情報保護學會論文誌
第18卷 第5號, 2008. 10

VANET 환경에서 프라이버시를 보호하면서 사고 발생 시 추적 가능한 인증 프로토콜*

김 성 훈†, 김 범 한, 이 동 훈
고려대학교 정보경영공학전문대학원

A Design of Traceable and Privacy-Preserving Authentication in Vehicular Networks

Sung Hoon Kim†, Bum Han Kim, Dong Hoon Lee
Graduate School of Information Management and Security

요 약

차량 네트워크(Vehicular Networks)환경에서 차량이 주행할 때 네트워크 기반 구조와 안전하게 통신을 하기 위해서는 상호간의 신원을 확인할 수 있어야 하며, 차량과 네트워크 기반 구조와의 통신 메시지로부터 차량의 위치와 아이디가 노출되지 않아야 한다. 반면 사고가 발생했을 경우 수사기관에서는 사고의 근원을 추적할 수 있어야 한다. 또한 차량 운행 시 차량은 하나의 RSU(Road Side Unit)와 통신하는 것이 아니라 여러 개의 RSU와 통신해야 하므로 위의 성질을 만족시키면서 차량과 RSU 사이의 통신 횟수와 연산량을 줄이는 것 또한 중요한 문제이다. 본 논문에서는 차량 네트워크 환경에서 차량과 RSU 간 상호인증 프로토콜을 수행할 때 익명아이디(pseudonym)와 MAC 체인(Massage Authentication Code chain)을 이용하여 차량의 프라이버시를 보호하면서 추적성을 제공할 수 있는 효율적인 상호 인증 프로토콜을 제안한다. 또한 제안하는 프로토콜에서는 익명아이디를 MAC 체인을 이용하여 일회성으로 구성하기 때문에, 익명아이디를 별도로 관리할 필요성이 없다.

ABSTRACT

In vehicular networks, vehicles should be able to authenticate each other to securely communicate with network-based infrastructure, and their locations and identifiers should not be exposed from the communication messages. however, when an accident occurs, the investigating authorities have to trace down its origin. As vehicles communicate not only with RSUs(Road Side Units) but also with other vehicles, it is important to minimize the number of communication flows among the vehicles while the communication satisfies the several security properties such as anonymity, authenticity, and traceability. In our paper, when the mutual authentication protocol is working between vehicles and RSUs, the protocol offers the traceability with privacy protection using pseudonym and MAC (Message Authentication Code) chain. And also by using MAC-chain as one-time pseudonyms, our protocol does not need a separate way to manage pseudonyms.

Keywords : Vehicle, Privacy, Authentication

I. 서 론

지능형 차량에 임베디드 컴퓨터(embedded computer), GPS (Global Positioning System), 근거리 무선장치(short-range wireless network interface) 기술을 통합하여 OBU (On-Borad-Unit) 형태로 설치가 가능하게 되면서 주행하는 차량 안에서 무선 통신을 할 수 있게 되었다[14]. 이러한 장치들을 이용하여 차량 내부에서는 다른 차량과의 통신(V2V : Vehicle-to-Vehicle)이 가능해졌으며, RSU (Road Side Unit)를 통하여 인터넷에 접속하여 인터넷에 연결된 인프라와의 통신(V2I : Vehicle-to-Infrastructure) 또한 가능해졌다. 차량 네트워크에서는 MAC 계층(Media Access Control Layer)에서의 프로토콜[4]과 물리 계층(Physical Layer)에서의 프로토콜[12]에 대한 연구에 중점을 두고 있다. 차량 네트워크 환경에서 안전한 통신에 대한 중요성은 많은 연구에서 인지하고 있지만 그에 대한 명백한 솔루션은 제안되고 있지 않다.

여러 보안 요구사항이 차량 네트워크 환경에서 충족되어야 하지만, 보안 요구사항과 프라이버시 요구사항 사이에는 반대되는 성질이 존재한다. 즉, 차량 운전자의 안전을 보장하기 위해서 아이디를 통한 인증과정이 이루어 져야 하지만 이 과정에서 아이디가 제 삼자에게 노출되었을 경우 운전자의 프라이버시가 제 삼자에게 침해될 수 있다. 그러나 인증과정이 없으면 위장공격에 대해서 안전하지 않게 된다. 따라서 이러한 문제를 해결하기 위해서는 익명성을 제공하는 인증 과정이 필요하다. 또 다른 문제로 운전자의 프라이버시를 보호하기 위해서는 특정 차량의 운행 경로를 제 삼자(수사기관 포함)가 추적할 수 없도록 해야 하며, 사고 발생 시 수사기관에서는 사고에 대한 분쟁을 해결하기 위해서 사고 발생 근원을 추적할 수 있어야한다. 앞서 설명한바와 같이 추적성(traceability)과 비연결성(unlinkability)은 상반되는 성질을 갖고 있지만 차량 네트워크에서는 이 두 성질을 동시에 만족시킬 필요성이 있다. 이러한 대립되는 성질들로 인해 차량 네트워크 환경에서 안전한 통신 시스템을 설계하는 것은 쉽지 않은 문제이다.

