情報保護學會論文誌
第20卷 第1號, 2010. 2

그룹 서명 기반의 차량 네트워크에서 상호 신분 확인 및 세션키 교환 기법*

김 대 훈,† 최 재 덕, 정 수 환‡
숭실대학교 정보통신전자공학부

Mutual Identification and Key Exchange Scheme in Secure Vehicular Communications based on Group Signature*

Daihoon Kim,† Jaeduck Choi, Souhwan Jung‡
School of Electronic Engineering, Soongsil University

요 약

본 논문에서는 인증 및 조건부 프라이버시, 부인방지 기능만 제공되는 그룹 서명 기반의 차량 네트워크 환경에서 상호 신분 확인 및 세션키 교환 기법을 제안한다. 다양한 차량 네트워크 환경에서 인증, 조건부 프라이버시, 부인방지, 데이터 기밀성과 같은 보안 서비스들이 요구되지만, 최근 연구되고 있는 그룹 서명 기반의 차량 네트워크 보안 기술들은 신분 확인 후 사용자 데이터를 보호하기 위한 세션키 교환 과정을 고려하고 있지 않다. 본 논문에서는 하나의 인증값으로 매번 다르게 생성되는 Diffie-Hellman 파라미터들의 인증 유효성을 제공하는 방법을 이용하여 신분 확인 및 세션키 교환 기능을 제공한다. 제안 기법은 인증값 저장 공간 및 인증값 생성 요청에 대한 통신 오버헤드가 적고, 매번 새로운 Diffie-Hellman 파라미터 생성으로 보다 안전한 세션키 교환이 가능하다. 또한 제안 기법은 다양한 차량 응용 서비스에서 요구하는 보안 요구사항들을 만족한다.

ABSTRACT

This paper proposes a mutual identification and session key exchange scheme in secure vehicular communication based on the group signature. In VANETs, security requirements such as authentication, conditional privacy, non-repudiation, and confidentiality are required to satisfy various vehicular applications. However, existing VANET security methods based on the group signature do not support a mutual identification and session key exchange for data confidentiality. The proposed scheme allows only one credential to authenticate ephemeral Diffie-Hellman parameters generated every key exchange session. Our scheme provides a robust key exchange and reduces storage and communication overhead. The proposed scheme also satisfies security requirements for various application services in VANETs.

Keywords: VANET, Group Signature, Mutual Identification, Key Exchange

I. 서 론

안전한 차량 서비스를 제공하기 위해서 차량 무선 네트워크 (VANET, Vehicle Ad hoc NETwork)를 이용한 지능형 교통 안전시스템 (ITS, Intelligent Transportation System)이 활발하게 연구되고 있다. VANET은 인터넷 서비스를 위한 V2I

접수일(2009년 8월 3일), 수정일(2009년 10월 27일), 게재확정일(2009년 12월 11일)
* 이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임. (No. 2009-0053879)
† 주저자, upitere@cns.ssu.ac.kr
‡ 교신저자, souhwanj@ssu.ac.kr

(Vehicular-to-Infrastructure) 통신 구조와 차량 사이 혹은 차량과 RSU (Road Side Unit) 사이에서 차량 상태 정보 및 교통안전 정보를 교환하는 V2V (Vehicular-to-Vehicular) 통신 구조가 있다. 이와 같은 차량 네트워크에서는 운전자의 생명을 보호하기 위한 차량 안전 통신 기술이 중요하기 때문에 차량의 속도, 방향, 차간 거리와 같은 상태 정보뿐만 아니라 교통사고 발생, 갑작스런 기상 변화, 노면 결빙 상태 등을 뒤따르는 차량들에게 안전하고 신뢰성 있게 전달하기 위한 차량 안전 메시지의 보안 서비스 제공이 중요한 이슈이다. 또한, 최근 사람들의 개인 프라이버시 보호 문제가 크게 이슈화 되면서 차량 네트워크에서도 운전자의 위치 및 이동 경로 등에 대한 프라이버시 보호가 중요하게 다루어지고 있다. 하지만, 차량 네트워크에서는 프라이버시 제공 기술뿐만 아니라 분쟁이 발생할 경우 분쟁을 해결할 수 있는 서명된 메시지를 개봉하여 신분을 확인할 수 있는 조건부 프라이버시 기술이 제공되어야 한다 [1-5].

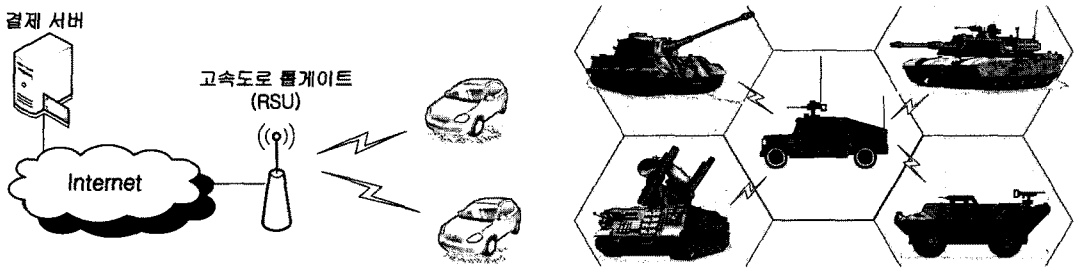
이를 제공하기 위하여 차량 네트워크에서는 인증 및 조건부 프라이버시, 부인방지 기능을 제공할 수 있는 그룹 서명 기법을 사용한 보안 기술들이 다양하게 연구되고 있다 [8-13]. 그룹 서명 방식은 [6] 서명자가 익명으로 메시지를 직접 서명함으로써 프라이버시를 제공할 뿐만 아니라 서명자를 밝힐 필요가 있다면 그룹 관리자를 통하여 서명자를 확인할 수 있는 조건부 프라이버시를 제공하기 때문에, 교통안전 정보를 교환하는 V2V 통신에서 요구하는 보안 요구 사항을 만족한다. 또한, 2004년 Boneh가 그룹 서명의 길이가 너무 길어서 실제 구현하여 사용하기 어렵다는 단점을 해결한 기법을 제안함으로써 [7], 그룹 서명 기법을 적용한 차량 네트워크에서 메시지에 대한 서명 및 조건부 프라이버시 제공 연구가 활기를 띠고 있다.

