情報保護學會論文誌
第19卷 第4號, 2009. 8

VANET를 위한 차량자체생성 조건부익명 인증시스템*

김 상 진,[1†] 임 지 환,[2] 오 희 국[2‡]
[1]한국기술교육대학교, [2]한양대학교

Self Generable Conditionally Anonymous Authentication System for VANET*

Sangjin Kim,[1†] Jihwan Lim,[2] Heekuck Oh[2‡]
[1]Korea University of Technology and Education, [2]Hanyang University

요 약

충돌회피, 협력운전과 같은 서비스를 차량 애드혹 네트워크(VANET, Vehicular Ad hoc NETwork)에서 제공하기 위해서는 차량 간 교환되는 메시지의 인증이 매우 중요하다. 하지만 일반 전자서명 기법을 사용할 경우에는 프라이버시 침해 문제가 발생할 수 있어, 조건부 익명성을 제공하는 인증시스템이 필요하다. 최근에 Zhang 등은 조작불가능한 하드웨어를 활용하는 VANET를 위한 조건부 익명 인증시스템을 제안하였다. 이 시스템은 차량에서 조건부 익명성이 보장되는 신원기반의 공개키 쌍을 생성하여 메시지를 서명하여 교환한다. 또한 많은 메시지를 효과적으로 검증하기 위해 일괄 확인 기법을 사용한다. 이 논문에서는 Zhang 등의 시스템을 다음 측면에서 개선한다. 첫째, 보다 효율적인 확률 서명기법을 사용한다. 둘째, Zhang 등과 달리 안전성이 증명된 일괄확인 기법을 사용한다. 이 밖에 키 철회 문제, 익명 철회 문제 등에 대한 효과적인 해결방안도 제시한다.

ABSTRACT

Messages exchanged among vehicles must be authenticated in order to provide collision avoidance and cooperative driving services in VANET. However, digitally signing the messages can violate the privacy of users. Therefore, we require authentication systems that can provide conditional anonymity. Recently, Zhang et al. proposed conditionally anonymous authentication system for VANET using tamper-resistant hardware. In their system, vehicles can generate identity-based public keys by themselves and use them to sign messages. Moreover, they use batch verification to effectively verify signed messages. In this paper, we provide amelioration to Zhang et al.'s system in the following respects. First, we use a more efficient probabilistic signature scheme. Second, unlike Zhang et al., we use a security proven batch verification scheme. We also provide effective solutions for key revocation and anonymity revocation problems.

Keywords: VANET, conditionally anonymity, batch verification

I. 서 론

컴퓨팅 기술과 무선 통신 기술의 발달로 통신 기반 구조를 사용하지 않고 자율적으로 구성되는 애드혹 네트워크에 대한 연구가 현재 꾸준히 이루어지고 있다. 특히, 최근에는 무선 통신을 지원하는 컴퓨팅 시스템을 차량에 설치하여 차량 간 통신을 통해 지능적인 서비스를 제공하는 차량 애드혹 네트워크에 대한 연구 및 표준화가 활발히 진행되고 있다[1-8]. VANET의 응용은 매우 다양하지만 그 중에도 충돌회피, 협력운전과 같이 차량 운행의 안전성을 높여주는 응용이 가장 가치가 높은 응용이 될 것으로 생각된다. 하지만 이와 같은 응용은 필요한 보안 요구사항이 충족되지 않으면 고의로 사고를 유발하는 등 그 위협이 매우 큰 서비스이다.

접수일(2009년 4월 7일), 게재확정일(2009년 6월 30일)
* 이 논문은 2008년도 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임. (KRF-2008-313-D01024)
† 주저자, sangjin@kut.ac.kr
‡ 교신저자, hkoh@hanyang.ac.kr

VANET에서는 안전 운행을 위해 가까운 차량 간에 메시지를 지속적으로 교환하게 되며, 메시지를 수신한 차량들은 메시지의 내용을 파악하여 안전 운행에 활용하게 된다. 예를 들어 사고가 발생할 경우에 뒤따라오는 차량들에게 자동적으로 경고 메시지를 보낼 수 있으며, 신호등이 없는 교차로, 차선 변경 시 메시지 교환을 통해 차량의 안전 운행을 도와 줄 수 있다. 하지만 허위 메시지는 차량 운행에 오히려 악영향을 줄 수 있다. 따라서 악의적인 행동을 한 차량을 식별하거나 사고 발생에서 책임자를 선별할 수 있는 방법이 필요하다. 이를 위해 VANET에서는 메시지를 발송한 차량을 인증할 수 있어야 한다. 이것을 지원하기 위한 가장 쉬운 방법은 모든 메시지를 전자서명하여 전달하는 것이지만 이 방법의 가장 큰 문제점은 사용자의 프라이버시가 침해될 수 있다는 것이다. 또 다른 문제점은 애드혹 네트워크에 적합한 공개키 기반구조가 아직 없다는 것이다. 물론 VANET에서는 기존 애드혹과 달리 RSU(Road Side Unit)를 통해 기반구조와 통신이 가능하지만 여전히 CRL(Certification Revocation List)이나 OCSP(Online Certification Status Protocol) 등과 같은 인증서 철회 메커니즘을 VANET에 사용하기에는 비용 측면에서 효과적이지 못한 메커니즘이다.

