Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.3, Jun. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.3.563

VANET 환경을 위한 계층적 구조의 익명 인증 기술*

배 경 진,† 이 영 경, 김 종 현, 이 동 훈‡
고려대학교 정보보호대학원

An Anonymous Authentication in the Hierarchy for VANET*

Kyungjin Bae,† Youngkyung Lee, Jonghyun Kim, Dong Hoon Lee‡
Graduate School of Information Security, Korea University

요 약

VANET(Vehicular Ad hoc Network)에서 안전한 통신을 지원하기 위해 차량 간 또는 차량과 기반 구조 사이에서 교환되는 메시지는 인증이 반드시 수행되어야 한다. 본 논문에서는 VANET 환경을 위한 계층적 구조의 익명 인증 시스템을 제안한다. 제안하는 시스템 모델은 계층적으로 비밀키를 발급하여 기존 시스템의 문제점인 PKG의 오버헤드를 줄여 실용성을 높인다. 또한 페어링을 사용하지 않고 설계된 효율적인 2레벨 계층적 ID 기반 서명(Two-Level Hierarchical Identity-Based Signature, TLHIBS) 기법을 제안한다. 제안하는 기법은 조건부 익명성을 만족하여 차량의 프라이버시를 보호하고, 일괄검증(batch verification)을 지원하여 다수의 서명을 효율적으로 검증할 수 있다. 마지막으로 기존의 VAENT 환경에서 ID 기반 서명 기법들의 안전성 증명이 잘못된 것과는 다르게 제안한 기법의 안전성은 이산 대수 문제(Discrete Logarithm Problem, DLP)에 리덕션되어 랜덤 오라클 모델(random oracle model)에서 증명된다.

ABSTRACT

In order to support secure communication in VANET(Vehicular Ad hoc Network), messages exchanged between vehicles or between vehicle and infrastructure must be authenticated. In this paper, we propose a hierarchical anonymous authentication system for VANET. The proposed system model reduces the overhead of PKG, which is a problem of previous system, by generating private keys hierarchically, thereby enhancing practicality. We also propose a two-level hierarchical identity-based signature(TLHIBS) scheme without pairings so that improve efficiency. The proposed scheme protects the privacy of the vehicle by satisfying conditional privacy and supports batch verification so that efficiently verifies multiple signatures. Finally, The security of the proposed scheme is proved in the random oracle model by reducing the discrete logarithm problem(DLP) whereas the security proof of the previous ID-based signatures for VANET was incomplete.
Keywords: VANET, authentication, conditional privacy, IBS, pairing-free

I. 서 론

1.1 개요

VANET(Vehicular Ad hoc Network)은 무선 통신 기능을 가진 차량들로 구성된 에드혹 네트워크로, 차량에 무선 통신 기기(On-Board Unit, OBU)를 장착하여 차량 간 통신(Vehicle to

Received(04. 20. 2018), Modified(05. 31. 2018), Accepted(06. 11. 2018)
* 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. 2016-6-00599, 함수서명 설계기법 및 응용기술 연구)
† 주저자, kjna0827@korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr(Corresponding author)

Vehicle, V2V) 또는 차량과 기반구조 간의 통신(Vehicle to Infrastructure, V2I)을 지원한다. 이러한 통신을 이용하여 VANET에서는 주행과 관련해 다양한 서비스를 제공할 수 있는 장점이 있다. 예를 들어 사고 발생시 다가오는 후속 차량에게 우회할 수 있도록 사고 정보를 제공하거나 차선 변경시 협력 운전을 통해 운전자의 안전을 도모하며 교통 흐름을 원활하게 할 수 있다. 그러나 위조나 변조된 메시지가 전송되는 경우 오히려 사고를 일으킬 수 있어 운전자와 보행자의 안전에 위협이 될 수 있다. 따라서 VANET에서 교환되는 메시지는 무결성을 보장받기 위해 반드시 인증이 수행되어야 한다. 이때 익명성을 지원하지 않는 일반 서명 기법을 적용하는 경우 전송된 메시지를 조합하여 차량의 이동 경로를 추적할 수 있어 차량의 프라이버시가 노출될 수 있다. 그러므로 차량의 프라이버시를 보호하도록 익명으로 인증을 수행해야 한다. 한편 사고가 발생한 경우에는 책임자를 식별할 수 있도록 차량의 추적이 가능해야 한다. 즉 일반 차량에 대해서는 프라이버시를 보호하면서 필요한 경우에는 추적이 될 수 있도록 조건부 익명성이 지원되어야 한다.

기존의 조건부 익명성을 제공하는 ID 기반 서명 기법[4, 6, 9, 10]에서는 차량의 프라이버시 보호를 위해 실제 ID로부터 Pseudo-ID를 생성하고 이에 대한 비밀키를 이용해 서명을 생성한다. 이때 서명된 메시지들이 동일한 차량으로부터 생성된 것인지 알 수 없도록 매번 다른 Pseudo-ID와 이에 대한 비밀키 쌍을 이용하고 있다. 한편 VANET 환경에서 차량은 100~300ms마다 자신의 상태 정보(위치, 속도, 방향 등) 메시지를 전송해야 한다. 따라서 매번 다른 Pseudo-ID와 이에 대한 비밀키를 이용하여 서명을 생성하기 위해서는 Pseudo-ID와 이에 대한 비밀키가 주기적으로 보충되어야 한다. 따라서 PKG(Private Key Generator)에 차량의 비밀키 발급이 빈번하게 요구된다.

그러나 VANET 환경에서 기존의 시스템 모델[4, 9]은 PKG가 시스템 내 모든 차량의 비밀키를 발급하기 때문에 차량의 빈번한 키 발급 요구로 인해 PKG에 큰 오버헤드가 발생할 수 있다. 이로 인해 기존의 시스템 모델은 시스템 내 차량의 수와 전송해야 할 메시지 양이 증가하는 경우 실용적인 모델이 될 수 없다. 따라서 본 논문에서는 PKG의 오버헤드를 줄이도록 계층적 구조의 익명 인증 시스템을 제안한다.

1.2 기여도

본 논문에서는 VANET 환경을 위한 계층적 구조의 익명 인증 시스템을 제안한다. 제안하는 인증 시스템은 시스템 모델과 제안한 시스템 모델에 적용될 서명 기법으로 구성된다. 본 논문의 기여도는 다음 3가지와 같다.

첫째, 제안하는 시스템 모델은 차량의 비밀키를 계층적으로 발급함으로써 기존의 모델에서 PKG에 발생하는 오버헤드를 줄인다. PKG가 각 제조사(manufacturer)의 비밀키를 발급하고 차량은 제조사로부터 비밀키를 발급받아 키 발급이 계층적으로 분산되어 이루어지므로 차량의 빈번한 키 발급 요구에도 PKG의 오버헤드를 낮출 수 있어 실용성을 높인다.

둘째, 겹선형 함수(bilinear map)를 사용하지 않고 설계된 효율적인 2레벨 계층적 ID 기반 서명(Two-Level Hierarchical Identity-Based Signature, TLHIBS) 기법을 제안한다. 기존의 겹선형 함수를 사용하여 설계된 TLHIBS 기법[1]은 연산량이 무거운 페어링 연산을 수행해야 하므로 비효율적이다. 또한 제안하는 기법은 일괄검증(batch verification)을 지원하여 다수의 서명을 효율적으로 검증할 수 있다.

셋째, 제안한 기법의 안전성을 이산 대수 문제(Discrete Logarithm Problem, DLP)에 리덕션하여 랜덤 오라클 모델(random oracle model)에서 증명한다. 기존의 VANET 환경에서 ID 기반 서명 기법들[1, 4, 9]의 안전성은 기반하는 어려운 문제에 특정한 한 경우에 한해서만 리덕션되어 안전성 증명이 잘못되었다. 본 논문에서는 제안한 기법의 안전성을 [11]에서의 리덕션 방식을 이용하여 general forking lemma 뿐 만 아니라 multiple forking lemma도 적용해 모든 경우에 대해 안전성을 증명한다.

1.3 관련연구

VANET에서 조건부 익명성을 제공하는 인증 시스템은 크게 공개키 기반 구조(Public Key Infrastructure, PKI), 그룹 서명, ID 기반 서명을 프리미티브로 이용하는 기법이 연구되어왔다. 그러나 PKI 구조를 이용한 기법[7]과 그룹 서명을 이용한 인증 기법[8]은 차량의 공개키에 대한

Table 1. Comparison of security

	Security model	Random oracle	Complexity assumption	Forking lemma	Completeness of security proof
He et al. [1]	Selective	O	CDH	General	X
Lo et al. [4]	Adaptive	O	DLP	General	X
KIBS(CPAS) [9]	Adaptive	O	CDH	General	X
Ours	Selective	O	DLP	General, Multiple	O

CDH : Computational Diffie-Hellman problem

CRL(Certificate Revocation List)을 관리하는 것이 어려웠고, 특히 [8]의 경우 서명의 길이가 일반 서명보다 길어 검증 비용이 비효율적이었다.