그러나 인증 및 부인방지, 조건부 프라이버시 기능을 제공하는 기존의 그룹 서명 기법만으로는 다양한 차량 네트워크 응용 서비스를 지원하기 힘들다. 예를 들어, 경찰차, 소방차, 구급차와 같은 특수 차량들 사이 또는 일반 차량들 사이에서 비밀통신 및 고속도로 톨게이트에서와 같은 결제 서비스에서는 상호 신분 확인 및 사용자의 데이터를 보호하기 위한 세션키 교환 방법이 필요하다. 본 논문에서는 다양한 차량 네트워크 응용 서비스에서 요구하는 보안 서비스를 만족시키기 위해서 그룹 서명 기반의 차량 네트워크에서 상호 신분 확인 및 세션키를 교환할 수 있는 기법을 제안한다. 제안 기법은 트랩도어 해쉬 함수를 통해 생성된 하나의 인증값으로 매번 다르게 생성되는 Diffie-Hellman (DH) 파라미터들의 인증 유효성을 제공하는 방법을 이용하여 인증 및 세션키 교환 기능을 제공한다. 제안 기법은 인증값 저장 공간 및 인증값 발급 요청에 대한 통신 오버헤드가 적고, 매번 새로운 Diffie-Hellman 파라미터 생성으로 보다 안전한 세션키 교환이 가능하다. 또한 제안 기법은 그룹 서명 기반의 차량 네트워크 환경에 상호 신분 확인 및 데이터 기밀성/무결성을 제공함으로써 다양한 차량 응용 서비스에서 요구하는 보안 요구사항들을 만족한다.

본 논문의 구성은 다음과 같다. 2장에서 차량 네트워크 환경에서 보안 요구사항, 그룹 서명 기반의 차량 네트워크 보안 기술, 본 논문에서 제안하는 기법의 이해를 돕기 위한 관련 연구들을 살펴보고, 3장에서 그룹 서명 기반의 차량 네트워크 환경에서 인증된 세션키 교환 프로토콜을 제안하고, 4장에서 제안 프로토콜의 안전성 및 효율성 측면을 분석한다. 마지막으로 5장에서 결론을 맺는다.

II. 관련 연구

2.1 보안 요구 사항



(a) 차량에서 결제 서비스 (b) 특수 목적 차량간 비밀통신

[그림 1] 차량 네트워크에서 비밀통신이 요구되는 환경

안전한 차량 네트워크 서비스를 제공하기 위해서 다음과 같은 보안 요구 사항을 만족해야한다.

· 인증 (Authentication)

차량 메시지에 대한 출처가 정당한 사용자라는 것을 검증할 수 있어야 하며, 전송되는 메시지는 중간에 위조 및 변조 되지 않았음을 확인 할 수 있어야 한다.

· 조건부 프라이버시 (Conditional Privacy)

차량 메시지의 출처에 대해서 제 3자가 알 수 없어야 하고, 분쟁이 발생할 경우 서명된 메시지를 신뢰할 수 있는 제 3의 기관이 개봉하여 신분을 확인 할 수 있어야 한다.

· 부인 방지 (Non-repudiation)

분쟁과 연관된 차량이 보낸 메시지에 대해서 부인하거나 반박할 수 없도록 보장되어야 한다.

· 키 교환 (Key Exchange)

기밀 통신을 요구하는 차량은 기밀 통신을 원하는 차량과 상호 신분 확인 후, 데이터를 보호할 수 있는 세션키를 생성해야 하며, 생성된 세션키는 다양한 공격으로부터 안전해야 한다.

위와 같은 차량 네트워크 보안 요구 사항을 만족할 수 있는 방법 중에 그룹 서명을 사용하는 것이 주목되고 있다. 왜냐하면, 안전한 차량 네트워크 서비스를 위해 그룹 서명 기법은 인증, 조건부 프라이버시, 부인 방지 등의 보안 서비스를 제공하기 때문이다. 기밀 통신을 요구하는 차량 통신의 경우, 그룹 서명 기법을 사용하여 세션키를 교환할 수 있지만, 비밀 통신을 하고자 하는 상대가 자신이 통신하기를 원하는 상대인지 신분 확인 절차가 반드시 필요하다. 즉, 그룹 서명만을 이용하여 세션키를 교환 할 경우 자신이 통신하고자 하는 상대가 아닌 그룹 멤버 중에 하나와 통신할 수 있게 되는데, 이는 두 통신자 사이에서 교환되는 중요 메시지에 대한 기밀성을 보장할 수 없다. [그림 1]은 차량 네트워크에서 상호 신분 확인 및 세션키 교환 절차가 필요한 예를 보여준다. [그림 1]의 (a)와 같이 차량이 고속도로 톨게이트를 지나갈 때 결제 과정이 필요한데, 이 결제 과정에서 운전자의 신분이 노출되지 않도록 차량과 고속도로 톨게이트 접속 지점과의 통신 구간에 보안 채널이 형성되어야 한다. 또한, 보안 채널 형성시 운전자의 신분이 노출되어서도 안된다. 이를 만족하기 위해서 그룹 서명 기반의 차량 안전 시스템에서 상호 신분을 확인하고 세션키를 교환한 후, 신분 노출이 되지 않도록 결제 과정이 암호화되어야 한다. 즉, 평상시 익명성을 제공해주면서 결제 시스템과 같이 상호 신분 확인 및 암호화 통신이 필요한 환경에서는 그룹 서명 시스템으로 구축된 차량 네트워크에 상호 신분 확인 및 세션키 교환 기능이 추가되어야 한다. 또 다른 예로, [그림 1]의 (b)는 특수 목적 차량 통신 환경에서 차량간 비밀통신 시나리오를 보여준다. 군용 차량들 간에 통신시 또는 범죄 현장에서 경찰 차량, 소방 차량, 군용 차량들 간에 통신시에도 그룹 멤버들 간 특수 작전 수행을 위한 기밀 메시지가 외부 차량에 노출되지 않도록 세션키를 교환한 후 암호화 통신하는 것이 필요하다.