VANET에서 사용자 프라이버시를 위해 익명인증서나 익명식별자를 이용한 신원기반 시스템의 사용을 고려해 볼 수 있다. 하지만 프라이버시나 익명을 고려할 때 단일 메시지만을 생각하지 않는다. 즉, 불관찰성(unobservability) 뿐만 아니라 불연결성(unlinkability)이 함께 제공되어야 한다. 여기서 불연결성이란 동일 차량에 의한 여러 메시지를 서로 연결할 수 없어야 한다는 것을 말한다. 하나의 공개키를 사용할 경우에는 본질적으로 불연결성을 제공하기 어렵다. 이와 같은 문제점을 극복하기 위한 기존 연구는 크게 두 종류로 구분된다. 첫째는 다량의 익명 인증서를 차량에 유지하여 사용하는 것이다[1]. 하지만 유효기간 설정 문제 때문에 다량의 익명 인증서의 사용은 철회 메커니즘을 더욱 어렵게 만든다. 둘째는 그룹 서명(group signature)을 활용하는 것이다[2-3]. 그룹 서명은 조건부 익명성을 제공하는 기법이기 때문에 VANET에 어울리는 기법이지만 이 기법 역시 철회 메커니즘이 효과적이지 못하며, 그룹 서명 비용이 저렴하지 않기 때문에 효율성 측면에서도 문제가 있다.

이 논문에서는 Zhang 등이 제안한 기법[7]을 개선한 VANET를 위한 새로운 조건부익명 인증시스템을 제안한다. Zhang 등은 차량 OBU(On-Board Unit)에 조작불가능한(tamper-resistant) 하드웨어를 포함하고, 여기에 신원기반 시스템의 마스터키를 설치하여 차량 자체에서 신원기반 공개키 쌍을 매번 새롭게 생성하여 사용하고 있다. 이 논문도 같은 방식을 활용하지만 다음과 같은 차이점을 지니고 있다.

- 차이점 1. 보다 효율적인 확률적 전자서명 기법을 사용한다. Zhang 등[7]은 결정적 서명방식을 사용하며 서명확인에 3개의 겹선형 사상(bilinear pairing) 연산이 필요하다. 반면에 이 논문에서 사용하는 서명은 2개의 겹선형 사상 연산만 필요하다. 전자서명의 길이 측면에서도 Zhang 등과 마찬가지로 확인키를 포함하여 3개의 타원곡선 점(약 480비트)만 필요하다.
- 차이점 2. 안전성이 증명된 일괄확인 기법을 활용한다. 이 논문에서 사용되는 서명 기법은 기존에 일괄확인이 가능하지 않다고 주장된 기법이지만 이 논문에서는 안전하게 일괄 확인이 가능하다는 것을 보이고 있다. Zhang 등도 일괄확인 기법을 사용하고 있지만 안전성 증명되어 있지 않다.
- 차이점 3. 짧은 수명의 키를 사용하여 키 철회 문제를 해결한다.
- 차이점 4. 임계(threshold)방식을 통한 조건부 익명성 철회가 가능하다.

이 논문의 구성은 다음과 같다. 2장에서 이 논문의 바탕이 되는 수학적 배경, 이 논문에서 사용하는 전자서명 기법, 이 논문과 관련된 기존 VANET 연구 결과를 소개한다. 3장에서는 이 논문에서 제안한 VANET를 위한 새 V2V(Vehicle-to-Vehicle) 통신 기법을 소개한다. 4장에서 제안된 기법을 분석하고, 5장에서 결론과 향후 연구방향을 제시한다.

II. 연구 배경

2.1 수학적 배경

$G=\langle P\rangle$는 위수가 소수 q인 타원곡선 기반의 덧셈군이라 하고, G_q는 위수가 소수 q인 곱셈순환군이라 하자. 그러면 G와 G_q에서 겹선형 사상 $\hat{e}$는 다음과 같이 정의된다.

정의 1. (겹선형 사상) 다음 3 가지 조건을 만족하는

$\hat{e}: G\times G\rightarrow G_q$를 사용가능 겹선형 사상(admissible bilinear map)이라 한다.

조건 1. 겹선형(bilinear): 임의의 P, Q, $R\in G$에 대해 다음을 만족해야 한다.

- $\hat{e}(P,Q+R)=\hat{e}(P,Q)\cdot\hat{e}(P,R)$
- $\hat{e}(P+Q,R)=\hat{e}(P,R)\cdot\hat{e}(Q,R)$

조건 2. 비퇴화성(non-degenerate): G의 모든 쌍 P, Q에 대해 $\hat{e}(P,Q)\neq O$이어야 한다. 여기서 O는 G의 영원이다.

조건 3. 계산 효율성(computable): G의 임의의 쌍 P, Q에 대해 $\hat{e}(P,Q)$를 계산할 수 있는 효율적인 알고리즘이 있어야 한다.

이 논문에서 사용하는 $G=\langle P\rangle$에서는 다음 문제들이 계산적으로 어렵다고 가정한다.

- 이산대수 문제: G의 원소 P와 aP가 주어졌을 때 a를 계산하는 문제.
- 계산적 DH(Diffie-Hellmna) 문제: G의 원소 P, aP, bP가 주어졌을 때 abP를 계산하는 문제.
- 변형 계산적 DH 문제(computational co-DH problem): P, aP, Q가 주어졌을 때 aQ를 계산하는 문제.

2.2 관련 기초 암호알고리즘

Boneh 등은 겹선형 사상을 이용한 다음과 같은 짧은 서명(short signature)을 제안하였다[9].

- 사용자의 서명 및 확인키: $x\in_R Z_q^*$를 서명키로 선택하고 공개키는 $Q=xP$가 된다.
- 서명 알고리즘: 서명키 x를 이용한 메시지 $m\in\{0,1\}^*$에 대한 서명은 $R=H_1(m)$를 계산한 다음에 서명값 $\sigma=xR$를 계산한다. 여기서 $H_1:\{0,1\}^*\rightarrow G$은 충돌회피 해쉬함수이다.
- 확인 알고리즘: 확인키 Q, 메시지 m, 서명 σ가 주어졌을 때 서명의 검증은 다음을 이용한다.

$$\hat{e}(H_1(m),Q)\stackrel{?}{=}\hat{e}(\sigma,P)$$

이 서명의 결과 값은 타원곡선 위의 한 점이므로 서명값을 표현하는데 160비트 정도 필요하며, 일반 RSA 서명의 1024비트나 DSA의 320비트에 비해 짧아 짧은 서명이라고 이들은 명명하였다. 이 서명의 안전성은 변형 계산적 DH 문제에 기반하고 있다.

