산	8	12	8
pairing 연산	4	6	4
XOR 연산	0	1	0
대칭키 암/복호화	0	1	0

단위: 회

러 개의 RSU를 통과하는 환경에서도 제안하는 프로토콜이 기존의 두 프로토콜보다 효율적이라고 할 수 있다.

기존의 연구들에서 차량은 서버와의 통신이 주기적으로 요구되는 환경이었으며, 서버와의 통신 때 철회 대상 차량을 철회하였다. 다량의 익명인증서를 발급받는 환경은 익명인증서를 재발급 받을 때 재발급을 거부하여 차량을 철회하였으며, RSU마다 차량 등록 과정을 수행해야 하는 환경은 RSU 간에 철회 정보를 공유하여 차량이 다른 RSU에 등록을 할 때 등록을 거부하여 차량을 철회하였다. 서버 및 RSU와의 빈번한 통신은 효율성을 떨어뜨리기 때문에 제안하는 프로토콜은 서버 및 RSU와의 주기적인 통신이 필요하지 않도록 하였다. 따라서 *GID*를 사용하여 실시간으로 차량을 철회시키는 방법을 제공하였다. 그러므로 기존 연구와 환경적인 차이가 있기 때문에 차량을 철회하는 방법에 대해 연산량의 비교가 어렵고, 기존연구들에 비해 제안하는 프로토콜의 차량 철회 과정의 효율성 정도를 유추하여 비교해본다.

제안하는 프로토콜에서 차량을 철회하는 방법 중 차량의 등록을 갱신하는 방법은 모든 차량에서 동시에 등록을 갱신하기 때문에 네트워크의 통신량과 서버의 연산량이 순간적으로 증가한다. 철회 대상 차량을 제외한 n개의 차량이 존재한다고 할 때, *GID*의 동기화를 위해 n개의 차량에서 동시에 차량 등록 과정을 서버에 요청하게 되며, 서버에서는 n번의 차량 등록 과정을 수행해야 한다. 새로운 *GID*를 발급하는 방법은 n개의 차량이 존재할 경우 *GID*에 대해 서버에서 n번의 암호화와 차량에서 최대 n번의 복호화의 연산이 필요하다. 기존 연구에서는 서버 및 RSU와의 다음번 요구되는 통신에서 차량이 철회되기 때문에 차량을 철회하기까지 시간 간격이 발생하고, 익명인증서를 계속 반복해서 사용할 경우나 RSU의 범위를 벗어나지 않고 작은 지역에서 운행하는 경우는 차량의 철회가 어렵다. 하지만 서버 및 RSU에서 철회리스트를 관리하고 철회 차량인지 비교하여 구분하기 때문에 철회에 필요한 연산량이 제안하는 프로토콜보다 비교적 적다고 할 수 있다.

철회과정의 제안하는 프로토콜의 차량 철회 방법은 기존 연구들의 차량 철회 방법에 비해 차량과 서버에서의 요구되는 연산량이 상대적으로 많으므로 비효율적이다. 하지만 기존 연구들의 차량 철회 방법보다 시간 지연 없이 즉시 철회가 가능하며, 보다 확실한 차량 철회를 제공한다.

VI. 결론

본 논문에서는 RSU의 의존성을 줄이고, 차량의 프라이버시를 강화한 그룹서명 기반의 인증 프로토콜을 제안하였다. 제안하는 프로토콜은 차량의 익명성을 RSU까지 확장하여 신뢰기관만 차량의 신원정보를 확인할 수 있도록 하였다. RSU가 차량의 신원정보를 확인할 수 없기 때문에, RSU 내에 저장된 정보가 어떠한 사고로 노출이 되더라도 차량의 신원정보가 보호될 수 있다. 그리고 보안 요구사항을 만족하는 안전한 통신을 위해 차량과 RSU 간에 어떠한 통신이 요구되지 않는다. 그러므로 어떤 RSU가 불능이 되어 역할을 할 수 없더라도 차량의 운행에 지장을 초래하지 않는다. 또한 차량이 빠르게 이동하는 VANET 환경에서 RSU와의 통신을 줄여, 기존 연구에 비해 차량 운행의 효율성을 높였다.