C. Zhang 등은 2008년에 처음으로 조건부 익명성을 만족하는 ID 기반 서명을 이용한 인증 기법을 제안하였다[6]. 제안된 기법은 인증서 검증 및 전송 비용을 제거해 CRL 문제를 해결하고 TPD(Tamper-Proof Device)를 이용하여 차량 자체에서 Pseudo-ID와 이에 대한 비밀키를 생성했다. 이후 TPD를 이용한 ID 기반 서명 기법이 활발하게 연구되었다[6, 10].

그러나 [6, 10]의 기법에서는 시스템 내 모든 차량의 TPD에 시스템 마스터 비밀키를 설치하여 TPD에 대한 안전성 의존도가 매우 높은 문제점이 있었다. TPD는 암호학적 키를 안전하게 저장하는 데 많이 이용되고 있으나 최근 연구[12, 13]에 따르면 부채널 공격과 전력 분석 등에 의해 TPD로부터 어느 정도 비밀 정보의 추출이 가능하게 되었기 때문이다. 이후 TPD에 대한 안전성 의존도를 줄이고자 TPD에 마스터 비밀키가 아닌 Pseudo-ID에 대한 비밀키를 설치해 조건부 익명성을 만족하는 ID 기반 서명 기법이 제안되었다[4, 9].

반면 [4, 9]에서는 PKG가 시스템 내 모든 차량의 비밀키를 발급하기 때문에 차량의 빈번한 키 발급 요구로 인해 PKG에 오버헤드가 발생할 수 있다. 따라서 Y. Wang 등은 2016년에 PKG의 오버헤드를 줄이고자 PKG를 여러 개로 확장하는 ID 기반 서명 기법을 제안하였다[15]. 그러나 제안된 기법은 PKG가 Pseudo-ID 생성 및 비밀키 발급을 모두 수행하여 PKG로부터 차량의 프라이버시가 보호되지 않는 문제점이 있다. 또한 제안된 기법은 페어링을 사용하여 설계되어 비효율적이다.

VANET 환경을 위한 인증 기법에서 계층적 구조의 시스템 모델은 제안되지 않았다. 그러나 2017년 D.He 등이 항공 시스템 관제를 위한 계층적 구조의 시스템 모델을 도입하고 시스템 모델에 적합한 TLHIBS 기법을 제안하여 적용하였다[1]. 그러나 [1]의 시스템 모델에서는 항공기의 프라이버시를 보호하지 않으며 제안된 기법은 페어링을 사용하여 설계되어 비효율적이다.

한편 기존의 VANET 환경에서 ID 기반 서명 기법[1, 4, 9]에서는 [Table 1]과 같이 기법의 안전성을 general forking lemma를 적용하는 특정한 한 경우에 한해서만 증명하였다. 서명 기법에서는 랜덤 오라클 개수가 2개 이상인 경우 general forking lemma뿐 만 아니라 multiple forking lemma를 적용하여 안전성을 증명해야 모든 경우에 대해 기반하는 문제에 리덕션이 이루어진다. 그러나 기존의 연구[1,4,9]에서는 랜덤 오라클이 2개 이상임에도 불구하고 general forking lemma만을 적용하여 안전성을 증명하였다. 즉, 기법의 안전성이 기반하는 어려운 문제에 특정한 한 경우에 한해서만 리덕션되었기 때문에 안전성이 증명되었다고 볼 수 없다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 제안하는 TLHIBS 기법의 이해와 안전성 증명에 필요한 배경지식을 설명한다. Ⅲ장에서는 TLHIBS 기법을 제안하고, 제안한 기법에 대한 안전성을 증명한다. Ⅳ장에서는 제안하는 인증 시스템을 설명한다. Ⅴ장에서는 안전성을 분석하고 기존 기법과 비교·분석한다. 마지막으로 Ⅵ장에서 결론을 맺는다.

Ⅱ. 배경지식

본 장에서는 기법 설계에 필요한 배경지식과 기법을 구성하는 알고리즘 및 안전성 모델을 설명한다.

2.1 DLP 문제 및 가정

정의 1. 〔DLP 문제 및 가정〕

- 문제: 위수가 q인 덧셈군 $\mathbb{G}$와 위수가 q인 $P \in \mathbb{G}$ 와 αP가 주어져 있을 때 $\alpha \in \mathbb{Z}_q$를 구하는 문제이다.
- 가정: 다항식 시간 안에 DLP 문제를 계산해내는 알고리즘 A가 존재할 때, A의 문제를 풀어내는 이점이 무시할 만큼 작은(negligible) 값이라면, DLP 문제는 풀기 어렵다고 정의한다. 이때 A의 이점을 다음과 같이 정의한다.

$$Adv_A^{ECDLP} = |\Pr[A(Z) = x]|$$

2.2 TLHIBS 기법의 정의

TLHIBS 기법은 $Setup$, $Extract^1$, $Extract^2$, $Sign$, $Verify$, $BVerify$ 여섯 개의 다항 시간(polynomial-time) 알고리즘으로 구성된다〔1〕.

- $Setup(k) \rightarrow (msk, pp)$: 설정 알고리즘은 보안 상수 k를 입력으로 받아서 마스터 비밀키 msk(master secret-key)와 공개 파라미터 pp(public parameter)를 출력한다.
- $Extract^1(ID_{|1}, msk, pp) \rightarrow sk_{ID_{|1}}$: 1레벨 키 발급 알고리즘은 1레벨 ID $ID_{|1} = (I_1)$과 마스터 비밀키 msk, 공개 파라미터 pp를 입력으로 받아서 1레벨 ID $ID_{|1}$의 비밀키 $sk_{ID_{|1}}$을 출력한다.
- $Extract^2(ID_{|2}, sk_{ID_{|1}}, pp) \rightarrow sk_{ID_{|2}}$: 2레벨 키 발급 알고리즘은 2레벨 ID $ID_{|2} = (I_1, I_2)$와 $ID_{|1} = (I_1)$의 비밀키 $sk_{ID_{|1}}$, 공개 파라미터 pp를 입력으로 받아서 2레벨 ID $ID_{|2}$의 비밀키 $sk_{ID_{|2}}$을 출력한다.
- $Sign(m, ID_{|2}, sk_{ID_{|2}}, pp) \rightarrow \sigma$: 서명 생성 알고리즘은 메시지 m과 2레벨 ID $ID_{|2}$, 2레벨 ID $ID_{|2}$의 비밀키 $sk_{ID_{|2}}$, 공개 파라미터 pp를 입력으로 받아서 서명 σ를 출력한다.
- $Verify(\sigma, m, ID_{|2}, pp) \rightarrow$ T/F: 검증 알고리즘은 서명 σ, 메시지 m, 2레벨 ID $ID_{|2}$, 공개 파라미터 pp를 입력으로 받아서 T(True) 또는 F(False)를 출력한다.
- $BVerify(\{\sigma_i\}_{i=1}^n, \{m_i\}_{i=1}^n, \{ID_{|2,i}\}_{i=1}^n, pp) \rightarrow$ T/F: 일괄검증 알고리즘은 n개의 서명 $\{\sigma_1, ..., \sigma_n\}$과 n개의 메시지 $\{m_1, ..., m_n\}$, n개의 ID $\{ID_{|2,1}, ..., ID_{|2,n}\}$, 공개 파라미터 pp를 입력으로 받아서 T 또는 F를 출력한다.

2.3 TLHIBS 기법의 안전성 모델

정의 2. 〔선택적 ID에 대해 선택 메시지 공격에 대한 존재적 위조 불가능성〕

TLHIBS 기법의 안전성 모델은 〔1〕에서 정의한 안전성 모델을 적용한다. 공격자 A는 챌린저 C와 다음과 같이 가상의 게임(game)을 수행한다.

- Setup: A는 챌린지 ID $ID_{|2}^* = (I_1^*, I_2^*)$를 선택하고 C에게 전송한다. C는 $Setup$ 알고리즘을 실행하여 마스터 비밀키 msk와 공개 파라미터 pp를 생성하고 A에게 공개 파라미터 pp를 전송한다.
- Query: A는 C에게 다음의 질의를 능동적으로 한다.

1. $Extract^1$: A가 C에게 $ID_{|1} = (I_1)$를 질의하면, C는 $Extract^1$ 알고리즘을 실행하여 $ID_{|1}$의 비밀키 $sk_{ID_{|1}}$을 생성하고 리스트 L_1에 $(ID_{|1}, sk_{ID_{|1}})$을 저장한다. C는 A에게 $ID_{|1}$의 비밀키 $sk_{ID_{|1}}$을 전송한다.
2. $Extract^2$: A가 C에게 $ID_{|2} = (I_1, I_2)$를 질의하면, C는 $Extract^2$ 알고리즘을 실행하여 $ID_{|2}$의 비밀키 $sk_{ID_{|2}}$를 생성하고 리스트 L_2에 $(ID_{|2}, sk_{ID_{|2}})$를 저장한다. C는 A에게 $ID_{|2}$의 비밀키 $sk_{ID_{|2}}$을 전송한다.
3. $Sign$: A가 C에게 $ID_{|2}$와 메시지 m을 질의하면, C는 $ID_{|2}$와 메시지 m에 대한 서명 σ을 생성하여 A에게 전송한다.