Bellare 등은 여러 서명을 하나의 서명 확인 비용으로 확인할 수 있도록 해주는 일괄 확인(batch verification)에 대해 처음으로 체계적으로 형식화하였다[10]. 이들이 제안한 것 중 작은 지수 검사(small exponent test)를 이용하면 사용하는 지수의 길이가 l일 때 개별 검증에서 실패하는 인스턴스가 일괄 확인 집합에 포함되어 있더라도 일괄확인을 통과할 확률은 2^{-l}이 된다.

2.3 이 논문에서 사용되는 전자서명 알고리즘

차량에 PKG의 마스터키를 포함하는 방식을 사용하기 위해서는 일괄확인이 가능한 효율적이고 안전성이 증명된 신원기반의 전자서명 기법이 필요하다. 현재 겹선형 사상을 기반으로 하는 신원기반의 전자서명의 경우 서명 검증을 위해 2개의 겹선형 사상 연산만 사용하는 것이 가장 효율적인 기법들이다[11-13]. 이 논문에서는 이 중 가장 효율적이고 일괄확인이 가능한 차재춘과 천정희가 제안한 다음과 같은 신원기반 전자서명 알고리즘을 사용한다[11].

- PKG(Private Key Generator) 마스터키 및 공개키: $s\in_R Z_q^*$를 마스터키로 선택하고 공개키는 $P_{pub}=sP$가 된다.
- 사용자의 서명 및 확인키: $Q_{ID}=H_1(ID)$가 확인키이고, 서명키는 $D_{ID}=sQ_{ID}$가 된다.
- 서명 알고리즘: 서명키 D_{ID}를 이용한 메시지 $m\in\{0,1\}^*$에 대한 서명은 $r\in_R Z_q^*$를 선택한 다음 $U=rQ_{ID}$를 계산하고, $w=H_2(m\|U)$와 $\sigma=(r+w)D_{ID}$를 계산한다. 결과 서명값은 $\langle U,\sigma\rangle$쌍이다. 여기서 $H_2:\{0,1\}^*\rightarrow Z_q^*$은 충돌회피 해쉬함수이다.
- 확인 알고리즘: 확인키 Q_{ID}, 메시지 m, 서명 $\langle U,\sigma\rangle$가 주어졌을 때 서명의 검증은 다음을 이용한다.

$$\hat{e}(U+wQ_{ID},P_{pub})\stackrel{?}{=}\hat{e}(\sigma,P)$$

이 서명은 타원곡선 위에 두 개의 점으로 표현되므로 서명을 표현하기 위해서는 Boneh 등의 짧은 서명의 두 배인 320비트 정도가 필요하다. 이 서명의 안전성은 [11]에 증명되어 있다.

이 서명은 [12]에서 다음과 같은 공격이 가능하기 때문에 일괄확인이 가능하지 않다고 주장되고 있다. 두 서명자의 공개키가 각각 $Q_1 = H_1(ID_1)$과 $Q_2 = H_1(ID_2)$일 때, 메시지 m_1과 m_2에 대한 각각 서명을 다음과 같이 설정하면, 각 개별 서명은 유효하지 않지만 결합하여 확인할 경우에는 유효한 서명이 된다.

$$U_1 = r_1 Q_1,\ w_1 = H_2(m_1 \| U_1)$$
$$\sigma_1 = (r'_2 + w_2) D_2$$
$$U_2 = r_2 Q_2 - w_1 Q_1 - r_1 Q_1,\ w_2 = H_2(m_2 \| U_2)$$
$$\sigma_3 = r''_2 D_2$$
$$\hat{e}(U_1 + w_1 Q_1 + U_2 + w_2 Q_2, P_{pub}) ? = \hat{e}(\sigma_1 + \sigma_2, P)$$

여기서 $r_2 = r'_2 + r''_2$이다.

하지만 이 서명의 경우에도 Bellare 등의 기법[10]을 활용하면 안전하게 일괄 확인이 가능하며 위와 같은 공격이 가능하지 않다. Q_i, m_i, U_i, σ_i가 하나의 일괄 확인할 인스턴스이고 총 n개가 주어졌고, 확인자가 선택한 지수 값들이 δ_1, ..., δ_n일 때 일괄 확인 식은 다음과 같다.

$$\hat{e}(\sum_{i=1}^{n} \delta_i (U_i + w_i Q_i), P_{pub}) ? = \hat{e}(\sum_{i=1}^{n} \delta_i \sigma_i, P) \qquad (1)$$

이 식의 정확성은 다음을 통해 확인할 수 있다.

$$\hat{e}(\sum_{i=1}^{n} \delta_i (r_i Q_i + w_i Q_i), sP) ? = \hat{e}(\sum_{i=1}^{n} \delta_i (r_i + w_i) D_i, P)$$
$$\hat{e}(\sum_{i=1}^{n} \delta_i (r_i + w_i) Q_i, P)^s ? = \hat{e}(s \sum_{i=1}^{n} \delta_i (r_i + w_i) Q_i, P)$$
$$\hat{e}(\sum_{i=1}^{n} \delta_i (r_i + w_i) Q_i, P)^s ? = \hat{e}(\sum_{i=1}^{n} \delta_i (r_i + w_i) Q_i, P)^s$$