2.2 차량 통신에 적용된 그룹 서명 기법들

최근 차량 통신에서 조건부 프라이버시 문제를 해결하기 위해서 그룹 서명 기법을 이용한 메시지 서명 기법이 활발하게 연구되고 있다. Guo 등은 차량 통신 환경을 위하여 Tamper Resistance Device 기반의 그룹 서명 기법을 이용하여, 신뢰성 및 데이터 무결성, 조건부 프라이버시를 제공하는 보안 프레임워크를 제안하였다 [8]. Zhang 등은 차량 네트워크 환경에서 메시지 인증 및 조건부 프라이버시를 제공하기 위한 그룹 서명 기법에 그룹 관리자가 발급하는 그룹 개인키에 대한 폐기와 관리를 위하여 그룹 개인키 폐기 과정을 추가한 그룹 서명 기법을 제안하였고; 그룹 서명에 대한 메시지 크기와 계산 복잡도를 개선하여 차량 통신 환경에 적합하도록 하였다 [9]. Chaurasia 등은 차량 통신에서 효율적으로 메시지를 전파하고 전파된 메시지의 인증과 차량의 조건부 프라이버시를 제공하기 위해서 그룹 서명 기반의 메시지 인증 기법을 제안하였다 [10]. 또한, 그룹에 가입된 차량을 관리하기 위해서 중앙 그룹 발급 기관부터 지역 그룹 발급 기관을 가진 계층화된 그룹 관리 구조를 제안하였다. Sun과 Lin 등은 프라이버시 기능이 요구되지 않는 차량과 RSU 사이에서 통신은 ID 기반 서명 기법을 적용하였고, 차량들 사이에서는 프라이버시 기능을 제공해주기 위해 그룹 서명 기법을 적용하였다 [11-12]. Hao 등은 그룹 서명 기반의 차량 통신 환경을 제안하고, 차량이 메시지 서명 시 필요한 그룹 개인키의 안전한 발급을 위하여 공개키/개인키 기반의 그룹 개인키 분배 프로토콜을 제안하였다 [13]. 이와 같이 기존 차량 네트워크 환경에 적용된 그룹 서명 기법들은 인증 및 조건부 프라이버시, 부인방지 기능만을 제공하고, 비밀 통신을 위한 상호 신분 확인 및 세션키 교환 기능은 제공하고 있지 않다.

2.3 그룹 서명 및 트랩도어 해쉬 함수

이 절에서는 3장에서 제안하는 기법의 이해를 돕기 위한 관련 기술들을 소개한다.

2.3.1 그룹 서명

그룹 서명 기법은 [6-7] 그룹의 소속원이 신분을 알리지 않고 그룹의 소속원임을 확인하는 방식을 일반화한 개념으로 다음과 같은 특징이 있다. (i) 그룹의 가입된 멤버만이 서명을 할 수 있다. (ii) 서명을 받은 멤버는 서명을 통해 서명자가 그룹의 가입된 멤버라는 사실을 확인 할 수 있으나, 누구인지는 확인 할 수 없다. (iii) 서명자가 누구인지 확인이 필요한 경우, 그룹 관리자는 서명을 개봉하여 서명자를 찾아 낼 수 있다. 이러한 특징들 때문에 그룹 서명 기법은 차량 안전 통신에서 인증 및 조건부 프라이버시, 부인방지 기능을 제공하는데 적합하다.

일반적으로 그룹 서명 기법은 SETUP, JOIN, SIGN, VERIFY, OPEN과 같이 5단계를 통하여 서술되고 있다.

· SETUP

그룹 관리자가 그룹 멤버들이 사용할 그룹 개인키 (k) 생성 및 관리를 위한 그룹 공개키 (gpk)와 그룹 비밀키 (gsk)를 생성하는 과정이다.

· JOIN

그룹 멤버들이 그룹에 가입하는 과정이고 성공적으로 그룹 가입을 끝낸 사용자는 본인이 사용할 그룹 개인키 k를 생성 받는다.

· SIGN

그룹 멤버가 메시지 M에 대한 그룹 서명을 만드는 과정이다. 서명자는 자신의 그룹 개인키 k와 랜덤값을 이용하여 그룹 개인키 k에 대응하는 익명값 K를 생성하고, 그룹 개인키 k에 대응하는 익명값 K와 그룹 공개키 gpk로 메시지 M에 대한 그룹 서명 값 ($\sigma_k(M)$)을 생성한다.

· VERIFY

서명을 받은 멤버가 서명을 통해 서명자가 그룹의 가입된 멤버라는 사실을 확인하는 과정이다. 서명자로부터 받은 그룹 개인키 k에 대응하는 익명값 K와 그룹 서명 값 $\sigma_k(M)$을 그룹 관리자가 제공한 그룹 공개키 gpk로 확인함으로써 서명자가 그룹에 가입된 멤버라는 사실을 확인한다.

· OPEN

서명자가 누구인지 확인이 필요한 경우, 그룹 관리자는 그룹 비밀키 (gsk)로 서명을 개봉하여 서명자를 찾아내는 과정이다.

2.3.2 트랩도어 해쉬 함수

트랩도어 해쉬 함수는 [14] 일반 해쉬 함수의 문제점이라고 할 수 있는 충돌을 만드는 함수로써, 트랩도어 키를 소유한 사용자만이 메시지에 대한 해쉬 충돌을 찾을 수 있는 특징이 있다. 큰 소수 g, p를 생성하고 트랩도어 키 (TK, Trapdoor Key) a를 모듈러 p로의 곱셈군 Z_p^*의 요소 값으로 선택한다. 트랩도어 키를 사용하여 트랩도어 해쉬키 (HK, Trapdoor Hash Key) $y = g^a$을 계산한다. 초기 메시지 m_0와 랜덤값 r을 생성하고, 트랩도어 해쉬값 $h_{HK}(r, m_0) = g^r y^{m_0}$을 계산한다. 새 메시지 m_i에 대해서 해쉬 충돌값 c_i는 식 (1)과 같이 계산한다. 새 메시지 m_i에 대한 해쉬 충돌값 c_i를 계산함으로써, 초기 생성한 트랩도어 해쉬값을 그대로 사용하여 새 메시지 m_i에 대한 인증 값으로 사용할 수 있다.