- Output: A는 $ID_{|2}^*$에 대해 메시지 m^*에 대한 서명 σ^*을 생성하여 C에게 전송한다.

다음의 조건을 만족하는 경우 A가 게임을 이긴 것으로 간주한다.

① σ^*는 $(ID_{|2}^*, m^*)$에 대해 $Verify$ 알고리즘을 통과해야 한다.

② $ID_{|1}^*$는 $Extract^1$에서 질의된 적이 없어야 한다.

③. $ID_{|2}^{*}$는 $Extract^{2}$에서 질의된 적이 없어야 한다.

④. $(ID_{|2}^{*}, m^{*})$은 $Sign$에 질의된 적이 없어야 한다.

게임에서 공격자 A가 얻는 이점(advantage)은 다음과 같이 정의된다.

$$Adv_{TLHIBS,A}^{EUF-CMA}(k) = |\Pr[Awins]|$$

정의 3. TLHIBS 기법에 대한 임의의 다항식 시간 공격자 A에 대해 공격자의 이점 $Adv_{TLHIBS,A}^{EUF-CMA}(k)$이 무시할 만큼 작은(negligible) 값이라면, TLHIBS 기법은 선택적 ID에 대해 선택 메시지 공격에 대하여 존재적 위조가 불가능(existential unforgeable against selective identity under chosen-message attack)하다.

III. 제안하는 TLHIBS 기법

본 장에서는 TLHIBS 기법을 제안하고 제안한 TLHIBS 기법의 안전성을 증명한다.

3.1 제안하는 TLHIBS 기법

- $Setup(k) \rightarrow (msk, pp)$: PKG는 시스템을 설정하기 위해 다음 과정을 수행한다.

1. 위수가 소수 q인 군 $\mathbb{G}$를 생성하고 $\mathbb{G}$의 생성원 $P \in \mathbb{G}$를 선택한다.
2. 임의의 $s \in Z_q^{*}$를 선택하고 $P_{pub} = sP$를 계산한다.
3. 세 개의 일방향 해시 함수 $h_i : \{0,1\}^{*} \rightarrow Z_q^{*} (i = 1,2,3)$를 선택하고, 공개 파라미터 $pp = \{q, P, P_{pub}, h_1, h_2, h_3\}$를 설정하여 공개한다. 여기서 $msk = s$로 설정된다.

- $Extract^{1}(ID_{|1}, msk, pp) \rightarrow sk_{ID_1}$: PKG는 1레벨 ID $ID_{|1} = (I_1)$에 대한 비밀키 sk_{ID_1}를 발급한다. PKG의 비밀키 sk_{ID_1} 발급 과정은 다음과 같다.

1. PKG는 임의의 $r_{ID_1} \in Z_q^{*}$을 선택하여 다음과 같이 계산한다.
   $R_{ID_1} = r_{ID_1} P,\ c_{ID_1} = h_1(ID_{|1}, R_{ID_1})$
   $S_{ID_1} = r_{ID_1} + c_{ID_1} \cdot s$을 계산한다.
2. PKG는 $sk_{ID_1} = \{R_{ID_1}, S_{ID_1}\}$을 안전한 채널을 통해 전송한다.

- $Extract^{2}(ID_{|2}, sk_{ID_1}, pp) \rightarrow sk_{ID_2}$: 1레벨 개체 $ID_{|1}$는 2레벨 개체 $ID_{|2}$에게 $ID_{|2}$에 대한 비밀키 sk_{ID_2}를 발급한다. 비밀키 sk_{ID_2} 발급 과정은 다음과 같다.

1. 임의의 $r_{ID_2} \in Z_q^{*}$를 선택하여 다음과 같이 계산한다.
   $R_{ID_2} = r_{ID_2} P,\ c_{ID_2} = h_2(ID_{|2}, R_{ID_2}, R_{ID_1})$
   $S_{ID_2} = S_{ID_1} + c_{ID_2} \cdot r_{ID_2}$
2. $sk_{ID_2} = \{R_{ID_1}, R_{ID_2}, S_{ID_2}\}$을 안전한 채널을 통해 전송한다.

- $Sign(m, ID_{|2}, sk_{ID_2}, pp) \rightarrow \sigma$: 비밀키 sk_{ID_2}을 이용하여 메시지 m에 대한 서명 σ를 생성한다. 구체적인 과정은 다음과 같다.

1. 임의의 $r_m \in Z_q^{*}$를 선택하여 다음과 같이 계산한다.
   $R_m = r_m P,\ c_m = h_3(m, ID_{|2}, R_{ID_2}, R_{ID_1}, R_m)$
   $S_m = S_{ID_2} + c_m \cdot r_m$
2. $ID_{|2}$의 메시지 m에 대한 서명 $\sigma = \{R_{ID_1}, R_{ID_2}, R_m, S_m\}$을 출력한다.

- $Verify(\sigma, m, ID_{|2}, pp) \rightarrow$ T/F: 검증자는 $ID_{|2} = (I_1, I_2)$의 메시지 m에 대한 서명 $\sigma = \{R_{ID_1}, R_{ID_2}, R_m, S_m\}$을 공개된 파라미터 pp를 이용하여 검증을 수행한다. 구체적인 과정은 다음과 같다.

1. 검증자는 다음식을 계산한다.

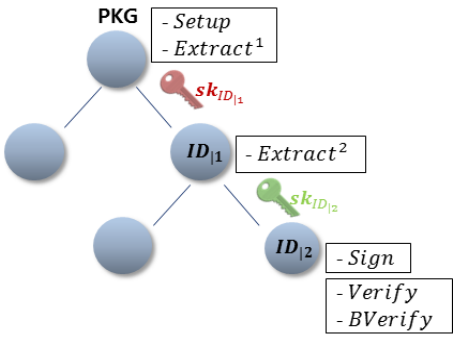

Fig. 1. The proposed TLHIBS scheme

$c_{ID_{|1}} = h_1(ID_{|1}, R_{ID_{|1}})$, $c_{ID_{|2}} = h_2(ID_{|2}, R_{ID_{|2}}, R_{ID_{|1}})$,
$c_m = h_3(m, ID_{|2}, R_{ID_{|2}}, R_{ID_{|1}}, R_m)$

2. 검증자는 다음 등식이 성립하는지 확인한다.
$S_m P = R_{ID_{|1}} + c_{ID_{|1}} P_{pub} + c_{ID_{|2}} R_{ID_{|2}} + c_m R_m$
성립하면 T를 출력하고, 그렇지 않으면 F를 출력한다. 성립하는 경우 서명 σ의 정당성이 검증된다.

- $BVerify(\{\sigma_i\}_{i=1}^n, \{m_i\}_{i=1}^n, \{ID_{|2,i}\}_{i=1}^n, pp) \rightarrow$ T/F: 검증자는 n개의 ID $\{ID_{|2,1}, ..., ID_{|2,n}\}$의 각 메시지 $\{m_1, ..., m_n\}$에 대한 각각의 서명 $\{\sigma_1, ..., \sigma_n\}$을 공개 파라미터 pp를 이용하여 일괄적으로 검증을 수행한다. 구체적인 과정은 다음과 같다.