유효하지 않은 인스턴스가 포함되어 있을 때 이 일괄 확인이 통과될 확률은 다음과 같이 계산할 수 있다. 일괄확인은 식 (1)을 이용하므로 $Q'_i = U_i + w_i Q_i$, $\sigma = s\sigma'$라 할 때 일괄확인을 통과하였으면 다음이 성립함을 의미한다.

$$\delta_1 Q'_1 + \cdots + \delta_n Q'_n = \delta_1 \sigma'_1 + \cdots + \delta_n \sigma'_n$$
$$\sum_{i=1}^{n} \delta_i (Q'_i - \sigma'_i) = 0$$
$$\delta_1 (Q'_1 - \sigma'_1) = -\sum_{i=2}^{n} \delta_i (Q'_i - \sigma'_i)$$

$\gamma_i = Q'_i - \sigma'_i$라 하면 $\delta_1 = -\gamma_1^{-1} \sum_{i=2}^{n} \delta_i \gamma_i$이 된다. 따라서 δ_2, ..., δ_n이 정해졌을 때 일괄확인 식을 충족하기 위해 $\delta_1 = -\gamma_1^{-1} \sum_{i=2}^{n} \delta_i \gamma_i$가 되어야 하며, δ_1이 이 조건을 만족할 확률은 δ_1이 l비트일 때 2^{-l}이다.

2.4 관련연구

Raya와 Hubaux는 다량의 익명인증서를 사용하는 시스템을 제안하였다[1]. 각 차량은 초기에 다량의 익명인증서와 인증기관의 인증서가 설치된 상태이며, 주기적으로 다량의 익명인증서를 발급받아 교체해야 한다. 따라서 차량에 많은 저장공간이 요구되며, 일반 인증서 철회 방법을 사용할 경우에는 CRL 크기가 매우 커지는 문제점을 지니고 있다. 이것을 완화하기 위해 인증서의 유효기간을 짧게 만들 수 있지만 인증서가 발급될 시점과 사용될 시점이 다르므로 짧은 유효기간을 가진 인증서를 차량에 저장하는 것은 가능하지 않다. 이 때문에 인증기관이 철회될 인증서를 보유한 차량에 메시지를 보내어 해당 인증서를 사용할 수 없도록 하는 방법을 제안하고 있다. 하지만 차량의 위치를 찾아 메시지를 전송하는 것은 간단한 문제가 아니며, 해당 메시지가 도달되지 못하도록 차단할 경우에는 철회가 적절히 이루어진다는 것을 보장하기 어렵다.

Lin 등은 Boneh 등의 그룹서명[14]과 신원기반을 활용한 시스템을 제안하였다[2]. 이 시스템에서 차량 간 통신은 그룹서명을 사용하고, RSU가 차량에게 메시지를 전달할 때에는 일반 신원기반 서명기법을 사용하고 있다. Boneh 등[14]은 그들의 논문에서 제안하는 그룹서명이 VANET에서 효과적으로 사용될 수 있음을 제시하고 있었으므로 Lin 등은 이것을 구체화한 것이다. 그룹서명을 사용할 경우에는 조건부 익명성을 제공할 수 있지만 개인키가 노출된 차량을 철회하기 위한 메커니즘이 효율적이지 못한 문제점이 있으며, Boneh 등의 서명은 영지식 기술을 이용하는 서명이므로 서명자체가 효율적이지도 못하다.

Calandriello 등[3]도 Lin 등과 마찬가지로 그룹서명 기법을 사용하지만 그룹서명을 사용하여 메시지를 서명하여 교환하는 것이 아니라 각 차량은 그룹서명키를 이용하여 익명인증서를 스스로 만들어 사용하는 방법을 제안하고 있다. 자체적으로 불연결성을 제공하는 익명의 공개키 쌍을 지속적으로 생성하여 사용할 수 있다는 장점을 지니고 있지만 생성된 익명인증서를 사용하기 위해서는 인증서를 확인하기 위해 그룹서명을 확인해야 하고 익명인증서를 이용하여 서명된 메시지를 확인해야 한다. 따라서 각 메시지를 확인하

기 위한 비용이 비교적 크다.

Xi 등은 센서 네트워크에서 사용된 랜덤 키 사전 분배 기법을 응용한 시스템을 제안하고 있다[4]. Xi 등의 제안은 차량 간의 통신보다는 차량과 RSU 간의 통신에 초점이 맞추어져 있으며, 차량에 사전에 키 풀로부터 일정한 개수의 키를 랜덤하게 선택하여 설치하여 이 키를 이용하여 RSU가 차량을 인증하는 방법을 제안하고 있다.

Lu 등은 차량이 이동하면서 RSU로부터 짧은 수명의 인증서를 받아 사용하는 시스템을 제안하고 있다[5]. 하지만 차량은 항상 동일한 익명ID를 이용하여 인증서를 RSU로부터 발급받기 때문에 RSU들이 수집한 정보를 이용하면 불연결성이 제공되지 않는 문제점을 지니고 있다. 다만, 짧은 수명의 인증서를 통해 철회 문제에 효과적으로 해결하고 있다.

Lin 등은 TESLA를 이용하여 기존 다량 익명 인증서를 사용하는 기법을 개선하고자 하였다[6]. Lin 등은 하나의 익명 인증서를 일정한 기간 동안 여러 번 사용하기 위해 각 익명 인증서마다 해쉬체인을 생성하고 TESLA 방식을 활용하는 기법을 제안하고 있다. 하지만 해쉬체인의 루트를 주기적으로 방송해야 하며, 해쉬체인의 특성상 해쉬체인 내에서는 불연결성을 제공할 수 없다는 문제점을 지니고 있다.