$$\begin{aligned} h_{HK}(r, m_0) &= h_{HK}(c_i, m_i) \\ g^r y^{m_0} &= g^{c_i} y^{m_i} \\ c_i &= a(m_0 - m_i) + r \end{aligned} \quad (1)$$

III. 제안 기법

본 논문은 인증 및 조건부 프라이버시, 부인방지 기능만 제공되는 그룹 서명 기반의 차량 네트워크 보안 기술에 트랩도어 해쉬 함수를 이용하여 상호 신분 확인 및 세션키 교환 기법을 제안한다. 즉, 기존 SETUP, JOIN, SIGN, VERIFY, OPEN과 같이 5 단계를 갖는 그룹 서명 기법에 KEY EXCHANGE 단계를 제안한다. 또한, 상호 신분 확인을 위하여 필요한 인증값 δ를 그룹 멤버가 그룹 관리자로부터 발급 받는 과정을 JOIN 단계에 추가하였다. [표 1]은 제안 프로토콜에서 사용되는 표기법을 보여준다.

〔표 1〕 프로토콜 표기법

표기	정의
$\|\|$	두 개의 비트열의 연접
ID_x	차량 x 의 식별자
δ	차량 신분확인을 위하여 그룹 관리자가 서명한 차량 인증값
T_{Expire}	인증값의 유효시간
$T_{Current}$	현재 시간
p	큰 소수
Z_p^*	모듈러 p로의 곱셈군
g	Z_p^*의 생성자
$rsaPK^+/PK^-$	RSA 공개키/개인키
$nonce$	일회성 랜덤값
h_{HK}	트랩도어 해쉬 함수
m_0, r	트랩도어 해쉬값 생성을 위한 초기 메시지 및 랜덤값
α	트랩도어 키
$y=g^{\alpha}$	트랩도어 해쉬키
m_i	트랩도어 메시지
c_i	트랩도어 해쉬 충돌값
k	그룹 개인키
$\sigma_k(M)$	그룹 서명
$E_{sk}(M)$	세션키 sk로 암호화된 메시지

• SETUP 단계

차량 그룹 관리자가 그룹의 차량 멤버들이 사용할 그룹 개인키 (k) 생성과 관리를 위한 그룹 공개키 (gpk)와 그룹 비밀키 (gsk)를 생성한다. 또한, 차량 상호 신분 확인 인증값를 위하여, 그룹 관리자의 RSA 공개키/개인키를 생성한다.

• JOIN 단계

본 논문에서 제안하는 기법은 차량 응용 서비스에서 상호 신분 확인을 위한 인증값이 필요하다. 각 차량 Alice와 Bob은 기존 그룹 서명 기법에서 JOIN 단계를 수행하여 각 그룹 개인키 k_A, k_B를 생성 받고 다음과 같이 멤버 차량들의 인증값을 생성한다. 먼저, 차량은 트랩도어 해쉬키 y 및 트랩도어 해쉬값 $h_{HK}(r, m_0)$을 식 (2)와 같이 생성하고, 차량 ID, 트랩도어 해쉬키 및 트랩도어 해쉬값을 그룹 관리자에게 전송한다. 그룹 관리자는 차량의 신분 확인에 사용할 인증값 δ을 식 (3)과 같이 생성하고, 차량이 사용할 그룹 개인키 k, 서명의 유효시간 T_{Expire}와 함께 차량에게 전송함으로써 JOIN 단계를 완료한다.

$$y = g^{\alpha},\ h_{HK}(r, m_0) = g^r y^{m_0} \quad (2)$$

$$\delta = rsaPK_{GM}^{-}(ID \| h_{HK} \| g^{\alpha} \| T_{Expire}) \quad (3)$$

• SIGN 단계

차량 Alice는 익명성을 제공하기 위하여 그룹 개인키 k_A와 그룹 공개키 gpk로 메시지 M에 대한 그룹 서명 값 $\sigma_{k(A)}(M)$을 생성한다. 마지막으로, 차량 Alice는 차량 안전 메시지 M, 그룹 서명 값 $\sigma_{k(A)}(M)$을 브로드캐스팅 한다.

• VERIFY 단계

익명의 차량으로부터 $\{M, \sigma_{k(A)}(M)\}$ 값들을 수신한 차량들은 그룹 관리자가 제공한 그룹 공개키 gpk로 서명 값을 검증하여 차량 안전 메시지 M을 보낸 익명의 차량이 그룹에 가입된 멤버라는 사실을 확인한다.

• OPEN 단계

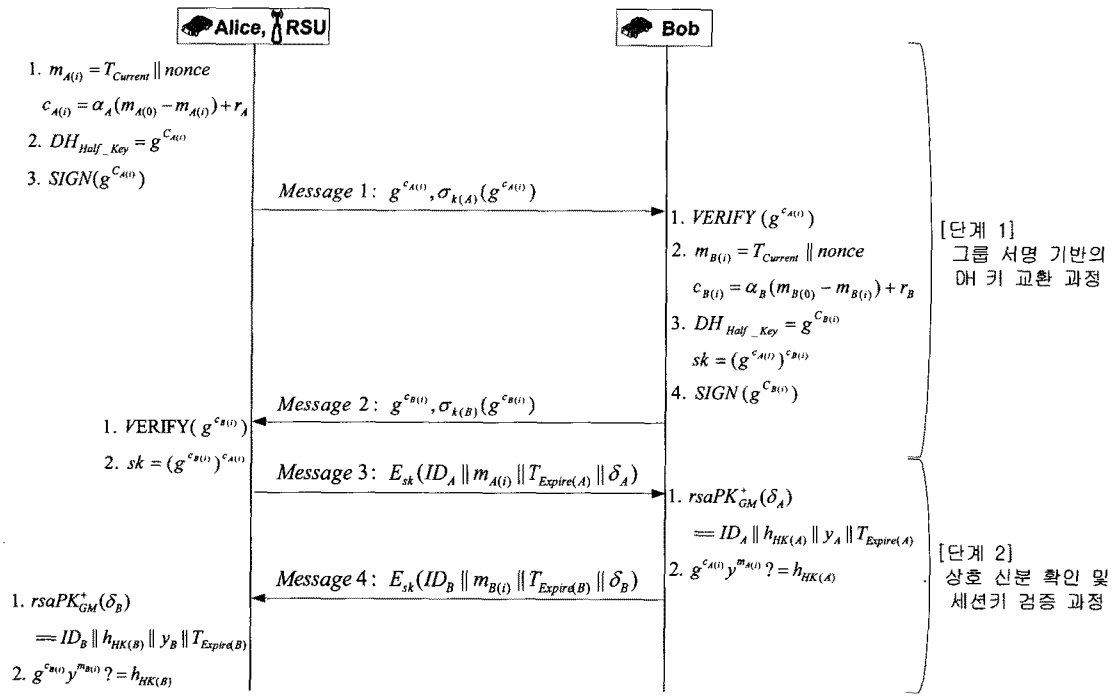
익명의 차량이 보낸 차량 안전 메시지 M으로 인하여 차량 사고 혹은 위급 상황이 발생 하였을 경우, 그룹 관리자는 차량 안전 메시지 M에 대한 $\sigma_k(M)$을 그룹 비밀키 (gsk)로 서명을 개봉하여 그룹 개인키 k 혹은 그룹 차량 ID를 확인한다.