F. Dötzer[3]는 차량 네트워크 환경에서의 사용자의 위치 프라이버시 문제와 아이디 프라이버시 문제를 시나리오 형태의 예를 이용하여 이를 설명하였고, 익명아이디와 스마트카드(smart card)사용을 통하여 익명성을 제공할 수 있게 하는 방식을 소개하였다. J. Choi 등[2]은 추적성(traceability)을 고려한 인증 프로토콜을 제안하였다. 그러나 위의 두 방식[2,3]은 CA(central authority)를 두고 이에 대한 완전한 신뢰(fully trust)를 가정하였기 때문에 CA에 대해서는 익명성을 보장해주지 못했다. 위의 문제를 해결하기 위해서 K. Sha 등[10]과 Y. Xi 등[11]은 CA에 대한 신뢰를 가정하지 않고 CA에 대해서도 사용자의 익명성을 보장해 줄 수 있도록 프로토콜을 설계하였다. 사용자의 익명성을 보장해 주기 위해서 K. Sha 등[10]은 GID-트리(Group ID-tree)를 사용한 그룹 기반(group-based) 인증 기법을 사용하였다. 효율성을 고려하였을 때, 이 방식은 공개키 기반 인증 기법이므로 연산 오버헤드가 크며, 새로운 사용자의 가입이나 탈퇴가 발생하였을 때의 GID-트리 업데이트(update) 및 관리 또한 어려운 문제이다. Y. Xi 등[11]은 사용자 익명성을 제공하기 위해서 랜덤 키 셋(random key-set)을 사용한 인증 기법을 설계하였다. 이 방식은 랜덤 키 셋을 이용한 확률적인 인증 방식이기 때문에 RSU는 정당한 차량에 대해서 인증하지 않을 확률이 존재한다. 이를 방지하기 위해서는 랜덤 키 셋 폐지 목록 (revoked random key-set list)에 대한 관리가 필요하다. 기존 사용자가 탈퇴하는 경우나 부정한 방법으로 프로토콜에 사용된(또는 공격된) 랜덤 키가 발견 되었을 경우, 해당 랜덤 키 셋에 대한 폐지 목록(revoked list)을 모든 차량 및 RSU는 CA를 통해 주기적으로 업데이트 해야만 하며, 이 과정으로 인해 사용가능한 랜덤 키 셋이 점차 줄기 때문에 특정 시점마다 시스템 전체의 랜덤 키 셋을 새로 생성해서 분배해야하는 문제점이 발생한다. 또한 위의 두 방식[10, 11]은 사고 발생 시의 추적성과 비연결성에 대한 문제를 고려하지 않았다. 본 논문에서는 이러한 문제를 해결하기 위해서 MAC-체인을 사용하여 사용자의 프라이버시를 보호하면서 사고발생시 추적성을 제공할 수 있는 V2I 환경에서의 인증 프로토콜을 제안한다.

위에서 언급한 바와 같이, 기존연구 [2,3]에서는 CA에 대해서 익명성과 비연결성을 제공하지 못하였으며, 기존연구 [10,11]에서는 사고 발생 시 추적성을 제공하

접수일 : 2008년 3월 26일; 수정일 : 1차-2008년 5월 19일, 2차-2008년 7월 4일; 채택일 : 2008년 8월 24일

* 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-(C1090-0801-0025))

† 주저자, kimsunghoon@korea.ac.kr

지 못하였다. 본 논문에서는 이러한 성질들을 적절하게 균형을 이루게 하기 위한 방안으로 MAC-체인을 이용한다. 제안하는 프로토콜은 초기 단계(initial step)에서는 CA에 대한 익명성을 제공하지 못한다. 그러나 MAC-체인을 사용함으로써 차량이 하나의 RSU를 지나칠 때마다 익명아이디가 자동적으로 업데이트 되므로 초기 단계 이후의 단계에서는 CA에 대한 익명성과 비연결성을 제공한다.

본 논문은 다음 네 가지에 대한 공헌을 한다. 첫째, MAC-체인을 적용한 V2I 환경에서의 인증프로토콜을 소개한다. 둘째, 사용자 프라이버시와 사고발생 시 추적성에 대한 균형을 고려하여 인증 프로토콜을 제안한다. 셋째, MAC-체인으로 일회성(one-time) 익명아이디를 생성함으로써 폐지 목록(revoked list) 관리가 어렵지 않도록 하며, 마지막으로 [그림 2]와 같은 새로운 메시지 전송방식을 도입함으로써 차량과 RSU간의 통신횟수를 기존 연구 [10,11]보다 줄인다.

Ⅱ. 보안 요구사항

공격자는 인증 프로토콜을 공격하기 위해서 도청(eavesdropping), 메시지 변조(message modification), 재생 공격(replay attack), 반사 공격(reflection)과 같은 공격 방법을 이용해서 위장 공격(impersonation attack)을 시도할 것이다. 또한 차량 네트워크 환경에서는 차량의 위치 노출과 차량의 실제 아이디(real identity) 노출과 같은 프라이버시 위협이 존재한다. 이에 대해서 F. Dötzer[3]는 차량 네트워크 환경에서 발생할 수 있는 프라이버시 위협을 예를 들어 설명하였다.