Zhang 등은 신원기반 시스템의 PKG의 마스터키를 조작불가능한 하드웨어에 포함하여 차량에 설치하고, 이를 이용하여 신원기반 공개키 쌍을 차량에서 직접 만들어 사용하는 방법을 제안하고 있다[7]. 따라서 이 제안은 Calendriello 등이 제안한 기법과 마찬가지로 차량에서 자체적으로 불연결성을 제공하는 익명의 공개키 쌍을 지속적으로 생성하여 사용할 수 있다. Zhang 등은 또한 일괄확인 서명 기법을 통해 서명들을 개별적으로 확인하지 않고 모아서 하나의 서명을 확인하는 비용으로 검증하여 효율성을 높이고자 하였다. 하지만 일괄확인 서명 기법은 서명들이 모두 유효할 경우에는 효율성을 높일 수 있는 수단이 되지만 일괄확인할 때 잘못된 서명이 포함되어 있을 경우에는 이를 식별하는 것이 어렵다는 문제점이 있다.

Zhang 등은 교통량이 많을 경우에는 짧은 시간 내에 서명된 많은 메시지를 각 차량이 확인해야 하는 문제점을 개선하기 위해 RSU의 도움을 받는 기법을 제안하고 있다[8]. 하지만 RSU가 차량보다 계산능력이 뛰어나기 때문에 RSU의 도움을 받는 것이 아니라 여러 차량이 동일한 메시지의 서명을 각자 확인하는 기존 방법의 중복성을 개선하고자 한 것이다. 이를 위해 Zhang 등은 차량이 RSU와 키 확립 프로토콜을 통해 세션키의 공유를 가정하고 이를 이용하는 방법을 제안하고 있다. 하지만 교통량이 많을 경우에는 RSU의 부하가 클 수 있으며, 각 RSU가 담당하는 영역의 크기가 작을 경우에는 오히려 이와 같은 세션키의 확립은 오버헤드로 작용할 수 있다. Zhang 등은 같은 논문에서 RSU의 도움을 받을 수 없는 경우 COMET이라는 협력 인증시스템을 추가로 제안하였다. 이 방식은 각 차량에서 정해진 확률에 따라 수신한 메시지를 검증하여 각 차량에서 많은 서명을 중복으로 확인하는 비용을 줄였다.

III. 제안하는 시스템

3.1 시스템 모델

3.1.1 조작불가능한 하드웨어

차량은 비용 측면에서 조작불가능한 하드웨어를 충분히 활용할 수 있으며, 암호키들을 안전하게 유지하기 위해 조작불가능한 하드웨어의 사용은 오히려 권장되어야 한다. 즉, 차량의 개인키와 같은 각 종 암호키들은 안전성을 위해 조작불가능한 하드웨어에 유지할 필요가 있다. 하지만 Zhang 등[7]은 이와 같은 개인적인 암호키뿐만 아니라 신원기반 시스템의 PKG의 마스터 키를 조작불가능한 하드웨어에 유지하고 있다. 조작불가능한 하드웨어가 절대적으로 안전하면 마스터키의 노출은 보안위협으로 생각하지 않아도 되며, 현재 하드웨어 기술을 고려할 때 이 가정은 충분히 현실성이 있는 가정이다. 다만, 이와 같은 환경에서 마스터 키의 변경이 필요하면 모든 차량에 설치되어 있는 조작불가능한 하드웨어를 교체해야 한다. 그러나 신원기반 시스템에서 마스터 키의 변경은 모든 공개키의 변경을 의미하므로 이와 같은 환경이 아니더라도 신원기반 시스템에서 마스터 키의 변경은 많은 문제점을 발생시킨다. 이것은 일반 PKI에서 인증기관의 공개키의 변경이 어려운 것과 유사하다. 이와 같은 근거에 따라 조작불가능한 하드웨어에 PKG의 마스터키를 포함하여 차량에 설치하는 것은 충분히 고려될 수 있는 방식임을 알 수 있다. 따라서 본 논문에서는 Zhang 등[7]과 마찬가지로 PKG의 마스터키를 조작불가능한 하드웨어에 포함하여 차량 내부 컴퓨팅시스템에 설치하여 사용한다.

3.1.2 조건부 익명성

VANET에서 프라이버시를 지원하지만 사고나 공격의 책임자를 식별하기 위해서는 조건부 익명성을 제공해야 한다. Zhang 등[7]은 이를 위해 차량의 실제 ID를 PKG의 공개키로 암호화하고 그 결과 암호문을 신원기반의 ID로 간주하여 다시 신원기반 공개키 쌍을 생성하고 있다. 따라서 PKG는 ID로 사용된 암호문을 복호화하여 언제든지 실제 차량을 식별할 수 있다. 하지만 Zhang 등에서는 차량에 설치된 마스터키에 대응되는 공개키로 실제 ID를 암호화하고 있어 권한 남용을 막기 위해 비밀공유 기법의 사용이 어렵다[1]1). 그런데 실제 이 공개키로 암호화할 특별한 이유가 없다. 차량에 설치된 다른 공개키로 암호화할 수 있으며, 이 공개키에 대응되는 개인키는 권한 남용을 방지하기 위해 임계방식(threshold)의 비밀공유 기법을 활용하여 여러 기관이 분산 공유해야 한다. 이 암호화의 정당성을 보장할 방법이 필요하다고 주장할 수 있지만 암호문을 제공하는 모듈과 이 암호문을 바탕으로 익명공개키 쌍을 만드는 모듈 간에 교환은 외부에서 조작될 수 없다고 가정하면 공격자가 임의로 만든 암호문을 기반으로 익명ID를 만드는 것은 가능하지 않다고 가정할 수 있다.