• KEY EXCHANGE 단계

일반적으로, 상호 신분을 확인한 후에 세션키를 교환하게 되지만, 본 논문에서는 그룹 서명 기반의 차량 네트워크에서 익명성 제공을 유지하기 위해서, 세션키 교환을 먼저 수행하고 상호 신분 확인은 교환된 세션키로 신분 확인' 정보를 암호화하여 상호 확인할 수 있도록 하였다. 본 논문에서는 제안하는 그룹 서명 기반의 안전한 차량 네트워크에서 상호 신분 확인 및 세션키 교환 기능은 다음과 같이 두 단계로 진행된다. 첫 번째 단계는 두 통신자 간에 그룹 서명 기반의 DH 키 교환 과정으로 세션키를 교환한다. 두 번째 단계는 두 통신자가 생성한 세션키로 상호 신분 확인을 위한 ID 값과 인증값 δ을 암호화하여 교환한다. 〔그림 2〕는 제안하는 그룹 서명 기반의 안전한 차량 네트워크에서 인증된 세션키 교환 프로토콜의 메시지 흐름을 보여준다.

· 단계 1 (그룹 서명 기반의 DH 키 교환 과정)

그룹 서명 기반의 세션키를 교환하기 위해서 차량 Alice는 본인의 트랩도어 키 α_A를 이용하여 현재시간이 포함된 트랩도어 메시지 $m_{A(i)}$에 대한 트랩도어 해쉬 충돌값 $c_{A(i)}$을 식 (4)와 같이 생성한다. 또한, 생성된 트랩도어 해쉬 충돌값 $c_{A(i)}$을 사용하여, DH



〔그림 2〕 그룹 서명 기반의 안전한 차량 네트워크에서 인증된 세션키 교환 프로토콜의 메시지 흐름

공개키 $g^{c_{A(i)}}$으로 생성하고 비밀통신을 요청하는 메시지로써 그룹 서명값 $\sigma_{k(A)}(g^{c_{A(i)}})$을 생성하여 차량 Bob에게 〔그림 2〕와 같이 전송한다. 여기서, 생성된 DH 공개키 $g^{c_{A(i)}}$은 매번 비밀통신 요청시 만들어지는 트랩도어 메시지 $m_{A(i)}$에 따라 새롭게 생성되는 트랩도어 충돌값으로 만들어진다. 메시지를 전달받은 차량 Bob은 그룹 서명 VERIFY 단계를 통하여 DH 공개키 $g^{c_{A(i)}}$가 포함된 그룹 서명값 $\sigma_{k(A)}(g^{c_{A(i)}})$을 검증한다. 만약, 두 값에 대한 검증이 성공적으로 이루어지면, 차량 Bob은 트랩도어 키 α_B를 이용하여 트랩도어 메시지 $m_{B(i)}$과 트랩도어 해쉬 충돌값 $c_{B(i)}$을 생성하고, 값 $c_{B(i)}$을 사용하여 DH 공개키 값 $g^{c_{B(i)}}$을 계산하고, 두 차량 간에 세션키 $sk = (g^{c_{A(i)}})^{c_{B(i)}}$를 생성한다.

$$\begin{matrix} m_{A(i)} = T_{current} \| nonce \\ c_{A(i)} = \alpha_A(m_{A(0)} - m_{A(i)}) + r_A \end{matrix} \quad (4)$$

차량 Alice가 Bob으로부터 〔그림 2〕와 같이 비밀통신 수락 메시지가 포함된 메시지들을 수신하면, 차량 Alice도 Bob의 DH 공개키 $g^{c_{B(i)}}$을 그룹 서명 VERIFY 단계를 통해 그룹 서명값 $\sigma_{k(B)}(g^{c_{B(i)}})$을 검증한다. 만약, 두 값에 대한 인증이 성공적으로 수행되면, 차량 Alice는 Bob과 동일한 세션키 sk를 생성한다. 이후 차량 Bob과의 통신은 세션키 sk를 사용하여 메시지를 암호화하여 전송한다.

· 단계 2 (상호 신분 확인 및 세션키 검증 과정)

차량 Alice는 교환된 세션키를 인증하고 차량 Bob에 대한 신분을 확인하기 위하여 본인의 ID_A, 현재시간이 포함된 트랩도어 메시지 $m_{A(i)}$ 그리고 그룹 관리자가 서명한 인증값 δ_A와 인증값의 유효기간 $T_{Expire(A)}$를 세션키 sk로 암호화 하여 차량 Bob에게 전송한다. 암호화 된 메시지를 수신한 차량 Bob은 미리 생성하였던 세션키 sk를 사용하여 암호문을 해독하고, 그룹 관리자가 서명한 인증값 δ_A과 상대 차량의 ID_A를 확인한다. 상대 차량을 확인하기 위해서 수신 받은 인증값 δ_A을 그룹 관리자의 RSA 공개키를 사용하여 해독하고, 상대 차량의 ID_A와 인증값의 유효시간 $T_{Expire(A)}$를 확인할 수 있다. 또한, 세션키 sk를 인증하기 위해서, 상대 차량에게 받은 DH 공개키 $g^{c_{A(i)}}$과 트랩도어 메시지 $m_{A(i)}$, 그리고 그