V2I에서 사용자의 프라이버시를 보호하고, 사고발생 시 추적성을 제공할 수 있는 인증 프로토콜의 설계 원칙을 세우기 위해서, 위에서 언급한 위협과 기존 연구 [3,5,10,13,14,15,16,17]를 기반으로 본 절에서는 V2I에서의 보안 요구사항을 정의한다.

2.1 일반적인 보안 요구사항

- 기밀성 (Data security) : 수집된 데이터는 원래의 데이터와 일치해야한다. 거짓 데이터(faked data)와 전송 도중 변조된 데이터는 발견되어 여과되어야 한다. 무선 환경에서의 도청은 유선 환경에서보다 쉬우므로 도청을 방지하기 위해서 데이터는 암호화 되어야 한다.
- 메시지 인증과 무결성 (Message Authentication and Integrity) : 수신자는 전송된 메시지가 적법한 발신자에 의해 생성된 것인지를 확인할 수 있어야 하며, 메시지가 네트워크에서 전송되는 도중에 변조되지 않았음을 확인할 수 있어야 한다. 이 성질은 메시지에 암호학적으로 안전한 해쉬 함수값(hased value)을 첨부함으로써 제공할 수 있다. 수식을 간략하게 표현하기 위해서 제안하는 프로토콜에서는 해쉬된 값을 별도로 첨부하여 표현하지 않는다.
- 객체 인증 (Entity Authentication) : 객체인증은 프로토콜의 구성원 A가 프로토콜 구성원 B의 특정 정보(identity) 또는 증거(evidence)를 확인함으로써 B가 실제 구성원임을 확인하는 과정이다. 그러나 이는 익명성과 비연결성에 반대되는 성질이다. 또한 이 두 성질은 추적성(traceability)과 반대되는 성질이다. 본 논문에서는 이러한 문제를 고려하여 프로토콜을 설계한다.
- 실시간 처리 (Real-time response) : 차량 네트워크 환경에서 도로 상태나 모바일 서비스를 제공할 때 수집된 정보와 서비스 전달, 특히 차량의 긴급 구조 요청할 경우 수집된 정보와 서비스 전달은 실시간(real-time)으로 이루어져야한다. 정보 수집과 서비스가 전달되기 전에 네트워크 내부 객체간의 인증과정이 필요하다. 이때, 차량이 고속으로 달리는 환경에서 메시지 전달이 실시간으로 이루어져야 하므로 인증 절차는 효율적이면서 안전해야한다.
- 가용성 (Availability) : 차량 운전자는 언제, 어디서든지 인증 요청할 수 있다. 가용성은 프로토콜 설계에 있어서 중요한 이슈이며 프로토콜 성능의 평가 기준이 된다. 안전한 프로토콜은 DoS(Denial of Service)공격과 같은 서비스 방해 공격을 피할 수 있어야한다.

2.2 프라이버시 요구사항

아이디 정보, 위치정보와 같은 사용자의 프라이버시를 보호하기 위해서 V2I에서는 다음과 같은 성질을 만족 시켜야한다.

- 익명성 (Anonymity) : 어떠한 차량의 아이디 정보

도 네트워크 내부의 메시지로부터 노출되지 않아야한다. 이 성질은 아이디 노출로 부터의 사용자의 프라이버시 위협을 보호하기 위해 제공돼야하는 성질이다. 익명아이디를 사용함으로써 이 성질을 만족시킬 수 있다.

- 비연결성 (Unlinkability) : 이웃 차량이나 RSU는 특정 메시지로부터 특정 차량의 이동경로를 파악할 수 없어야 한다. 비연결성은 사용자의 위치에 대한 프라이버시를 제공하기 위한 성질이다. 익명아이디를 특정 주기마다 변경해줌으로써 이 성질을 만족시킬 수 있다.

제안하는 프로토콜에서는 익명성을 제공하기 위해서 실제아이디 (real identifier) 대신 익명아이디를 사용하고, MAC 체인을 사용하여 익명아이디를 매번 업데이트(update) 시켜줌으로써 비연결성을 제공한다. 또한 MAC 체인을 사용하기 때문에 아이디 폐지 목록(revoked list)을 별도로 관리할 필요성이 없다.

2.3 추적성 (Traceability)

평소에 사용자의 프라이버시는 수사기관에 대해서도 보호되어야만 하지만, 사고가 발생하였을 경우에는 수사기관에서 사고의 발생 근원지와 사고 차량의 아이디를 알아야할 필요성이 있다. 그러므로 다음의 성질은 만족되어야 한다. 그러나 앞에서 언급한바와 같이 추적성을 제공하면서 동시에 프라이버시를 보호하는것은 어려운 문제이다. 본 논문에서는 이를 MAC 체인을 사용하여 해결한다.

- 추적성 (Traceability) : 사고가 발생하였을 경우, 수사 기관에서는 사고 발생 근원지를 추적할 수 있어야 하며, 사고 발생 차량의 실제 아이디를 알 수 있어야한다. 안전 메시지 (safety messages) 는 EDR (Event Data Recoder [13])에 저장되고, RSU 로그 (log)는 추적에 대한 증거로 유효해야한다.