3.1.3 시스템 가정

이 논문에서는 차량 간 통신에 초점을 맞추어 차량 간에 통신할 때 사용할 수 있는 익명 공개키 쌍을 차량에서 자체적으로 생성하는 방법을 제안한다. 이 방법은 기존 Zhang 등이 제안한 방법과 유사하다. 즉, 이 논문은 기존 Zhang 등[7]의 제안을 개선한 논문이다.

이 논문에서는 행정부에 소속된 차량등록기관, 사법부에 소속된 익명철회기관, 다수의 차량의 참여를 가정한다. VANET에는 이 외에 도로에 설치된 RSU가 있지만 본 논문에서는 RSU와 차량 간의 통신은 고려하지 않는다. 실제 차량에서 RSU로의 통신은 차량간 통신과 동일한 방법으로 진행될 수 있으며, RSU에서 차량 간 통신은 익명성이 요구되지 않으므로 기존 보안 메커니즘을 사용하여도 무방하다.

1) 개인키를 비밀분산공유 기법을 통해 생성한다는 것은 누구도 직접적으로 개인키를 얻을 수 없다는 것을 의미하며, 각 참여자는 자신의 몫(share)만 유지한다.

3.2 제안하는 프로토콜

3.2.1 표기법

본 논문에서는 2.1 수학적 배경에서 제시된 표기법과 [표 1]에 제시된 표기법을 사용하여 시스템과 프로토콜을 기술한다.

[표 1] 표기법

표기	의미
s_R	차량등록기관의 마스터키
s_T	(t,n) 임계방식으로 비밀 공유된 익명철회기관의 개인키
$P_R = s_R P$	차량등록기관의 공개키
$P_T = s_T P$	익명철회기관의 공개키
RID	차량의 실제 ID
$H_3 : G \rightarrow \{0,1\}^k$	충돌회피 해쉬함수

3.2.2 시스템 설정

$G=\langle P\rangle$는 타원곡선 위의 점 P에 의해 생성되는 위수가 소수 q인 덧셈군이며, G_q는 위수가 소수 q인 곱셈 순환군이고, $\hat{e}: G\times G\rightarrow G_q$는 두 군에서 동작하는 겹선형 사상이다. 이 군에서 계산적 DH 문제가 어려울 정도로 q가 충분히 커야 한다. 전체 VANET를 관리하는 별도 기관이 이와 같은 군들을 설정한다. 차량등록기관은 마스터키 $s_R \in_R Z_q^*$를 임의로 선택하고, 공개키 $P_R = s_R P$를 계산하여 공개한다. 익명철회기관은 임계방식으로 적절한 기관과 비밀 공유 기법을 통해 마스터키를 설정하고 공개키 $P_T = s_T P$를 계산하여 공개한다. 각 차량은 등록 과정에서 차량의 OBU에 다음이 설치되며, 이들 정보들은 조작불가능한 하드웨어에 유지된다.

- 차량등록기관의 마스터키: s_R
- 익명철회기관의 공개키: P_T
- 차량의 실제 ID: RID

3.2.3 익명 공개키 쌍 생성

조건부 익명성을 제공해야 하므로 Zhang 등[7]과 동일한 방법으로 차량의 실제 식별자를 다음과 같이 암호화한다.

$PID_1 = rP,\ PID_2 = RID \oplus H_3(rP_T)$

여기서 $r \in_R Z_q^*$은 암호화할 때 선택한 랜덤요소이다. 그 다음 결과 암호문을 신원기반 시스템의 식별자로 간주하여 공개키를 다음과 같이 생성한다.

$Q = H_1(PID_1 \| PID_2 \| T_S \| T_E)$

여기서 T_S는 공개키의 시작시간이고, T_E는 공개키의 만료기간이다. 공개키를 생성한 다음 차량등록기관의 마스터키를 이용하여 개인키 $D = s_R Q$를 생성한다. 이 과정은 모두 조작불가능한 하드웨어 내에서 이루어져야 한다.

차량에 GPS(Global Positioning System)가 설치되어 있어 각 차량이 절대 시간에 정확한 시간 동기화가 가능하고 고정된 유효기간을 사용하면 T_S와 T_E 대신에 시작시간만 사용할 수 있다. 두 경우 모두 유효기간은 매우 짧게 설정한다. 이것은 철회 문제를 효과적으로 해결하기 위함이다. 유효기간이 짧으면 인증서철회목록 자체가 필요 없게 된다. 프라이버시 측면에서는 각 차량에서 생성된 공개키쌍마다 하나의 메시지만 서명하는 것이 가장 좋지만 이 경우 공개키 생성 비용이 많이 소요되므로 생성된 공개키마다 일정한 작은 개수의 메시지에 서명하는 것이 바람직하다.

3.2.4 V2V 통신

RSU는 정기적으로 비콘(beacon) ϕ를 방송한다. 이 값에는 RSU의 식별자, 최신성 정보(nonce) 등을 포함한다. 각 차량은 메시지 m를 이웃 차량들에게 방송하고 싶으면 다음과 같이 최근에 생성한 익명 공개키 쌍을 이용하여 서명을 생성한다.

- 단계 1. $r \in_R Z_q^*$를 선택하고 $U = rQ$를 계산한다.
- 단계 2. $w = H_2(m \| U \| \phi)$와 $\sigma = (r + w)D$를 계산한다.

서명을 생성할 때 ϕ를 포함하는 것은 각 개별 메시지의 사용가능한 지리적 위치를 제한하기 위함이다. 그 다음 m, U, σ, PID_1, PID_2, T_S, T_E를 함께 방송한다. 이것을 수신한 차량은 다음과 같은 순서로 메시지를 확인한다.

- 단계 1. T_S와 T_E를 이용하여 유효기간을 확인한다.
- 단계 2. 수신한 값들을 이용하여 다음을 계산한다.