룹 관리자가 서명한 인증값 δ_A에서 얻은 트랩도어 해쉬키 g^{α_A}를 식 (5)와 같이 트랩도어 해쉬값을 생성하고 그룹 관리자가 서명한 인증값 δ_A에서 얻은 트랩도어 해쉬값 $h_{HK(A)}(r_A, m_{A(0)})$와 동일한지 확인함으로써 세션키 sk를 인증한다.

$$g^{c_{A(i)}} y^{m_{A(i)}} ? = h_{HK(A)}(r_A, m_{A(0)}) \quad (5)$$

비밀 통신을 요청한 상대차량을 확인 및 세션키에 대해 인증을 성공적으로 수행한 후, 비밀 통신을 요청한 상대차량과 비밀통신에 대한 유지 및 수락을 하기 위하여 차량 Bob은 세션키 sk로 암호화 된 메시지 $\{E_{sk}(ID_B \| m_{B(i)} \| T_{Expire(B)} \| \delta_B)\}$를 차량 Alice에게 전송한다. 마지막으로, 차량 Alice는 인증값 δ_B로 상대 차량의 신분을 확인하고, 트랩도어 해쉬값을 생성하여 세션키 sk를 인증함으로써, 그룹 서명 기반의 안전한 차량 네트워크에서 다양한 응용 서비스 지원을 위한 상호 신분 확인 및 세션키 생성 과정을 완료한다.

IV. 분 석

4.1 안전성 분석

제안 기법은 그룹 서명 기반에 상호 신분 확인 및 세션키 교환 기능을 추가한 기법이기 때문에 인증, 조건부 프라이버시 및 부인방지 기능은 그룹 서명 기법의 안전성에 의존한다. 본 장에서는 제안하는 상호 신분 확인 및 세션키 교환 기법에 대해서 다음과 같이 안전성 분석을 한다.

· ID 스캐닝 공격 (ID Scanning Attack)

제안 프로토콜은 프라이버시를 제공하는 그룹 서명 기반의 세션키 교환 과정 (단계 1)과 상호 신분 확인 및 세션키 검증 과정 (단계 2)으로 구성되어 있고 총 4번의 메시지를 교환한다. 2번의 메시지를 교환하는 단계 1은 트랩도어 해쉬 함수로 생성한 DH 공개키를 그룹 서명 기법으로 확인함으로써 그룹에 가입된 정당한 차량임을 확인하고 세션키 sk를 설립하는 단계이다. 이 단계를 통해 그룹에 가입된 정당한 차량은 익명성을 유지할 수 있다. 다음 2번의 메시지를 교환하는 단계 2는 상호 신분 확인 및 세션키 검증을 수행하는 과정으로 상대 차량의 신분을 확인하고 단계 1에서 생성된 DH 세션키 교환에 사용된 DH 공개키를 인증하는 단계이다. 만약, 메시지 교환 횟수를 3번으로 줄이기 위해 Alice가 보낸 첫 번째 메시지에 대해 Bob이 두 번째 메시지로 응답할 때 Bob의 신분을 노출한다면, 공격자는 자신의 신분을 노출시키지 않고 상대방의 신분만 확인할 수 있는 공격이 가능하다. 따라서 본 논문에서는 위와 같은 공격을 차단하기 위해 신분 확인을 원하는 차량이 먼저 자신의 신분을 알려주는 방식을 취해 총 4번의 메시지를 교환하도록 하였다.

다음으로, Bob이 그룹 내의 다른 사용자 Carol로 위장하여 메시지 3에서 수신한 ID_A와 δ_A를 통해 Alice의 신분을 확인할 수 있는 공격을 가정할 수 있다. 그러나 Bob이 Carol의 정당한 $m_{c(i)}$를 생성할 수 없기 때문에 메시지 4를 수신한 Alice는 Carol의 신분 확인 과정에서 $h_{HK(c)}$ 검증을 실패하게 된다. 즉, Alice는 Carol로 위장한 Bob과의 비밀 통신을 종료하게 된다. 또한, Bob이 Alice의 ID_A와 δ_A를 알고 있다고 하더라도, Bob은 Alice의 이후 통신에서 사용되는 파라미터들이 매번 변경되기 때문에 Alice를 추적할 수 없다. 제안 프로토콜에서 공개된 파라미터들인 DH 공개값 $g^{c_{A(i)}}$과 서명값 $\sigma_{k(A)}(g^{c_{A(i)}})$은 매 세션 i 때마다 변경되는 값이므로 이전에 통신한 경험이 있거나 공개된 파라미터들을 알고 있다고 해도 상대 차량을 추적하기 어렵다.

· 위장 공격 (Impersonation Attack)

공격자는 임의의 비밀 통신을 요청하는 메시지 $\{g^{c_{A(i)'}}, \sigma_{k(A)}(g^{c_{A(i)'}})\}$를 생성하여 차량 Alice로 위장하고, Bob과 세션키 $(g^{c_{B(i)}})^{c_{A(i)'}}$교환을 시도할 수 있다. 하지만, 공격자는 제안 기법의 상호 신분 및 세션키 인증 확인을 위한 차량 Alice의 유효한 파라미터 $m_{A(i)}$를 생성 할 수 없기 때문에 Bob이 공격자를 인증하는 과정에서 실패한다. 즉, 공격자는 차량 Alice의 트랩도어 초기 파라미터 $\{m_{A(0)}, r_A\}$와 트랩도어 키 α_A를 모르기 때문에 유효한 파라미터 $m_{A(i)}$를 생성 할 수 없다. 따라서 제안 기법은 위장 공격으로부터 안전하다.

· 중간자 공격 (Man-In-The-Middle Attack)

공격자가 차량 Alice와 Bob 사이에서 DH 키 교환의 문제점인 중간자 공격을 시도할 수 있다. 공격자는 차량 Alice가 키 교환 요청 메시지의 DH 공개값 $g^{c_{A(i)}}$을 저장하고 $g^{c_{A(i)'}}$를 생성하여 차량 Bob에게 전송하고, 차량 Bob의 키 교환 응답 메시지의 DH 공개값 역시 저장 및 생성하여 차량 Alice에게 전송함으

로써 각 차량들과 비밀 통신 세션을 $\{(g^{c_{A(i)}})^{c_{B(i)'}}, (g^{c_{B(i)}})^{c_{A(i)'}}\}$ 생성할 수 있다. 그러나 제안 기법은 차량들 사이에서 키 교환되는 DH 공개값이 δ값에 의해서 인증되기 때문에 공격자는 중간자 공격을 수행할 수 없다.