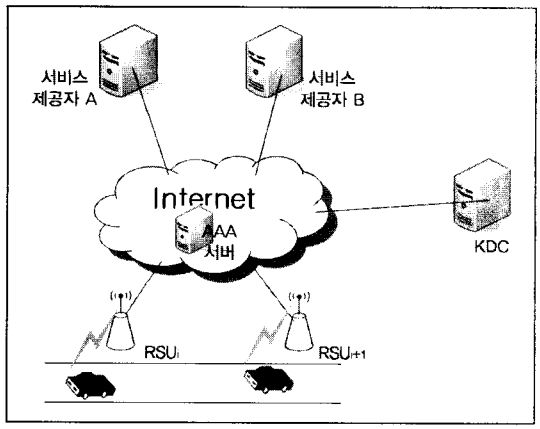
Ⅲ. 제안하는 프로토콜

3.1 표기법

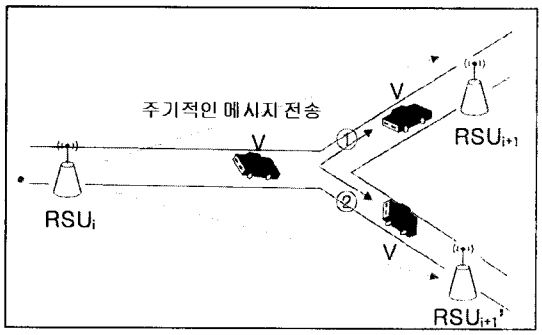
- AAA(Authentication, Authorization, Accounting) : 인증, 인가, 요금 계산 기능을 제공하는 서버이며, 신뢰기관에서 관리
- RSU_i : i번째 베이스 스테이션, 도로변에 위치해 있으며, 차량과 기반구조 간 무선통신을 위한 게이트웨이 역할을 함
- V : 차량
- ID_V : 차량 등록 시 차량 등록 기관에서 발급하는 차량의 고유한(unique) ID
- m : 메시지
- $E_K(m)$: 키를 K로 사용하는 대칭키 암호화 함수
- $D_K(m)$: 키를 K로 사용하는 대칭키 복호화 함수
- $PE_{ID_i}(m)$: 키를 ID_i의 공개키를 사용하는 공개키 암호화 함수
- $PD_{ID_i}(m)$: 키를 ID_i의 개인키를 사용하는 공개키 복호화 함수
- K_{ARi} : AAA와 RSU_i가 사전에 공유하고 있는 대칭키
- $K_{i,j}$: RSU_i와 RSU_j가 사전에 공유하고 있는 대칭키
- K_{AV} : AAA와 V가 사전에 공유하고 있는 대칭키
- KDC (Key Distribution Center) : $K_{i,j}$를 분배
- r_i : V가 생성하는 i번째 난수 값 (random value)
- t_i : i번째 타임스탬프(time stamp)
- $MAC_K(m)$: 키를 K로 사용하는 MAC (Message Authentication code) 함수
- $h(m)$: 암호학적 해쉬 함수
- K_{ENC_i} : V와 RSU_i가 상호인증을 한 후에 안전한 통신을 위해 사용될 세션 키 (session key),
  $K_{ENC_i} = h(1 \| r_i)$
- K_{MAC_i} : i+1번째 MAC 체인을 생성할 때 사용되는 MAC 함수의 키
- ps_i : ID_V를 시드(seed)로 사용하여 MAC 체인으로 생성되는 ID_V의 i번째 익명아이디이며,
  $ps_i = MAC_{K_{MAC_i}}(ps_{i-1})$
- n : V가 출발지에서 목적지까지 이동하면서 통신한 RSU_i의 개수

3.2 네트워크 구조

V2I의 네트워크 구조는 [그림 1]과 같다. 차량 네트워크는 신뢰 서버 (AAA : Authentication, Authorization



〔그림 1〕 네트워크 구조



〔그림 2〕 차량의 이동에 따른 익명 아이디 전송

and Accounting), 서비스 제공자 서버, 차량 등록 기관, *RSU* (Road Side Unit), 차량(V : Vehicle)으로 구성되어있다. 차량이 판매 되면 차량 등록기관에서는 차량에 고유한 ID(unique identifier)를 부여 하고 이를 차량 내부의 안전한 저장 공간(tamper-proof)에 저장한다. 각 차량 V와 RSU_i에는 AAA의 공개키가 들어있는 인증서가 저장되어 있다. AAA는 대칭키 K_{AV}와 K_{AR_i}를 생성하고 프로토콜을 시행하기 이전에 안전한 방법으로 K_{AV}를 V에게 K_{AR_i}를 RSU_i에게 분배한다. KDC는 대칭키 $K_{i,i+1}$를 생성하고 RSU_i와 바로 옆에 위치한 RSU_{i+1}가 $K_{i,i+1}$를 공유할 수 있도록 안전한 방법으로 분배한다. 각 RSU_i는 자신의 공개키가 포함되어있는 인증서를 주기적으로 브로드캐스팅(broadcasting)한다. 또한 각 RSU_i는 [그림 3]의 단계 5), 8)과 같은 메시지를 하나의 V에 대해서만 전송하는 것이 아니고, 여러 메시지를 모아두었다가 주기적으로 RSU_{i+1}로 전송하며, 각 RSU_i와 RSU_{i+1}은 유선 네트워크로 연결되어있다. 도로에 갈림길이 없을 경우는 위와 같으며 [그림 2]와 같이 갈림길이 발생할 경우 RSU_i의 옆에 위치하는 RSU는 RSU_{i+1}과 RSU_{i+1}' 두 개가 된다. 통신량을 고려했을 때, 위와 같은 메시지 전송 방식을 사용함으로써 기존 연구 [19,22]보다 V와 RSU_i간의 통신(무선 통신 환경) 횟수를 1회 줄일 수 있었다. 이는 다음의 프로토콜 세부에서 확인 할 수 있다.