1. 검증자는 $i = 1, ..., n$에 대해 다음식을 계산한다.
$c_{ID_{|1,i}} = h_1(ID_{|1,i}, R_{ID_{|1,i}})$,
$c_{ID_{2,i}} = h_2(ID_{|2,i}, R_{ID_{2,i}}, R_{ID_{|1,i}})$,
$c_{m_i} = h_3(m_i, ID_{|2,i}, R_{ID_{2,i}}, R_{ID_{|1,i}}, R_{m_i})$
2. 검증자는 다음 등식이 성립하는지 확인한다.
$$(\sum_{i=1}^n S_{m_i})P = \sum_{i=1}^n R_{ID_{|1,i}} + (\sum_{i=1}^n c_{ID_{|1,i}})P_{pub} + (\sum_{i=1}^n c_{ID_{2,i}} R_{ID_{2,i}}) + (\sum_{i=1}^n c_{m_i} R_{m_i})$$
성립하는 경우 n개의 서명 $\{\sigma_1, ..., \sigma_n\}$의 정당성이 일괄적으로 검증된다.
3. 여기서 일괄검증의 안전성을 보장하기 위해 작은 지수 활용 검사(small exponents test) 기법을 ID 기반 서명 기법에 적용할 수 있다[2, 4, 5]. 이 방법을 통해 2014년 Liu 등[3]이 제안한 일괄검증 공격으로부터 안전성을 보장받을 수 있다.
   ①. 검증자는 작은 지수 활용 검사를 수행하기 위해 임의의 벡터 $\delta = \{\delta_1, ..., \delta_n\}$을 선택한다. 여기서 $i = 1, ..., n$에 대해 $\delta_i \in \{0,1\}^l$이다. 일반적으로 VANET에서 $l = 80$으로 충분하다.
   ②. 검증자는 다음 등식이 성립하는지 확인한다.
$$(\sum_{i=1}^n \delta_i S_{m_i})P = (\sum_{i=1}^n \delta_i R_{ID_{|1,i}}) + (\sum_{i=1}^n \delta_i c_{ID_{|1,i}})P_{pub} + (\sum_{i=1}^n \delta_i c_{ID_{2,i}} R_{ID_{2,i}}) + (\sum_{i=1}^n \delta_i c_{m_i} R_{m_i})$$
성립하면 T를 출력하고, 그렇지 않으면 F를 출력한다. 성립하는 경우 n개의 서명 $\{\sigma_1, ..., \sigma_n\}$의 정당성이 일괄적으로 검증된다.

3.2 제안한 TLHIBS 기법의 안전성 증명

정리 1. 3.1 절에서 제안한 TLHIBS 기법은 DLP 문제가 어렵다는 가정하에 선택적 ID에 대해 선택 메시지 공격에 대한 존재적 위조가 불가능하다.

증명. TLHIBS 기법에 대한 다항식 시간 공격자 A의 이점을 이용하여 DLP 문제를 풀도록 챌린저 C를 설계할 수 있다.

DLP 문제의 인스턴스로 (P, sP)가 주어지면, C는 s를 구해서 문제를 풀 수 있다. C는 $P_{pub} \leftarrow sP$로 설정한다. A는 챌린지 ID로 2레벨 ID $ID_{|2}^* = (I_1^*, I_2^*)$를 선택하여 C에게 전송하고, C는 공개 파라미터 $pp = \{q, P, P_{pub}, h_1, h_2, h_3\}$를 A에게 전송한다. C는 A의 질의에 대해 다음과 같이 응답한다.

- $h_1(ID_{|1}, R_{ID_{|1}})$: C는 공란으로 초기화되어있는 리스트 L_{h_1}을 다음과 같이 관리한다. C는 쌍 $(ID_{|1}, R_{ID_{|1}}, c_{ID_{|1}})$이 L_{h_1}에 있는지 확인한다. 만약 쌍 $(ID_{|1}, R_{ID_{|1}}, c_{ID_{|1}})$이 L_{h_1}에 있으면 A에게 $c_{ID_{|1}}$을 전송하고, 그렇지 않은 경우 임의로 $c_{ID_{|1}}$을 선택해 쌍 $(ID_{|1}, R_{ID_{|1}}, c_{ID_{|1}})$을 L_{h_1}에 추가하고 $c_{ID_{|1}}$은 A에게 전송한다.
- $h_2(ID_{|2}, R_{ID_{|2}}, R_{ID_{|1}})$: C는 공란으로 초기화되어있는 리스트 L_{h_2}을 다음과 같이 관리한다. C는 쌍 $(ID_{|2}, R_{ID_{|2}}, R_{ID_{|1}}, c_{ID_{|2}})$이 L_{h_2}에 있는지 확인한다.

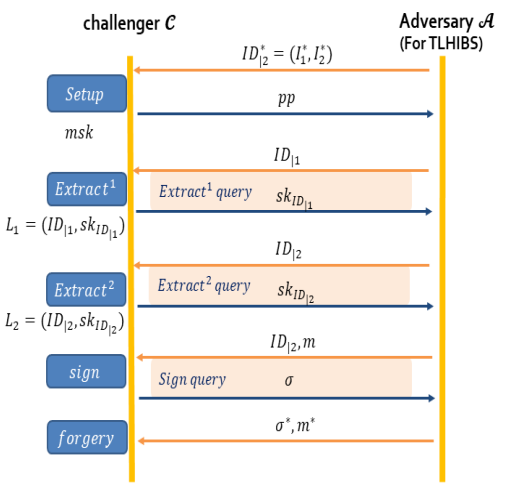

Fig. 2. The security model of TLHIBS scheme

만약 쌍 $(ID_{|2}, R_{ID_2}, R_{ID_1}, c_{ID_2})$이 L_{h_2}에 있으면 A에게 c_{ID_2}을 전송하고, 그렇지 않은 경우 임의로 c_{ID_2}을 선택해 쌍 $(ID_{|2}, R_{ID_2}, R_{ID_1}, c_{ID_2})$을 L_{h_2}에 추가하고 c_{ID_2}은 A에게 전송한다.

- $h_3(m, ID_{|2}, R_{ID_2}, R_{ID_1}, R_m)$: C는 공란으로 초기화되어있는 리스트 L_{h_3}을 다음과 같이 관리한다. C는 쌍 $(m, ID_{|2}, R_{ID_2}, R_{ID_1}, R_m, c_m)$이 L_{h_3}에 있는지 확인한다. 만약 쌍 $(m, ID_{|2}, R_{ID_2}, R_{ID_1}, R_m, c_m)$이 L_{h_3}에 있으면 A에게 c_m을 전송하고, 그렇지 않은 경우 임의로 c_m을 선택해 쌍 $(m, ID_{|2}, R_{ID_2}, R_{ID_1}, R_m, c_m)$을 L_{h_3}에 추가하고 c_m은 A에게 전송한다.
- $Extract^1(ID_{|1})$: C는 공란으로 초기화되어있는 리스트 L_1을 다음과 같이 관리한다. C는 쌍 $(ID_{|1}, R_{ID_1}, S_{ID_1})$이 L_1에 있는지 확인한다. 만약 쌍 $(ID_{|1}, R_{ID_1}, S_{ID_1})$이 있으면 A에게 $sk_{ID_1} = \{R_{ID_1}, S_{ID_1}\}$을 전송하고, 그렇지 않은 경우 다음 과정을 수행한다.

1. $ID_{|1} = ID_1^*$ 인 경우 C는 임의의 $r_{ID_1}, c_{ID_1} \in Z_q^*$을 선택해 $R_{ID_1} = r_{ID_1}P$를 계산하고 $S_{ID_1} \leftarrow \perp$로 설정하여 (R_{ID_1}, S_{ID_1})를 A에게 전송한다. C는 $(ID_{|1}, R_{ID_1}, S_{ID_1})$를 L_1에, $(ID_{|1}, R_{ID_1}, c_{ID_1})$를 L_{h_1}에 각각 저장한다.
2. $ID_{|1} \neq ID_1^*$인 경우 C는 임의의 $r_{ID_1}, c_{ID_1} \in Z_q^*$를 선택해 $R_{ID_1} = r_{ID_1}P - c_{ID_1}P_{pub}$를 계산하고 $S_{ID_1} = r_{ID_1}$로 설정하여 (R_{ID_1}, S_{ID_1})를 A에게 전송한다. C는 쌍 $(ID_{|1}, R_{ID_1}, S_{ID_1})$를 L_1에, 쌍 $(ID_{|1}, R_{ID_1}, c_{ID_1})$를 L_{h_1}에 각각 저장한다.

- $Extract^2(ID_{|2})$: C는 공란으로 초기화되어있는 리스트 L_2을 다음과 같이 관리한다. C는 쌍 $(ID_{|2}, R_{ID_2}, S_{ID_2})$이 L_2에 있는지 확인한다. 만약 쌍 $(ID_{|2}, R_{ID_2}, S_{ID_2})$이 있으면 A에게 $sk_{ID_2} = \{R_{ID_1}, R_{ID_2}, S_{ID_2}\}$을 전송하고, 그렇지 않은 경우 다음 과정을 수행한다.