$Q = H_1(PID_1 \| PID_2 \| T_S \| T_E)$

- 단계 3. $w = H_2(m \| U \| \phi)$를 계산한 후에 다음과 같이 서명을 확인한다.

$\hat{e}(U + wQ, P_R) \stackrel{?}{=} \hat{e}(\sigma, P)$

차량은 n개의 메시지 m_i, U_i, σ_i, $PID_{i,1}$, $PID_{i,2}$, $T_{i,S}$, $T_{i,E}$를 다음과 같이 일괄 확인할 수 있다.

- 단계 1. 모든 $T_{i,S}$와 $T_{i,E}$를 이용하여 모든 공개키의 유효기간을 확인한다.
- 단계 2. 수신한 값들을 이용하여 다음을 계산한다.

$Q_i = H_1(PID_{i,1} \| PID_{i,2} \| T_{i,S} \| T_{i,E})$

- 단계 3. $w_i = H_2(m_i \| U_i \| \phi)$를 계산하고 $\delta_1, \ldots, \delta_n \in_R \{0,1\}^l$를 선택한 후에 다음과 같이 일괄로 서명을 확인한다.

$\hat{e}(\sum_{i=1}^{n} \delta_i (U_i + w_i Q_i), P_R) \stackrel{?}{=} \hat{e}(\sum_{i=1}^{n} \delta_i \sigma_i, P)$

뿐만 아니라 [8]에서 제안한 것처럼 각 차량에서 중복하여 모든 메시지를 일괄확인하는 것이 아니라 RSU가 대신 일괄확인한 후에 결과 정보만 각 차량에게 보내주는 방식을 사용할 수도 있다.

IV. 분 석

이 논문에서 사용하는 전자서명 기법은 2장에서 설명한 바와 같이 계산적 DH 문제에 의존하는 서명기법이며, 적응적 선택 메시지 공격에 대해 강건하다는 것이 증명된 전자서명이다[11]. 이 전자서명은 [12]에서 결합하여 확인할 수 없는 전자서명이라고 주장되었지만 [10]에서 제시된 기법을 사용하여 안전하게 일괄 확인할 수 있음을 2장에서 보였다.

차량은 자체적으로 공개키를 생성할 때마다 서로 연결할 수 없는 암호문을 입력값으로 사용하기 때문에 한 차량에서 사용되는 공개키들은 불연결성을 제공한다. 하지만 이 암호문은 차량의 실제 ID를 암호화하여 만들기 때문에 필요하면 이를 복호화하여 익명을 철회할 수 있다. 정의된 방법이 아닌 다른 방법으로 공개키가 생성될 경우에는 익명 철회가 이루어지지 않

을 수 있다. 하지만 제안한 시스템은 익명 공개키 쌍을 조작불가능한 하드웨어 내에서 만들기 때문에 이와 같은 공격은 가능하지 않다.

[7]에서 사용된 다음과 같은 전자서명 기법과 제안한 시스템에서 사용하는 기법과 비교 분석하여 보자.

- PKG(Private Key Generator) 마스터키 및 공개키: $s_1, s_2 \in_R Z_q^*$를 마스터키로 선택하고 공개키는 $P_{pub1} = s_1 P$와 $P_{pub2} = s_2 P$가 된다.
- 사용자의 서명 및 확인키: $Q_1 = H_1(ID\|1)$과 $Q_2 = H_1(ID\|2)$가 확인키이고, 서명키는 각각 $D_1 = s_1 Q_1$과 $D_2 = s_2 Q_2$이다. 실제 논문에서는 Q_1과 Q_2를 다르게 생성하지만 비교를 위해 이렇게 가정하여도 차이가 없다.
- 서명 알고리즘: 서명키 D_1과 D_2를 이용한 메시지 $m \in \{0,1\}^*$에 대한 서명은 $w = H_2(m)$를 계산한 다음 $\sigma = D_1 + wD_2$를 계산한다.
- 확인 알고리즘: 확인키 Q_1과 Q_2, 메시지 m, 서명 σ가 주어졌을 때 서명의 검증은 다음을 이용한다.

$$\hat{e}(Q_1, P_{pub1})\hat{e}(wQ_2, P_{pub2}) ?= \hat{e}(\sigma, P)$$

- 일괄확인 알고리즘: m_i, σ_i, $Q_{i,1}$, $Q_{i,2}$이 일괄확인 인스턴스일 때 다음 식을 이용하여 일괄확인 한다.

$$\hat{e}(\Sigma Q_{i,1}, P_{pub1})\hat{e}(\Sigma w_i Q_{i,2}, P_{pub2}) ?= \hat{e}(\Sigma\sigma, P)$$

이 서명은 다음과 같은 문제점을 지니고 있다.

- 첫째, 결정적 서명방식이다.
- 둘째, 일회용으로만 사용가능하다. 같은 서명키로 두 메시지에 서명을 하였을 경우 누구나 다음과 같이 사용자의 서명키를 계산할 수 있다. $w_1 = H_2(m_1)$과 $w_2 = H_2(m_2)$이고 결과 서명이 σ_1과 σ_2일 때, $D_2 = (w_1 - w_2)^{-1}(\sigma_1 - \sigma_2)$이다.

물론 [7]에서 한번 생성된 키로 하나의 메시지만 서명하기 때문에 일회용 서명이라는 것이 문제가 안 될 수 있지만 공개키 쌍을 메시지마다 새롭게 생성하는 것보다 한번 생성된 공개키를 최소 몇 번 사용하는 것이 보다 효율적이다. 하지만 [7]의 경우에는 이것이 가능하지 않다.