제안하는 프로토콜에 사용하는 공개키 암호 시스템, 대칭키 암호 시스템, MAC 함수, 해쉬 함수는 암호학적으로 안전하다고 가정한다. 또한 본 논문은 RSU와 V간의 인증에 프로토콜에 중점을 두었으므로 각 RSU_i와 RSU_{i+1}간의 인증에 대해서는 설명하지 않는다. 마지막으로 각 RSU는 올바른 MAC 값을 생성해 준다고 가정한다.

3.3 프로토콜 세부

본 절에서는 추적성, 프라이버시, 효율성, 보안을 고려하여 V2I에서의 인증 프로토콜을 제안한다. 제안하는 프로토콜은 [그림 3]과 같다. 차량이 시동을 거는 시점에서 V는 차량의 시작점에 위치한 RSU_1를 통해 AAA와 상호인증을 한다. [그림 3]의 단계 1)~4)는 RSU_1, AAA, V는 각각 상호인증을 수행하는 과정이다. 이 후 V와 RSU_1은 r_0로 세션 키 K_{ENC_0}를 생성하고 이 키를 이용하여 안전하게 암호화 통신한다. 이 후 차량이 $RSU_i\ (2 \le i \le n)$ 운행되기 시작하면 [그림 3]의 단계 5)~7)과 같은 상호인증 과정을 수행한다. 이때 단계 4)와 단계 5)는 동시에 수행되는 과정이며, 설명의 편의를 위해서 단계를 구분한 것이다. 위의 상호인증 과정이 수행되면 V와 $RSU_i\ (2 \le i \le n)$는 안전한 통신을 위한 세션 키 K_{ENC_i}를 r_i로 생성한다. 제안하는 프로토콜의 세부는 아래와 같다.

0-1) V : r_0를 랜덤하게 선택,

$ps_0 = MAC_{K_{AV}}(ID_V, t_0)$ 계산,

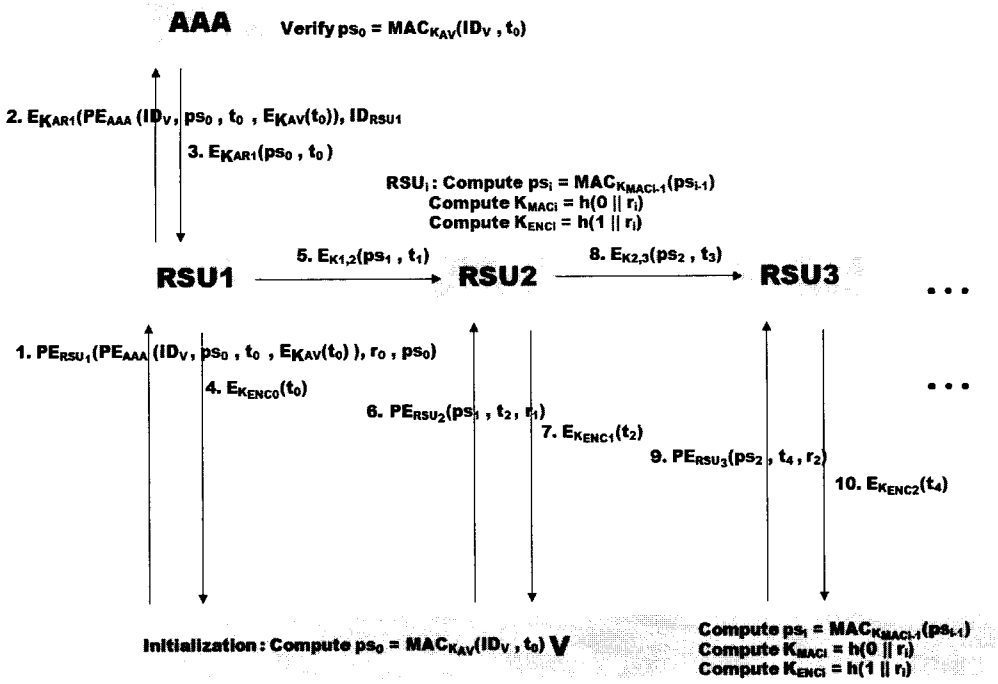
$K_{MAC_0} = h(0 \| r_0)$ 계산,

$K_{ENC_0} = h(1 \| r_0)$ 계산

1) $V \rightarrow RSU_1$:

$PE_{RSU_1}(PE_{AAA}(ID_V, ps_0, t_0, E_{K_{AV}}(t_0)), r_0, ps_0)$

1-1) RSU_1 : 단계 1)의 메시지를 개인키로 복호화 하



〔그림 3〕 제안하는 프로토콜

여 ps_0와 r_0 저장

2) $AAA \leftarrow RSU_1$:
$E_{K_{AR_1}}(PE_{AAA}(ID_V, ps_0, t_0, E_{K_{AV}}(t_0))), ID_{RSU_1}$

2-1) AAA : 단계 2)의 메시지를 대칭키 K_{AR_1}으로 복호화 하고, 이 메시지를 AAA의 개인키로 복호화,
$ps_0 = MAC_{K_{AV}}(ID_V, t_0)$ 임을 확인,
$t_0 = D_{K_{AV}}(E_{K_{AV}}(t_0))$ 임을 확인

3) $AAA \rightarrow RSU_1 : E_{K_{AR_1}}(ps_0, t_0)$

3-1) RSU_1 : 단계 1-1)에서 저장된 ps_0 와
$D_{K_{AR_1}}(E_{K_{AR_1}}(ps_0, t_0))$에서의 ps_0가 같음을 확인,
$K_{MAC_0} = h(0 \| r_0)$ 계산,
$K_{ENC_0} = h(1 \| r_0)$ 계산,
$ps_1 = MAC_{K_{MAC_0}}(ps_0)$ 계산

4) $V \leftarrow RSU_1 : E_{K_{ENC_0}}(t_0)$

4-1) $V : D_{K_{ENC_0}}(E_{K_{ENC_0}}(t_0)) = t_0$ 임을 확인,
$ps_1 = MAC_{K_{MAC_0}}(ps_0)$ 계산,
r_1을 랜덤하게 선택,
$K_{MAC_1} = h(0 \| r_1)$ 계산,
$K_{ENC_1} = h(1 \| r_1)$ 계산

5) $RSU_1 \rightarrow RSU_2 : E_{K_{1,2}}(ps_1, t_1)$

5-1) RSU_2 : 대칭키 $K_{1,2}$로 단계 5)의 메시지를 복호화 한 후 ps_1과 t_1 저장

6) $V \rightarrow RSU_2 : PE_{RSU_2}(ps_1, t_2, r_1)$

6-1) $RSU_2 : PD_{RSU_2}(PE_{RSU_2}(ps_1, t_2, r_1))$에서의 ps_1과 단계 5-1)에서 저장된 ps_1이 같음을 확인,
$K_{MAC_1} = h(0 \| r_1)$ 계산,
$K_{ENC_1} = h(1 \| r_1)$ 계산,
$ps_2 = MAC_{K_{MAC_1}}(ps_1)$ 계산

7) $V \leftarrow BS_2 : E_{K_{ENC_2}}(t_2)$

7-1) $V : D_{K_{ENC_1}}(E_{K_{ENC_1}}(t_1)) = t_1$ 임을 확인,
$ps_2 = MAC_{K_{MAC_1}}(ps_1)$ 계산,
r_2를 랜덤하게 선택,
$K_{MAC_2} = h(0 \| r_2)$ 계산,
$K_{ENC_2} = h(1 \| r_2)$ 계산

8) 이후에 V와 $RSU_i (3 \le i \le n)$는 5), 6), 7)과 같은 절차를 V가 목적지에 도착할 때 까지 반복한다.

Ⅳ. 제안하는 프로토콜 분석

4.1 인증

[정리 1] 프로토콜의 단계 1~4에서 정당한 AAA만이 V의 인증을 받을 수 있고, 정당한 V만이 AAA의 인증을 받을 수 있다.

[증명] AAA가 V를 인증하기 위해서는, V는 올바른 ps_0을 생성할 수 있어야 한다. 안전한 MAC함수를 사용한다고 가정하였으므로 K_{AV}없이는 AAA와 V를 제외한 어느 누구도 ps_0를 생성할 수 없다. 따라서 V가 정당한 차량이라면 단계 1, 2 이후에 AAA는 V를 인증한다. 정당한 AAA만이 t_0를 RSU_1에 전송할 수 있으며 단계 4가 수행됨으로서 V는 프로토콜이 정상적으로 수행되었음을 확인할 수 있으며 AAA를 인증한다.
RSU의 주 된 목표는 올바른 메시지를 전송하는데 있다. 만약 RSU_1이 공격의도를 갖고 있다면 RSU_1은 단계 2, 3 을 정상적으로 수행하지 않고 단계 4의 값을 생성하려 할 것이다. 그러나 단계 2가 시행되지 않는다면 RSU_1은 t_0값을 알 수 없으므로 단계 4의 메시지를 생성할 수 없게 된다.

[정리 2] 프로토콜의 단계 1~4에서 정당한 AAA만이 RSU_1의 인증을 받을 수 있고, 정당한 RSU_1만이 AAA의 인증을 받을 수 있다.