1. $ID_{|1} \neq ID_1^*$ 인 경우 C는 L_1에서 쌍 $(ID_{|1}, R_{ID_1}, S_{ID_1})$를 확인한다. C는 임의의 $r_{ID_2}, c_{ID_2} \in Z_q^*$를 선택해 $R_{ID_2} = r_{ID_2}P$, $S_{ID_2} = S_{ID_1} + c_{ID_2} \cdot r_{ID_2}$를 계산하고, A에게 $sk_{ID_2} = \{R_{ID_1}, R_{ID_2}, S_{ID_2}\}$을 전송한다. 쌍 $(ID_{|2}, R_{ID_2}, S_{ID_2})$를 L_2에, 쌍 $(ID_{|2}, R_{ID_2}, R_{ID_1}, c_{ID_2})$를 L_{h_2}에 각각 저장한다.
2. $ID_{|1} = ID_1^*$인 경우 C는 L_1에서 쌍 $(ID_{|1}, R_{ID_1}, S_{ID_1})$를, L_{h_1}에서 쌍 $(ID_{|1}, R_{ID_1}, c_{ID_1})$을 확인한다. 만약 L_1, L_{h_1}에 없는 경우 $Extract^1(ID_{|1})$의 1번 과정과 동일하게 생성하여 L_1, L_{h_1}에 추가한다.
   ①. $I_2 = I_2^*$인 경우 C는 임의의 $r_{ID_2}, c_{ID_2} \in Z_q^*$을 선택해 $R_{ID_2} = r_{ID_2}P$를 계산하고 $S_{ID_2} \leftarrow \perp$로 설정하여 $sk_{ID_2} = \{R_{ID_1}, R_{ID_2}, S_{ID_2}\}$를 A에게 전송한다. C는 쌍 $(ID_{|2}, R_{ID_2}, S_{ID_2})$를 L_2에, 쌍 $(ID_{|2}, R_{ID_2}, R_{ID_1}, c_{ID_2})$를 L_{h_2}에 각각 저장한다.
   ②. $I_2 \neq I_2^*$인 경우 C는 임의의 $r_{ID_2}, c_{ID_2} \in Z_q^*$를 선택해 $R_{ID_2} = c_{ID_2}^{-1}(r_{ID_2}P - R_{ID_1} - c_{ID_1}P_{pub})$를 계산하고 $S_{ID_2} = r_{ID_2}$로 설정하여 $sk_{ID_2} = \{R_{ID_1}, R_{ID_2}, S_{ID_2}\}$를 A에게 전송한다. C는 쌍 $(ID_{|2}, R_{ID_2}, S_{ID_2})$를 L_2에, 쌍 $(ID_{|2}, R_{ID_2}, R_{ID_1}, c_{ID_2})$를 L_{h_2}에 각각 저장한다.

- $Sign(m, ID_{|2})$: C는 먼저 $ID_{|2} = ID_{|2}^*$인지 확인하고 L_2에서 쌍 $(ID_{|2}, R_{ID_2}, S_{ID_2})$을, L_{h_2}에서 쌍 $(ID_{|2}, R_{ID_2}, R_{ID_1}, c_{ID_2})$을 확인한다. 만약 L_2, L_{h_2}에 없는 경우 $Extract^2(ID_{|2})$의 2번 과정과 동일하게 생성하여 L_2, L_{h_2}에 추가한다.

1. $ID_{|2} = ID_{|2}^*$인 경우 C는 L_1, L_2에서 쌍 $(ID_{|1}, R_{ID_1}, S_{ID_1})$, $(ID_{|2}, R_{ID_2}, S_{ID_2})$를 확인한다. C는 임의의 $r_m, c_m \in Z_q^*$를 선택해 $R_m = c_m^{-1}(r_mP - R_{ID_1} - c_{ID_1}P_{pub} - c_{ID_2}R_{ID_2})$를 계산하고 $S_m = r_m$로 설정하여 $\sigma = \{R_{ID_1}, R_{ID_2}, R_m, S_m\}$를 A에게 전송한다. C는

쌍 $(m, ID_{|2}, R_{ID_2}, R_{ID_1}, R_m, c_m)$를 L_{h_3}에 저장한다.

2. $ID_{|2} \neq ID_{|2}^*$인 경우 C는 임의의 $r_m, c_m \in Z_q^*$을 선택해 $R_m = r_m P, c_m = h_3(m, ID_{|2}, R_{ID_2}, R_{ID_1}, R_m)$, $S_m = S_{ID_2} + c_m \cdot r_m$을 계산하여 $\sigma = \{R_{ID_1}, R_{ID_2}, R_m, S_m\}$를 A에게 전송한다. C는 쌍 $(m, ID_{|2}, R_{ID_2}, R_{ID_1}, R_m, c_m)$를 L_{h_3}에 저장한다.

• Output: A는 $(ID_{|2}^*, m^*)$에 대한 서명 σ^*을 생성하여 C에게 전송한다.

A는 리덕션 기법인 oracle replay attack을 통해 $(ID_{|2}^*, m^*)$에 대한 $\sigma^{*\prime}(\neq \sigma^*)$를 생성하여 C에게 전송할 수 있다. C는 [11]에서 정의된 하나의 랜덤 오라클에 대한 general forking lemma와 2개 이상의 랜덤 오라클에 대한 multiple forking lemma를 이용하여 σ^*와 $\sigma^{*\prime}$로부터 s를 구할 수 있다. 이때 A가 C로부터 $(ID_{|2}^*, m)$에 대해 $Sign$ 질의를 어떻게 받았는지에 따라 s를 다르게 구하므로 각 경우를 모두 고려해서 s를 구해야 한다.

C가 받은 위조 서명 $\sigma^* = \{R_{ID_1}^*, R_{ID_2}^*, R_m^*, S_m^*\}$이 주어졌을 때 A가 $(ID_{|2}^*, m)$에 대해 C에게 $Sign$ 질의를 하여 ①$R_{ID_1}^*, R_{ID_2}^*$를 C로부터 받은 적이 있는 경우와 ②$R_{ID_1}^*$만 받은 적이 있는 경우, ③$R_{ID_2}^*$만 받은 적이 있는 경우, ④둘 다 받은 적이 없는 경우로 나누어진다.

①의 경우: C가 r_{ID_1}, r_{ID_2}를 모두 아는 경우이므로 r_{ID_1}, r_{ID_2}를 상쇄시키기 위해 multiple forking lemma를 적용할 필요가 없다. 따라서 oracle replay attack을 통해 r_m을 상쇄시키기 위해 general forking lemma를 적용한다.

1-1) $S_m = r_{ID_1} + sc_{ID_1} + r_{ID_2} c_{ID_1} + r_m c_m$

1-2) $S_m' = r_{ID_1}' + sc_{ID_1}' + r_{ID_2}' c_{ID_1}' + r_m' c_m'$

(여기서 $r_{ID_1} = r_{ID_1}', r_{ID_2} = r_{ID_2}'$이다.)

식 1-1), 1-2)에 의해 $S_m c_m' - S_m' c_m$로부터 s를 구할 수 있다.

$$s = (c_{ID_1} c_m' - c_{ID_1}' c_m)^{-1} \cdot [S_m c_m' - S_m' c_m - r_{ID_1}(c_m' - c_m) - r_{ID_2}(c_{ID_2} c_m' - c_{ID_2}' c_m)]$$

②의 경우: C가 r_{ID_1}만 아는 경우이므로 r_{ID_2}와 r_m을 상쇄시키기 위해 multiple forking lemma

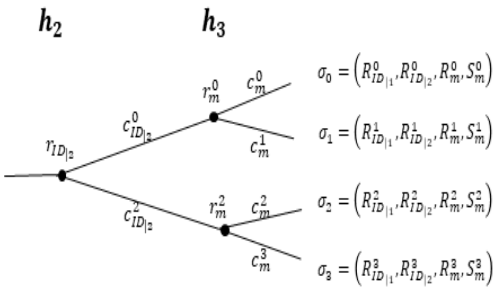

Fig. 3. Structure of the forgeries in the case h_2 query is followed by h_3 query.

를 적용해야 한다. 이때 h_2 질의와 h_3 질의 순서에 따라 multiple forking lemma가 적용된 위조 서명 구조가 달라진다. 먼저 h_2 질의 후 h_3 질의가 일어나는 경우, [Fig. 3]과 같이 위조 서명의 구조를 나타낼 수 있다. r_{ID_2}에서 forking lemma에 의해 서로 다른 h_2 해시값인 $c_{ID_2}^0$, $c_{ID_2}^2$을 가질 수 있고, 그 후 h_3 오라클에서 다른 난수 r_m^0, r_m^2에 대해 각각 forking lemma를 적용하여 서로 다른 h_3 해시값 $c_m^0, c_m^1, c_m^2, c_m^3 (c_m^0 \neq c_m^1, c_m^2 \neq c_m^3)$을 얻을 수 있다.

다음 4개의 식 2-1), 2-2), 2-3), 2-4)로부터 다음과 같이 s를 구할 수 있다.

2-1) $S_m^0 = r_{ID_1} + sc_{ID_1}^0 + r_{ID_2} c_{ID_2}^0 + r_m^0 c_m^0$

2-2) $S_m^1 = r_{ID_1} + sc_{ID_1}^1 + r_{ID_2} c_{ID_2}^1 + r_m^1 c_m^1$

2-3) $S_m^2 = r_{ID_1} + sc_{ID_1}^2 + r_{ID_2} c_{ID_2}^2 + r_m^2 c_m^2$

2-4) $S_m^3 = r_{ID_1} + sc_{ID_1}^3 + r_{ID_2} c_{ID_2}^3 + r_m^3 c_m^3$

(여기서 $c_{ID_2}^0 = c_{ID_2}^1 \neq c_{ID_2}^2 = c_{ID_2}^3$, $r_m^0 = r_m^1 \neq r_m^2 = r_m^3$, $c_m^0 \neq c_m^1 \neq c_m^2 \neq c_m^3$ 이다.)