현재까지 제안된 그룹서명 방법은 보안 요구사항을 모두 만족시키지만, 서명 과정과 서명 확인과정에 pairing 연산이 많이 사용되기 때문에 연산량 측면에서 비효율적이다. 또한 기존의 제안된 프로토콜과 제안하는 프로토콜에서의 철회 방법도 비효율적이다. 향후에는 보안 요구사항을 모두 만족시키면서 효율적인 인증기법과 철회 방법에 대한 연구가 더 필요하다.

참고문헌

〔1〕 오종택, "미국의 5.9GHz 차세대 DSRC 주파수 및 표준화 현황," TTA Journal, No. 98, pp. 122-132, 2005년 3월.

〔2〕 강전일, 양대헌, 이석준, 이경희, "실행활 응용을 위한 짧은 그룹 서명 기법(BBS04)에 대한 연구," 정보보호학회논문지, 제 19권, 제 5호, pp. 3-15, 2009년 10월.

〔3〕 M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions," Proceedings of Eurocrypt 2003, Lecture Notes in Computer Science, Vol. 2656, pp. 614-629, 2003.

〔4〕 D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," Advances in Cryptology, Crypto 2004, Lecture Notes

in Computer Science, Vol. 3152, pp. 41-55, 2004.

〔5〕 D. Boneh and M. Franklin, "Identity-based Encryption from the Weil Pairing," Advances in Cryptology, Crypto 2001, Lecture Notes in Computer Science, Vol. 2139, pp. 213-229, 2001.

〔6〕 M. Raya and J. P. Hubaux, "Securing Vehicular Ad hoc Networks," Journal of Computer Security, Vol. 15, No. 1, pp. 39-68, Jan. 2007.

〔7〕 X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications," IEEE Transaction on Vehicular Technology, Vol. 56, No. 6, pp. 3442-3456. Nov. 2007.

〔8〕 R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," Proceedings - IEEE INFOCOM, pp. 1903-1911, Apr. 2008.

〔9〕 C. Zhang, X. Lin, R. Lu, and P. Ho, "RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks," IEEE International Conference on Communications, art. no. 4533317, pp. 1451-1457, May. 2008.

〔10〕 L. Sweeney, "K-ANONYMITY: A Model for Protecting Privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based System, Vol. 10, No. 5, pp. 557-570, Oct. 2002.

〔11〕 C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," Proceedings - IEEE INFOCOM, pp. 816-824, Apr. 2008.

〔12〕 A. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, "Practical Short Signature Batch Verification," Proceedings of CT-RSA, Lecture Notes in Computer Science, Vol. 5473, pp. 309-324, Apr. 2009.

〔13〕 L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A Scalable Robust Authentication Protocol for Secure Vehicular Communications," IEEE Transactions on Vehicular Technology, Vol. 59, No. 4, pp. 1606-1617, May. 2010.

〈著者紹介〉

임 원 우(Wonwoo Rhim) 학생회원
2010년 2월: 한양대학교 컴퓨터공학과(학사)
2010년 3월~현재: 한양대학교 컴퓨터공학과(석사과정)
〈관심분야〉 네트워크 보안, 암호기술 응용

김 종 식(Jongsik Kim) 정회원
2002년 2월: 한양대학교 컴퓨터공학과(학사)
2008년 3월~2008년 10월: 한양대학교 컴퓨터공학과(석사과정)
2009년 1월~현재: (주) 그래텍
〈관심분야〉 암호기술 응용, 키 관리

김 상 진(Sangjin Kim) 종신회원
1995년 2월: 한양대학교 전자계산학과(학사)
1997년 2월: 한양대학교 전자계산학과(석사)
2002년 8월: 한양대학교 전자계산학과(박사)
2003년 3월~현재: 한국기술교육대학교 컴퓨터공학부 부교수
〈관심분야〉 암호기술 응용

오 희 국(Heekuck Oh) 종신회원
1983년: 한양대학교 전자공학과(학사)
1989년: 아이오와주립대학 전자계산학과(석사)
1992년: 아이오와주립대학 전자계산학과(박사)
1993년~1994년: 한국전자통신연구원 선임연구원
1995년 3월~현재: 한양대학교 컴퓨터공학과 교수
〈관심분야〉 암호프로토콜, 네트워크 보안