[증명] RSU_1을 제외한 어느 누구도 K_{AR_1} 없이는 단계 2)와 같은 메시지를 생성할 수 없다. 또한 RSU_1은 $E_{K_{AR_1}}(t_0)$를 생성할 수 없기 때문에 $PE_{AAA}(ID_1, ps_0, t_0, E_{K_{AR_1}}(t_0))$를 변조 할 수 없다. 그러므로 AAA는 K_{AR_1}으로 RSU_1을 인증한다. AAA를 제외한 어느 누구도 K_{AR_1} 없이는 단계 3)의 메시지를 생성할 수 없다. 또한 정당한 AAA만이 단계 2)에서의 메시지로부터 올바른 ps_0값을 구할 수 있다. 그러므로 RSU_1은 단계 1-1)에서 저장된 ps_0 와 단계 3-1)의 $D_{K_{AR_1}}(E_{K_{AR_1}}(ps_0, t_0))$에서 ps_0가 같음을 확인함으로써 AAA를 인증한다.

[정리 3] 프로토콜의 단계 1~4에서 정당한 V만이 RSU_1의 인증을 받을 수 있고, 정당한 RSU_1만이 V의 인증을 받을 수 있다.

[증명] 단계 3과 단계 3-1이 올바르게 수행되었다는 것은 AAA가 V를 인증했음을 뜻하므로 RSU_1은 AAA를 신뢰하고 V를 인증한다. V는 단계 4-1에서 원래의 t_0값과 단계 4의 t_0값이 같음을 확인하고 RSU_1을 인증한다.

[정리 4] 정당한 차량 V만이 $RSU_i(i \geq 2)$의 인증을 받을 수 있고, 정당한 $RSU_i(i \geq 2)$만이 V의 인증을 받을 수 있다.

[증명] 차량 V가 RSU_i에게 인증을 받기 위해서는 ID_V에 대응되는 익명아이디 ps_{i-1}을 생성할 수 있어야 한다. V가 올바른 ps_{i-1}를 생성하기 위해서는 $K_{MAC_{i-2}}$를 계산할 수 있어야 하며 $K_{MAC_{i-2}}$을 계산하기 위해서는 r_{i-2}를 소유하고 있어야 한다. r_{i-2}는 정당한 V가 생성하는 값이므로 올바른 V만이 ps_{i-1}를 생성할 수 있다. 따라서 RSU_i는 RSU_{i-1}로부터 받은 단계 5)와 같은 메시지를 $K_{i-1,i}$로 복호화 하여 얻은 ps_{i-1}와 단계 6)과 같은 메시지에서 받은 값을 자신의 개인키로 복호화 하여 얻은 ps_{i-1}이 같음을 확인함으로써 V를 인증한다. 이때 AAA는 $i \geq 2$ 일 때 ps_{i-1}을 계산할 수 없다. 왜냐하면, $ps_{i-1}(i \geq 2)$을 계산하기 위해서는 $K_{MAC_{i-1}}$을 계산할 수 있어야 한다. 그러나 AAA는 $r_{i-1}(i \geq 2)$을 계산할 수 없으므로 $K_{MAC_{i-1}}$또한 계산할 수 없다.
$RSU_i(i \geq 2)$가 V의 인증을 받기 위해서는 V의 챌린지 값 t_{2i-2}에 대응하는 $E_{K_{RSU_i}}(t_{2i-2})$을 계산할 수 있어야 하며 이를 계산하기 위해서는 r_{i-1}와 t_{2i-2}을 계산할 수 있어야 한다. 그러나 정당하지 않은 $RSU_i(i \geq 2)$는 단계 6)에서와 같은 RSU_i의 공개키로 암호화된 r_{i-1}와 t_{2i-2}을 계산할 수 없다. 그러므로 정당하지 않은 $RSU_i(i \geq 2)$는 $E_{K_{RSU_i}}(t_{2i-2})$을 계산할 수 없다.

4.2 프라이버시 보호

• 익명성

[정리 5] $i=1$일 때 AAA를 제외한 어느 누구도 ps_0에 대응하는 ID_V를 계산할 수 없고 $2 \leq i \leq n$ 일 때에는, AAA 뿐만 아니라 어느 누구도 ps_{i-1}에 대응하는 ID_V를 계산할 수 없다.

[증명] 제안하는 프로토콜에서 사용되는 MAC 함수는 암호학적으로 안전하다고 가정하였으므로 MAC 함수는 역상저항성(pre-image resistance)을 갖는다. 따라서 $ps_{i-1}(1 \le i \le n)$에 대응하는 ID_V를 누구도 계산할 수 없다. 단계 1)과 단계 2)에서 ps_0와 이에 대응되는 ID_V는 AAA의 공개키로 암호화 되어있으므로 AAA를 제외하고는 어느 누구도 ps_0에 대응하는 ID_V를 계산할 수 없다.

• 비연결성

[정리 6] $i \ge 1$ 일 때, RSU_i를 제외한 어느 누구도 (AAA 포함) ps_{i-1}에 대응하는 ps_i를 계산할 수 없으며, $2 \le j \le i$ 일 때, RSU_i와 AAA를 포함한 어느 누구도 ps_{i-j}에 대응하는 ps_i를 계산할 수 없다.