식 2-1), 2-2)에 의해 $r_m^0 = (c_m^0 - c_m^1)^{-1}(S_m^0 - S_m^1)$이고, 식 2-3), 2-4)에 의해 $r_m^2 = (c_m^2 - c_m^3)^{-1}(S_m^2 - S_m^3)$이다. 이를 이용해 식 2-1), 2-3)으로부터 다음과 같이 r_{ID_2}를 구할 수 있다.

$$r_{ID_2} = (c_{ID_2}^0 - c_{ID_2}^2)^{-1}(S_m^0 - r_m^0 c_m^0 - S_m^2 + r_m^2 c_m^2)$$

따라서 r_{ID_2}와 r_m^0를 모두 구했으므로 식 2-1)에서 s를 구할 수 있다. 나머지 구체적인 과정은 분량의 제한으로 생략한다.

③, ④의 경우도 ②와 마찬가지로 multiple

forking lemma를 적용하여 식 1), 2)로부터 s를 구할 수 있다. 이때 TLHIBS 기법에서 h_1질의는 h_2질의보다 항상 먼저 일어나므로 반대의 순서에 대해서는 고려하지 않아도 된다.

이로써 경우 ①~④ 모두에서 s를 구할 수 있으므로 공격자 A가 게임에서 승리하는 모든 경우에 대해서 C가 A를 이용해 DLP 문제를 풀 수 있음을 의미한다. □

IV. 제안하는 인증 시스템

본 장에서는 3.1절에서 제안한 TLHIBS 기법을 적용하여 VANET 환경을 위한 익명 인증 시스템을 제안한다.

4.1 제안하는 시스템 모델

4.1.1 시스템 모델

제안하는 시스템 모델은 [Fig. 4]와 같이 5개의 개체로 PKG, TRA(tracing authority), 차량의 제조사, 도로에 있는 RSU(Road-Side Unit), 차량에 탑재된 OBU로 이루어져 있다.

TRA와 PKG는 신뢰기관으로, TRA는 차량의 실제 ID로부터 Pseudo-ID를 생성하며 필요한 경우 서명된 메시지의 실제 ID를 복원할 수 있는 권한을

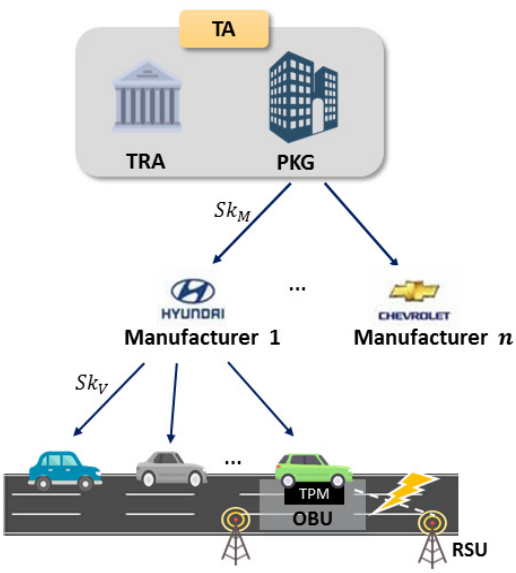

Fig. 4. The proposed system model

가지고, PKG는 제조사의 비밀키를 발급할 수 있는 권한을 가진다. 제조사는 PKG로부터 발급받은 비밀키를 이용하여 차량의 비밀키를 발급한다. 차량은 탑재된 OBU에 제조사로부터 발급받은 키를 설치하여 서명을 생성해 주변의 다른 차량(OBU)이나 RSU에 전송한다. 기존의 연구[4, 6, 9, 10]에서 차량 네트워크 모델은 2계층으로 구성되어 있다. 하위 계층은 차량의 OBU와 도로 위에 있는 RSU로 구성되고, 상위 계층은 신뢰기관과 교통관제 센터와 같은 응용 서버(application server)로 구성된다. 하위 계층에서 OBU와 RSU는 무선 통신 표준으로 DSRC(Dedicated Short-Range Communication) 프로토콜을 사용한다[14]. 상위 계층에서 RSU는 신뢰기관과 응용 서버와 TLS(Transport Layer Security) 프로토콜을 사용하여 안전한 채널로 유선 통신한다. 제안하는 시스템 모델에서 하위 계층은 동일하며 상위 계층에 제조사가 추가되어 구성된다. 제안하는 시스템 모델에서는 다음과 같이 가정한다:

1. TRA와 PKG는 항상 신뢰되고 공모하지 않는다. 또한 이들은 충분한 연산 능력과 저장 공간을 가진다. 한편 OBU는 제한적인 연산 능력을 가진다.
2. 모든 차량에는 적어도 하나 이상의 OBU가 장착되어 있으며 GPS(Global Positioning System)를 통해 위치 정보를 알 수 있다. 또한 RSU와 통신하며 시간 동기화를 통해 정확한 시간 정보를 얻을 수 있다.
3. 모든 차량에는 시큐어 엘리먼트(secure element)와 같은 TPD가 장착되어 여기에 Pseudo-ID에 대한 비밀키를 저장한다. 차량은 주기적으로 제조사와 TRA를 통해 Pseudo-ID 과 비밀키 쌍을 보충한다.

4.1.2 보안요구사항

제안하는 인증 기법이 VANET 환경에서 안전한 통신을 지원하기 위해 만족해야 할 보안요구사항은 다음과 같다:

- 메시지 인증(message authentication): 검증자는 메시지가 정당한 차량으로부터 위조나 변조 없이 전송되었는지 검증할 수 있어야 한다.
- ID 프라이버시 보호(ID privacy preserving): 차량의 실제 ID는 다른 차량이나 RSU로부터 익명으로 보호되어야 한다.

- 추적가능성(traceability): 차량의 실제 ID가 보호되더라도 필요한 경우 신뢰기관으로부터 차량의 실제 ID를 복원하여 추적할 수 있어야 한다.
- 부인방지(non-repudiation): 악의적인 차량은 신뢰기관에 의해 추적된 경우 잘못된 메시지를 전송한 것에 대해 부인할 수 없어야 한다.
- 불연결성(unlinkability): 서명된 메시지들이 동일한 차량으로부터 생성된 것인지 알 수 없어야 한다.
- 재전송 저항성(Replay assistance): 악의적인 운전자가 메시지가 유효하지 않은 시점에 서명된 메시지를 재전송할 수 없어야 한다.

4.2 조건부 익명성

VANET에서는 차량의 프라이버시를 보호하지만 사고가 발생하였을 경우 책임자를 식별할 수 있도록 조건부 익명성이 보장되어야 한다. 제안하는 인증 기법은 신뢰기관 TRA를 통해 조건부 익명성을 제공한다. 차량은 TRA로부터 차량의 실제 ID에 대한 Pseudo-ID를 생성하고 이를 이용해 서명을 생성한다. Pseudo-ID에 대한 비밀키로 서명을 생성하여 프라이버시를 보호하고 식별이 필요한 경우 TRA가 자신의 마스터 비밀키를 이용하여 차량의 실제 ID를 복원할 수 있다.

4.3 제안하는 인증 기법

제안하는 인증 기법은 제안한 TLHIBS 기법을 이용하며 다음 5단계로 구성된다: 시스템 설정 단계, 제조사의 비밀키 발급 단계, Pseudo-ID 생성/차량의 비밀키 발급 단계, 차량의 서명 생성 단계, 메시지 검증/일괄검증 단계

시스템 설정 단계에서는 TRA와 PKG가 공개 파라미터를 생성한다. 제조사의 비밀키 발급 단계에서는 PKG가 시스템 내 모든 제조사의 비밀키를 발급한다. Pseudo-ID 생성/차량의 비밀키 발급 단계에서는 TRA가 차량의 실제 ID를 확인한 뒤 실제 ID에 대한 Pseudo-ID를 생성하고, 제조사에서 생성된 Pseudo-ID에 대한 비밀키를 발급한다. 차량은 TRA로부터 생성된 Pseudo-ID와 제조사로부터 발급받은 비밀키 여러 쌍을 OBU에 탑재된 TPD에 사전에 설치하고 정기적으로 TRA와 제조사를 통해 보충한다. 차량의 서명 생성 단계에서는 설치된 공개 파라미터와 비밀키를 이용하여 서명을 생성해 주변의 다른 차량이나 RSU에게 서명을 전송한다. 메시지 검증/일괄검증 단계에서는 서명을 전송받은 주변 차량이나 RSU에서 하나의 메시지 또는 여러 메시지를 일괄적으로 검증한다.

- **시스템 설정 단계**: PKG와 TRA는 시스템을 설정을 위해 다음 과정을 수행한다.