· PFS/PBS (Perfect Forward Secrecy/Perfect Backward Secrecy)

차량 Alice는 본인의 트랩도어 키 α_A를 이용하여 현재시간이 포함된 트랩도어 메시지 $m_{A(i)}$로부터 트랩도어 해쉬 충돌값 $c_{A(i)}$을 생성하고, 이를 DH 공개키 $g^{c_{A(i)}}$로 사용한다. 여기서, 일회성 랜덤값 $nonce$를 포함한 트랩도어 메시지 $m_{A(i)}$와 트랩도어 비밀값인 트랩도어 키 α_A로 해쉬 충돌값 $c_{A(i)}$ 생성한다. 매번 생성된 해쉬 충돌값 $c_{A(i)}$을 DH 비밀키로 사용하기 때문에 임의의 새로운 세션키를 생성한다. 따라서 제안 기법은 생성된 세션키에 대한 완전한 전방향 및 역방향 비밀성이 보장된다. 즉 DH 세션키의 안전성은 트랩도어 비밀값인 트랩도어 키 α_A의 안전성에 기반을 두므로, 트랩도어 키 α_A가 노출 되지 않는한 완전한 전방향 및 역방향 비밀성은 제공된다.

· 도청 공격 (Eavesdropping Attack)

공격자는 무선으로 전송되는 키 교환 메시지를 도청하고, 차량들 사이에서 세션키를 계산하여 사용자의 비밀 통신 내용을 알아내려고 시도할 수 있다. 하지만, 제안 기법은 차량들이 안전하게 비밀 정보를 공유하기 위해 상호 신분 확인 및 인증된 세션키를 교환한다. 이 과정에서 교환된 세션키는 DH 파라미터 g^{c_i}에서 c_i를 알 수 없다는 DLP (Discrete Logarithm Problem) 성질을 가진다. 따라서 공격자는 도청 공격을 통해 획득한 두 차량들 사이의 키 교환 메시지로 DH 세션키를 생성할 수 없고, 세션키로 암호화된 두 사용자의 데이터를 알아낼 수 없다.

· 재전송 공격 (Replay Attack)

공격자는 차량 Alice가 Bob에게 비밀 통신을 요청하는 메시지 $\{g^{c_{A(i)}}, \sigma_{k(A)}(g^{c_{A(i)}})\}$를 재사용하여 차량 Bob과 키 교환을 시도하는 재전송 공격을 시도할 수 있다. 그러나 공격자는 재사용한 Alice의 DH 공개값 $g^{c_{A(i)}}$에서 $c_{A(i)}$를 알 수 없다는 DLP 성질에 의해, Bob으로부터 DH 공개값 $g^{c_{B(i+1)}}$를 수신 받았을 때 정상적인 세션키를 생성할 수 없다. 또한 Bob은 세션이 설립된 후에 δ_A를 확인하는 과정에서 트랩도어 메시지 m_i에 포함된 현재 시간 필드 $T_{Current}$를 체크함으로써 재전송 공격을 차단할 수도 있다.

4.2 그룹 서명 기법이 적용된 차량 보안 기술들 기능 비교

차량 통신에 적용된 그룹 서명 기법들과 제안 프로토콜을 비교하여 [표 2]에 정리하였다. 기존의 차량 통신에 적용된 그룹 서명들은 인증, 조건부 프라이버시, 부인방지 측면만을 강조한다. 즉, 각 기법들은 그룹 서명 기법 기반의 통신 환경을 제안하였기 때문에 인증 및 부인방지, 조건부 프라이버시 기능을 동일하게 제공한다. Sun과 Lin 등이 제안하는 ID 기반의 그룹 서명 기법은 그룹 관리자가 서명한 ID 기반 시스템을 이용하여 세션키를 교환할 수 있다. 하지만, 제 3의 기관이 가입자들의 동의 없이 키를 복원 할 수

[표 2] 차량 통신에 적용된 그룹 서명 기법들 기능 비교

	Guo 등 [8]	Zhang 등 [9]	Chaurasia 등 [10]	Sun, Lin 등 [11-12]	Hao 등 [13]	제안 기법
인증	O	O	O	O	O	O
조건부 프라이버시	O	O	O	O	O	O
부인방지	O	O	O	O	O	O
신분 확인 및 세션키 교환	×	×	×	O (key escrow 문제)	O (PKI 구축 문제)	O
그룹키 폐기/갱신 과정	×	O	×	×	×	×

(O : 제공, × : 제공안됨)

있다는 key escrow 문제가 있다. 즉, ID 기반 시스템을 기반으로 하는 Sun과 Lin 등의 제안 기법들은 근본적으로 KGC (Key Generation Center)에서 사용자의 개인키를 생성하기 때문에 KGC에 의해 사용자들의 개인키가 오남용 되어 암호화된 데이터가 복구되는 등의 사용자 프라이버시 문제가 발생할 수 있다. 반면, 제안 기법은 사용자가 DH 비밀키를 생성하여 세션키 교환하고 인증하기 때문에 Sun과 Lin의 기법보다 사용자 프라이버시 문제에 안전하다. 또한 Hao 등이 제안한 PKI가 적용된 그룹 서명 기법은 PKI를 사용하여 키 교환을 할 수 있지만, PKI 구축 문제와 함께 차량들 간에 상호 신분 확인 과정에서 매번 제 3의 서버로부터 인증서 검증 과정이 요구된다. 그러나 제안 기법은 하나의 인증값 g로 매번 새로운 인증된 DH 파라미터 값 g^{a}을 차량 스스로 생성할 수 있기 때문에 제 3의 노드와 통신해야 하는 부담이 없다. 즉, 제안 기법은 인증값에 대한 저장 혹은 생성 요청에 의한 오버헤드를 줄이고, 인증 유효성을 제공하는 키 교환 단계를 수행함으로써 보다 안전한 키 교환 기능을 제공한다. 또한 Zhang 등의 기법만이 그룹 서명 기법에서 그룹키 폐기/갱신 과정을 제공하고 있지만, 이는 5 단계를 갖는 일반적인 그룹 서명 기법에 유연하게 적용할 수 있다.