효율성 측면에서도 기존 Zhang 등[7]이 사용하는 전자서명 기법보다 확인 비용이 저렴하다. Zhang 등[7]은 서명확인을 위해 3개의 겹선형 사상이 필요한 반면에 이 논문에 제안된 서명은 2개의 겹선형 사상만 필요하다. 길이 측면에서 결과 서명은 오히려 Zhang 등이 하나의 타원곡선 점으로 표현되므로 짧다고 할 수 있지만 함께 전달해야 하는 공개키를 고려할 때 Zhang 등과 이 논문에서 사용하는 전자서명은 모두 동일하게 3개의 타원곡선 점이 필요하다. Zhang 등과 이 논문에서 제안된 시스템과의 차이점은 [표 2]에 요약되어 있다.

V. 결 론

이 논문에서는 기존 Zhang 등[7]이 제안한 시스템을 개선한 새 시스템을 제안하고 있다. 이 제안은 1장에서 설명하고 있는 것처럼 4가지 측면에서 Zhang 등의 논문을 개선하였다. 뿐만 아니라 기존에 일괄 확인이 어렵다고 주장된 전자서명을 안전하게 일괄 확인할 수 있음을 보였고, Zhang 등과 달리 한번만 사용

[표 2] Zhang 등의 시스템과의 비교

		Zhang 등의 시스템	제안된 시스템
서명방식	특징	결정적이며 일회용 • 생성된 키 쌍으로 하나의 메시지만 서명 가능	확률적 • 생성된 키쌍으로 여러 메시지 서명 가능
	공개키	두 쌍 사용	한 쌍 사용
	서명비용	3개의 겹선형 사상 연산	2개의 겹선형 사상 연산
	서명크기(공개키 포함)	3개의 타원곡선 점	3개의 타원곡선 점
일괄확인 기법		안전성이 증명되어 있지 않은 기법 사용	안전성이 증명된 기법 사용
조건부 익명성		임계방식 사용이 어려움	권한 남용을 방지하기 위한 임계방식을 고려함
키 철회 문제		일회용이므로 고려할 필요 없음	짧은 유효기간으로 해결함

할 수 있는 것이 아니라 여러 번 사용하여도 안전성에 문제가 없는 전자서명 기법을 사용하고 있다. VANET에서는 [7-8]에서 제시된 것과 같이 많은 전자서명 메시지를 효과적으로 검증할 방법이 필요하다. 이를 위해 이 논문도 [7]처럼 일괄확인 기법을 사용하고 있지만 일괄확인 기법의 경우 일괄확인이 실패할 경우 어느 서명 때문에 실패하였는지 확인하는 것이 어렵다. 따라서 향후에 일괄확인이 실패하였을 경우에 어떤 서명 때문에 실패하였는지 빠르게 찾을 수 있는 방법에 대한 연구가 필요하다.

참 고 문 헌

[1] M. Raya and J. Hubaux, "Securing Vehicular Ad hoc Networks," J. of Computer Security, vol. 15, no. 1, pp. 39-68, Jan. 2007.

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

[3] G. Calandriello, P. Papadimitratos, J. Hubaux, and A. Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," Proc. of the 4th ACM Int. Workshop on Vehicular Ad Hoc Networks, pp. 19-28, Sep. 2007.

[4] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks," Proc. of the 8th Int. Symp. on Autonomous Decentralized Systems, pp. 344-351, Mar. 2007.

[5] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," Proc. of the IEEE INFOCOM 2008, pp. 1229-1237, Apr. 2008.

[6] X. Lin, C. Zhang, X. Sun, P. Ho, and X. Shen, "TSVC: Efficient and Secure Vehicular Communications with Privacy Preserving," IEEE Trans. on Wireless Communications, vol. 7, no. 12, pp. 4987-4998, Dec. 2008.

[7] C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks," Proc. of the IEEE INFOCOM 2008, pp. 246-350, Apr. 2008.

[8] C. Zhang, X. Lin, R. Lu, P. Ho, and X. Shen, "An Efficient Message Authentication Scheme for Vehicular Communications," IEEE Trans. on Vehicular Technology, vol. 57, no. 6, pp. 3357-3368, Nov. 2008.

[9] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from Weil Pairing," J. of Cryptology, vol. 17, no. 4, pp. 297-319, Apr. 2004.

[10] M. Bellare, J.A. Garay, and T. Rabin, "Fast Batch Verification for Modular Exponentiation and Digital Signatures," Advances in Cryptology, Eurocrypt 1998, LNCS 1403, pp. 236-250, 1998.

[11] J. Cha and J. Cheon, "An Identity-based Signature from Gap Diffie-Hellman Groups," Proc. of the Public Key Cryptography 2003, LNCS 2567, pp. 18-30, 2003.

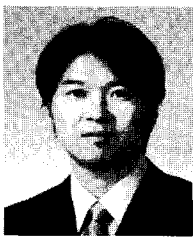
[12] H. Yoon, J. Cheon, and Y. Kim, "Batch Verifications with ID-based Signatures," Proc. of International Conference on Information Security and Cryptology 2004, LNCS 3506, pp. 233-248, 2005.

[13] F. Hess, "Efficient Identity based Signature Schemes based on Pairings," Proc. of the International Workshop on Selected Areas in Cryptography 2002, LNCS 2595, pp. 310-324, 2002.

[14] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," Advances in Cryptology, Crypto 2004, LNCS 3027, pp. 41-55, 2004.

〈著者紹介〉

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 인터넷미디어공학부 부교수
〈관심분야〉 암호기술 응용



임 지 환 (Jihwan Lim) 학생회원
2005년 2월: 한양대학교 전자컴퓨터공학부(학사)
2007년 2월: 한양대학교 컴퓨터공학과(석사)
2007년 3월 ~ 현재: 한양대학교 컴퓨터공학과 (박사과정)
〈관심분야〉 네트워크 보안

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