1. PKG와 TRA는 TLHIBS 기법의 $Setup$ 알고리즘을 이용하여 위수가 소수 q인 군 $\mathbb{G}$를 생성하고 $\mathbb{G}$의 생성원 $P \in \mathbb{G}$를 선택한다.
2. PKG는 임의의 $s \in Z_q^*$를 선택하고 $P_{pub} = sP$를 계산한다. s는 PKG의 비밀키 발급을 위한 마스터 비밀키이다. TRA 또한 임의의 $\alpha \in Z_q^*$를 선택하여 $T_{pub} = \alpha P$를 계산한다. 여기서 α는 TRA의 Pseudo-ID 생성을 위한 마스터 비밀키이다.
3. PKG와 TRA는 네 개의 일방향 해시 함수 $H: \{0,1\}^* \rightarrow Z_q^*, h_i : \{0,1\}^* \rightarrow Z_q^* (i = 1,2,3)$를 선택하고, 공개 파라미터 $pp = \{q, P, P_{pub}, T_{pub}, H, h_1, h_2, h_3\}$를 설정하여 공개한다. 여기서 공개 파라미터 pp는 시스템 내 모든 제조사와 차량에 분배되고 차량은 TPD에 pp를 저장한다.

- **제조사의 비밀키 발급 단계**: 이 단계에서 시스템 내 모든 제조사는 자신의 ID_M에 대한 비밀키 sk_{ID_M}를 PKG로부터 발급받는다. 구체적인 과정은 다음과 같다.

1. PKG는 TLHIBS 기법의 $Extract$[1] 알고리즘을 이용하여 sk_{ID_M}을 다음과 같이 계산한다.
   $R_{ID_M} = r_{ID_M} P,\ c_{ID_M} = h_1(ID_M, R_{ID_M})$
   $S_{ID_M} = r_{ID_M} + c_{ID_M} \cdot s$
   여기서 $r_{ID_M} \in Z_q^*$은 난수이다.
2. 제조사 M은 PKG로부터 비밀키 $sk_{ID_M} = \{R_{ID_M}, S_{ID_M}\}$를 안전한 채널을 통해 발급받는다.

- **Pseudo-ID 생성 단계/차량의 비밀키 발급 단계**: 이 단계에서는 [Fig. 5]와 같이 각 차량은 실제 ID RID_V를 TRA로 전송하고 TRA는 실제 ID RID_V에 대한 Pseudo-ID PID_V를 생성한다. TRA는 생성된 PID_V를 제조사 M에게

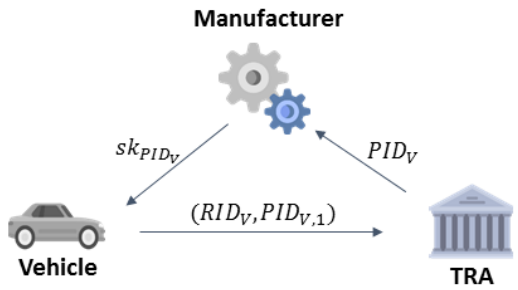

Fig. 5. Pseudo-ID generation and vehicle's private key extraction

전송하고, 제조사 M은 차량 V에게 Pseudo-ID PID_V에 대한 비밀키 sk_{PID_V}를 발급한다. Pseudo-ID 생성은 C. Zhang이 제안한 방법 [6]을 이용한다. 구체적인 과정은 다음과 같다.

1. 실제 ID가 RID_V인 차량 V는 임의의 $d_V \in Z_q^*$를 선택하여 $PID_{V,1} = d_V P$를 계산한다. 그리고 $(RID_V, PID_{V,1})$을 안전한 채널을 통해 TRA로 전송한다.
2. TRA는 전송받은 RID_V를 확인한 뒤 $PID_{V,2}$을 계산한다.
   $PID_{V,2} = RID_V \oplus H(\alpha PID_{V,1}, PID_{V,1}, t_V, T_{pub})$
   여기서 t_V는 Pseudo-ID PID_V의 유효기간을 의미한다. TRA는 비밀키 발급을 위해 Pseudo-ID $PID_V = (PID_{V,1}, PID_{V,2}, t_V)$를 안전한 채널을 통해 제조사 M으로 전송한다.
3. Pseudo-ID PID_V를 전송받은 제조사 M은 TLHIBS 기법의 $Extract^2$ 알고리즘을 이용하여 PID_V에 대한 비밀키 sk_{PID_V}를 다음과 같이 계산한다.
   $R_{PID_V} = r_{PID_V} P$, $c_{PID_V} = h_2(PID_V, R_{PID_V}, ID_M, R_{ID_M})$, $S_{PID_V} = S_{ID_M} + c_{PID_V} \cdot r_{PID_V}$
   여기서 $r_{PID_V} \in Z_q^*$은 난수이다.
4. 제조사 M은 $sk_{PID_V} = \{R_{ID_M}, R_{PID_V}, S_{PID_V}\}$을 차량 V로 안전한 채널을 통해 전송한다.

- **차량의 서명 생성 단계**: 이 단계에서 차량은 전송할 메시지에 대한 서명을 생성하고 생성한 서명을 RSU나 주변 차량에게 전송한다. 구체적인 과정은 다음과 같다.

1. 차량 V는 TPD에 저장되어있는 Pseudo-ID와 이에 대한 비밀키 쌍 중 임의로 한 Pseudo-ID PID_V와 이에 대한 sk_{PID_V}를 선택하고 TLHIBS 기법의 $Sign$ 알고리즘을 이용하여 다음과 같이 서명 σ을 계산한다.
   $R_m = r_m P$
   $c_m = h_3(m, PID_V, R_{PID_V}, ID_M, R_{ID_M}, R_m, tt_m)$,
   $S_m = S_{PID_V} + c_m \cdot r_m$
   여기서 $r_m \in Z_q^*$는 난수이며 tt_m은 현재의 타임스탬프이다. 서명 $\sigma = \{R_{ID_M}, R_{PID_V}, R_m, S_m\}$은 메시지 m에 대한 서명이고, 현재의 타임스탬프 tt_m은 PID_V에 대한 타임스탬프이다.
2. 차량 V는 $\{PID_V, m, tt_m, \sigma\}$을 근처의 RSU나 다른 차량에게 전송한다.

- **메시지 검증/일괄검증 단계**: 서명된 메시지를 받은 RSU나 주변 차량은 정당하지 않은 차량이 위장하여 메시지를 생성하거나 잘못된 메시지를 생성하는 것을 방지하기 위해 메시지의 서명을 검증한다. 구체적인 과정은 다음과 같다.

1. 검증자는 n개의 서로 다른 메시지와 서명 쌍 $\{PID_{V_i}, m_i, tt_{m_i}, \sigma_i\}$ $(i = 1, ..., n)$을 받게 되면, 우선 타임스탬프 tt_{m_i}와 Pseudo-ID PID_{V_i}의 t_i가 유효한 시간 구간에 속하는지 확인한다.
2. 시간 정보가 모두 유효하다면 검증자는 TLHIBS 기법의 $BVerify$ 알고리즘을 이용하여 다음 과정을 통해 검증을 수행한다.
   ①. 검증자는 $i = 1, ..., n$에 대해 다음식을 계산한다.
   $c_{ID_{M_i}} = h_1(ID_{M_i}, R_{ID_{M_i}})$
   $c_{PID_{V_i}} = h_2(PID_{V_i}, R_{PID_{V_i}}, ID_{M_i}, R_{ID_{M_i}})$
   $c_{m_i} = h_3(m_i, PID_{V_i}, R_{PID_{V_i}}, ID_{M_i}, R_{ID_{M_i}}, R_{m_i}, tt_{m_i})$
   ②. 검증자는 작은 지수 활용 검사를 수행하기 위해 임의의 벡터 $\delta = \{\delta_1, ..., \delta_n\}$을 선택한다. 여기서 $i = 1, ..., n$에 대해 $\delta_i \in \{0,1\}^l$이다. 일반적으로, VANET에서 $l = 80$으로 충분하다.
   ③. 검증자는 다음 등식이 성립하는지 확인한다.
   $$(\sum_{i=1}^{n} \delta_i S_{m_i}) P = (\sum_{i=1}^{n} \delta_i R_{ID_{M_i}}) + (\sum_{i=1}^{n} \delta_i c_{ID_{M_i}}) P_{pub} + (\sum_{i=1}^{n} \delta_i c_{PID_{V_i}} R_{PID_{V_i}}) + (\sum_{i=1}^{n} \delta_i c_{m_i} R_{m_i})$$

Table 2. Comparison of computational complexity of the ID-based signature schemes : T_P = time for performing a pairing operation, T_{MTP} = time for performing a MapToPoint operation, T_{PM} = time for performing a point multiplication, T_M = time for performing a scalar multiplication operation

	Sign	*Verify*	*Bverify*	Pairing	Hierarchy
He et al. [1]	$2T_{PM}+T_M$	$2T_P+3T_{PM}$	$2T_P+(2n+1)T_{PM}$	O	O
Lo et al. [4]	$T_{PM}+T_M$	$3T_{PM}$	$(n+2)T_{PM}$	X	X
Wang et al. [15]	$3T_{PM}$	$2T_P+$ $2T_{PM}+T_M$	$2T_P+$ $(n+1)T_{PM}+nT_M$	O	X
Ours	$T_{PM}+T_M$	$4T_{PM}$	$(2n+2)T_{PM}$	X	O

성립하는 경우 n개의 서명 $\{\sigma_1,...,\sigma_n\}$의 정당성이 일괄적으로 검증된다.