V. 결 론

다양한 차량 네트워크 환경에서는 인증, 조건부 프라이버시, 부인방지, 기밀성 및 무결성 등과 같은 보안 서비스들이 제공되어야 한다. 그러나 최근 그룹 서명 기반의 차량 네트워크 보안 기술들은 인증, 조건부 프라이버시, 부인방지 기능만을 제공하고, 차량들 사이에서 비밀 통신을 위한 상호 신분 확인 및 세션키 교환 과정을 고려하고 있지 않다. 본 논문에서는 차량 안전 메시지에 대한 보안 요구사항을 만족시키면서 비밀 통신이 요구되는 차량 응용 서비스를 위해서 그룹 서명 기반의 상호 신분 확인 및 세션키 교환 기법을 제안하였다. 제안 프로토콜은 트랩도어 해쉬 함수를 사용하여 하나의 인증값으로 매번 다르게 DH 파라미터들을 생성하고, 생성된 DH 파라미터들의 인증 유효성을 제공한다. 제안 기법은 하나의 인증값으로 매번 새로운 인증 세션키 교환을 수행하기 때문에, 인증값 저장 공간 및 새로운 인증값 생성 요청에 대한 통신 오버헤드를 적다. 또한 매번 새로운 DH 파라미터 생성으로 보다 안전한 세션키 교환이 가능하다. 본 논문에서는 그룹 서명 기법 기반의 차량 네트워크 보안 기술에 상호 신분 확인 및 세션키 교환 기법을 제안함으로써, 다양한 차량 네트워크 응용 서비스에서 요구하는 보안 요구사항들을 만족한다.

참 고 문 헌

[1] M.E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security Issues in a Future Vehicular Network," Proceedings of European Wireless 2002, pp. 270-274, Feb. 2002.

[2] M. Raya and J.P. Hubaux, "The Security of Vehicular Ad Hoc Networks," Proceedings of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks, pp. 11-21, Nov. 2005.

[3] M. Raya, P. Papadimitratos, and J.P. Hubaux, "Securing Vehicular Communications," IEEE Wireless Communications, vol. 13, no. 5, pp. 8-15, Oct. 2006.

[4] K. Plößl, T. Nowey, and C. Mletzko, "Towards a Security Architecture for Vehicular Ad Hoc Networks," Proceedings of the First International Conference on Availability, Reliability and Security, pp. 374-381, Apr. 2006.

[5] S. Eichler, "A Security Architecture Concept for Vehicular Network Nodes," Proceedings of 6th International Conference on Information, and Communications & Signal Processing, pp. 1-5, Dec. 2007.

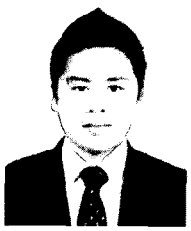
[6] D. Chaum and E. van Heyst, "Group Signatures," EUROCRYPT'91, LNCS 547, pp. 257-265, 1991.

[7] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," CRYPTO 2004, LNCS 3152, pp. 41-55, 2004.

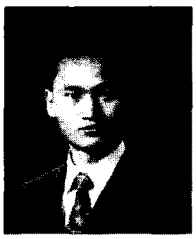
[8] J. Guo, J.P. Baugh, and S. Wang, "A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework," Proceedings of 2007 Mobile Networking for Vehicular Environments,

pp. 103-108, May 2007.
[9] J. Zhang, L. Ma, W. Su, and Y. Wang, "Privacy-Preserving Authentication Based on Short Group Signature in Vehicular Networks," Proceedings of the First International Symposium on Data, Privacy, and E-Commerce, pp. 138-142, Nov. 2007.
[10] B.K. Chaurasia, S. Verma, and S.M. Bhasker, "Message broadcast in VANETs using Group Signature," Proceedings of Fourth International Conference on Wireless Communication and Sensor Networks, pp. 131-136, Dec. 2008.
[11] X. Sun, X. Lin, and P.H. Ho, "Secure Vehicular Communications Based on Group Signature and ID-based Signature Scheme," Proceedings of IEEE International Conference on Communications, pp. 1539-1545, June 2007.
[12] 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, Dec. 2007.
[13] Y. Hao, Y. Cheng, and K. Ren, "Distributed Key Management with Protection Against RSU Compromise in Group Signature Based VANETs," Proceedings of IEEE Global Telecommunications Conference, pp. 1-5, Dec. 2008.
[14] H. Krawczyk and T. Rabin, "Chameleon Signatures," Proceedings of Network and Distributed System Security Symposium, pp. 143-154, Feb. 2000.

〈著者紹介〉



김 대 훈 (Daihoon Kim) 정회원
2008년 2월: 숭실대학교 정보통신전자공학부 학사
2008년 3월~현재: 숭실대학교 전자공학과 석사과정
〈관심분야〉 차량 네트워크 보안



최 재 덕 (Jaeduck Choi) 정회원
2002년 2월: 숭실대학교 정보통신전자공학부 학사
2004년 2월: 숭실대학교 정보통신공학과 석사
2004년 1월~12월: (주)애드팍테크놀러지 S/W 연구원
2009년 2월: 숭실대학교 전자공학과 박사
2009년 3월~현재: 숭실대학교 전자공학과 박사후 연구원
〈관심분야〉 이동 네트워크 보안, VoIP 보안, 차량 네트워크 보안

정 수 환 (Souhwan Jung) 종신회원
1985년 2월: 서울대학교 전자공학과 학사
1987년 2월: 서울대학교 전자공학과 석사
1988년~1991년: 한국통신 전임 연구원
1996년 6월: University of Washington 박사
1996년~1997년: Stellar One S/W Engineer
1997년~현재: 숭실대학교 정보통신전자공학부 부교수
2009년 3월~현재: 지식경제부 지식정보보안 PD
〈관심분야〉 이동 네트워크 보안, VoIP 보안, 차량 네트워크 보안, RFID/USN 보안