V. 분 석

본 장에서는 4.3절에서 제안한 인증 기법의 안전성을 분석하고 기존 기법과 비교·분석한다.

5.1 안전성 분석

- 메시지 인증, 부인방지: 4.3절에서 제안한 인증 기법은 3.1절에서 제안한 TLHIBS 기법을 이용하여 제안하였다. TLHIBS 기법의 안전성은 3.2절에서 DLP의 어려움에 기반하여 선택적 ID에 대해 선택 메시지 공격에 대한 존재적 위조가 불가능함을 증명하였다. 따라서 제안한 인증 기법의 안전성은 제안한 TLHIBS 기법의 안전성으로 리덕션되어 안전성이 증명된다. 이 기법을 통해 메시지 인증과 부인방지가 보장된다.
- ID 프라이버시 보호: 제안한 인증 기법에서 차량의 Pseudo-ID는 TRA의 마스터 비밀키 α와 차량이 선택한 난수 d_V의 조합으로 α나 d_V를 알아야만 실제 ID 복원에 필요한 $\alpha PID_{V,1}$를 구할 수 있다. 즉 이것의 안전성은 CDH(Computational Diffie-Hellman) 문제로 귀결되어 실제 ID의 차량과 TRA를 제외하고는 차량의 Pseudo-ID로부터 실제 ID를 알아낼 수 없다.
- 추적가능성: 서명된 메시지에서 차량의 Pseudo-ID $PID_V=(PID_{V,1},PID_{V,2},t_V)$가 주어졌을 때 TRA는 자신의 마스터 비밀키 α를 이용하여 차량의 실제 ID를 다음과 같이 구할 수 있다.

$$PID_{V,2}\oplus H(\alpha PID_{V,1},PID_{V,1},t_V,T_{pub})=RID_V$$

- 불연결성: 불연결성은 공격자가 서명된 메시지들이 동일한 차량으로부터 생성된 것인지 알 수 없음을 의미한다. 제안하는 기법은 매 서명 생성시 다른 Pseudo-ID를 이용하므로 불연결성을 만족한다. 다른 Pseudo-ID로부터 동일한 차량인지 확인하기 위해서는 CDH 문제를 풀어야 하므로 공격자는 이를 확인할 수 없다.

5.2 비교·분석

본 절에서는 기존의 ID 기반 서명 기법들과 제안한 TLHIBS 기법의 효율성을 비교·분석한다.

[Table 2]은 기존의 ID 기반 서명 기법들과 제안한 TLHIBS 기법의 알고리즘 수행에 필요한 계산 복잡도를 비교하여 나타낸다.

제안한 기법은 페어링을 사용하지 않는 기법 [4]와 비교하면, 서명 검증, 일괄검증 연산량이 각각 T_{PM}, nT_{PM} 늘어난 비용으로 계층적 구조를 제공한다. 또한 페어링을 사용하는 기존의 TLHIBS 기법 [1]에 비해 서명 생성, 서명 검증, 일괄검증 연산량이 T_{PM}, $2T_P-T_{PM}$, $2T_P-T_{PM}$ 만큼 감소하였다. PKG의 오버헤드를 해결하는 기존의 연구[15]에 비해서는 서명 생성, 서명 검증, 일괄검증 연산량이 각각 $2T_{PM}-T_M$, $2T_P-2T_{PM}+T_M$, $2T_P-(n+1)T_{PM}+nT_M$ 만큼 감소하였다. 제안한 기법은 비교적 적은 비용으로 계층 구조를 제공하며, 계층을 고려하더라도 [1], [15]에 비해 효율적이다.

VI. 결 론

본 논문에서는 VANET 환경을 위한 계층적 구조의 새로운 익명 인증 시스템을 제안하였다. 기존 시스템 모델의 문제점인 PKG의 오버헤드를 줄이는 실용성을 높인 새로운 계층적 구조의 시스템 모델을 제안하고, 제안한 시스템 모델에 적용할 수 있는 효율적인 계층적 ID 기반 서명 기법을 제안하였다. 제안한 기법은 겹선형 함수를 사용하지 않고 설계되어 검증 과정에서 페어링 연산을 필요로 하지 않는다. 따라서 기존의 계층을 지원하는 기법보다 효율적이며 기존의 계층을 지원하지 않는 기법보다 검증 과정에서 T_{PM}만큼의 비교적 적은 추가 연산으로 제안한 계층적 구조의 시스템 모델에서 지원된다. 마지막으로 기존의 VANET 환경에서 ID 기반 서명 기법들의 안전성 증명이 잘못된 것과는 다르게 제안한 기법의 안전성을 이산 대수 문제에 리덕션하여 증명하였다.

References

[1] D. He, N. Kumar, KKR. Choo, and W. Wu, "Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system," IEEE Transactions on Information Forensics and Security, vol. 12, no. 2, pp. 454-464, Feb. 2017.

[2] M. Bellare, J.A. Garay, and T. Rabin, "Fast batch verification for modular exponentiation and digital signatures," In International Conference on the Theory and Applications of Cryptographic Techniques, pp. 236-250, May 1998.

[3] J.K. Liu, T.H. Yuen, M.H. Au, and W. Susilo, "Improvements on an authentication scheme for vehicular sensor networks," Expert Systems with Applications, vol. 41, no. 5, pp. 2559-2564, Apr. 2014.

[4] N.W. Lo and J.L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 5, pp. 1319-1328, May 2016.

[5] J. Camenisch, S. Hohenberger, and M.Ø. Pedersen, "Batch verification of short signatures," J. Cryptology, vol. 25, no. 4, pp. 723 - 747, 2012.

[6] C. Zhang, R. Lu, X. Lin, P.H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," Proceeding of IEEE INFOCOM, pp. 246 - 250, 2008.

[7] M. Raya and J.P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39 - 68, 2007.

[8] X. Lin, X. Sun, P.H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, Nov. 2007.

[9] K.A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," IEEE Transactions on Vehicular Technology, vol. 61, no. 4, pp. 1874 - 1883, May 2012.

[10] S.F. Tzeng, S.J. Horng, T. Li, X. Wang, P.H. Huang, and M.K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," IEEE Transactions on Vehicular Technology vol. 66, no. 4, pp. 3235-3248, Apr. 2017.

[11] S. Chatterjee, C. Kamath, and V. Kumar, "Galindo-Garcia identity-based signature revisited," International Conference on Information Security and Cryptology, 2012.

[12] R. Anderson and M.G. Kuhn, "Tamper

resistance－a cautionary note," Proceedings of the second Usenix workshop on electronic commerce, vol. 2, pp. 1-11, 1996.

[13] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper resistance mechanisms for secure embedded systems," In VLSI Design, 2004. Proceedings. 17th International Conference on, pp. 605-611, 2004.

[14] Dedicated Short Range Communications (DSRC). [Online]. Available: http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm

[15] Y. Wang, H. Zhong, Y. Xu, J. Cui, and F. Guo, "Efficient extensible conditional privacy preserving authentication scheme supporting batch verification for VANETs," Security and Communication Networks, vol. 9, no. 18, pp. 5460-5471, 2016.

〈저자소개〉

배 경 진 (Kyungjin Bae) 학생회원
2016년 2월: 고려대학교 수학과 졸업
2016년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 암호 프로토콜, 암호이론, 인증

이 영 경 (Youngkyung Lee) 학생회원
2014년 2월: 고려대학교 수학과 졸업
2016년 2월: 고려대학교 정보보호대학원 석사 졸업
2016년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 암호 프로토콜, 암호이론, 인증 및 키 교환

김 종 현 (Jonghyun Kim) 학생회원
2014년 2월: 성균관대학교 수학과 졸업
2014년 3월~현재: 고려대학교 정보보호대학원 석박사 통합과정
〈관심분야〉 암호 프로토콜, 암호이론, 함수 암호

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학사 졸업
1987년 12월: Oklahoma University 전산학과 석사 졸업
1992년 5월: Oklahoma University 전산학과 박사 졸업
1993년 3월~1997년 2월: 고려대학교 전산학과 조교수
1997년 3월~2001년 2월: 고려대학교 전산학과 부교수
2001년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 암호 프로토콜, 암호이론, USN이론, 키 교환, 익명성 연구, PET 기술