[증명] $i \ge 1$ 일 때, ps_{i-1}에 대응하는 ps_i를 계산하기 위해서는 r_{i-1}을 계산할 수 있어야 한다. r_{i-1}은 RSU_i의 공개키로 암호화 되어 있으므로 RSU_i를 제외한 어느 누구도 ps_{i-1}에 대응하는 ps_i를 계산할 수 없다. $2 \le j \le i$ 일 때, ps_{i-j}에 대응하는 ps_i를 계산하기 위해서는 $r_{i-j-1}, \ldots, r_{i-1}$ 모두를 계산할 수 있어야 하지만 앞의 각 계수는 $RSU_{i-j}, \ldots, RSU_i$의 공개키로 암호화 되어 있으므로 $RSU_{i-j}, \ldots, RSU_i$의 개인키를 모두 계산할 수 있어야만 ps_{i-j}에 대응하는 ps_i를 계산할 수 있다. 따라서 $RSU_{i-j}, \ldots, RSU_i$가 모두 공모하지 않는다면 어느 누구도 ps_{i-j}에 대응하는 ps_i를 계산할 수 없다.

4.3 사고 발생 시 추적성

사고발생시 수사기관에서 차량을 추적할 필요성이 있을 경우에는 사고 차량의 최초의 위치부터 사고 발생 위치까지 추적할 수 있어야한다. 추적성을 제공해야 하는 사고는 환경에 따라 입법기관에서 정책적으로 정의할 수 있다.

사고발생시 수사기관에서는 적법한 절차(입법기관에서 정의)에 따라 AAA에게 차량 ID_V에 대한 추적을 의뢰한다. AAA는 ID_V의 최초의 익명아이디 ps_0를 계산하고 ID_V가 최초로 통신한 BS_1을 검색한다. BS_1에서는 ps_0의 다음 익명 아이디인 ps_1을 계산한다. BS_1 다음 경로에 위치한 BS_2와 BS_2(다음 경로에 위치한 BS는 1개 이상이다.)에서는 ps_1을 검색한다. BS_2에서 ps_1이 검색됐다면 BS_2에서는 ps_1에 대응되는 ps_2를 계산한다. 이후 사고 발생지까지 이러한 과정을 반복하여 ID_V의 최초 위치인 BS_1부터 사고 발생 위치 BS_n까지 추적한다.

사고 발생 시 추적하는 방법은 위와 같이 AAA 단독적으로 수행할 수 없으며 n개의 BS_i의 협력을 받아야 수사기관에 추적성을 제공할 수 있다. 이는 AAA가 효율적으로 차량의 위치를 추적할 수 없게 함으로써 사용자의 프라이버시 보호 측면과 균형을 이루게 한다.

4.4 비교 분석

본 절에서는 V2I 환경에서의 익명 인증 기법에서의 기존 연구[10, 11]와 제안하는 프로토콜을 차량 네트워크 환경에서의 요구 사항인 프라이버시, 사고 발생 시 추적성, 효율성의 항목을 두고 비교 분석한다. 비교 분석을 위한 표기법은 [표 1]과 같고, 분석 결과는 [표 2]와 같다.

[10]과 [11]는 모든 과정에서 V에 대한 익명성을 보장하지만, 제안하는 프로토콜은 AAA에 대해서 V의 익명성을 초기단계에서 보장해주지 못한다. 그러나 이후의 과정에서는 [10], [11]과 같이 V의 익명성을 보장해주기 때문에 △로 표기한다. [10], [11]에서는 발고 발생 시의 추적성을 고려하지 않았으나 제안하는 프로토콜에서는 4.3절과 같이 추적성을 제공해준다. 제안하는 프로토콜에서는 [그림 2]와 같은 전송방식을 사용함으로써 V의 통신량을 [10], [11] 보다 1w 줄였다. 반면 RSU의 통신량은 1c 늘었다. 그러나 이는 유선으로 연결된 환경이며 매번 하는 통신이 아니라 주기적으로 여러 세션에서의 정보를 모아서 한 번에 전송하는 것이므로, 즉, 통신이 발생하지 않을 경우도 있으므로 소괄호로 표기한다. 연산량 측면에서, 제안하는 프로토콜은 [10]보다 공개키 연산량이 적으므로 [10]보다 효율적이며, [11]과는 비슷한 연산량을 갖는다. 마지막으로, 서론에서 언급한 바와 같이 [10]은 그룹기반 인증 기법을

〔표 1〕 비교 분석을 위한 표기법

표기	설 명
b	브로드캐스트(broadcast)
w	무선통신 환경에서의 유니캐스트(unicast)
c	유선통신 환경에서의 유니캐스트
p	공개키 연산
s	대칭키 연산
h	해쉬 연산

〔표 2〕 안전성과 효율성 비교

		[10]		[11]		제안하는 프로토콜	
		V	RSU	V	RSU	V	RSU
안전성	프라이버시	○		○		△	
	추적성	X		X		○	
효율성	통신량	2w	1b+1w	2w	1b+1w	1w	1b+1w+(1c)
	연산량	3p+2s	3p+2s	1p+3s	1p+3s	1p+2s+2h	1p+3s+2h
비 고		GID-트리 관리를 위한 추가적인 연산이 요구됨		랜덤 키 셋 관리의 어려움		초기(initial) 단계에서의 추가적인 통신량이 요구됨	

사용하기 때문에 GID-트리 업데이트에 대한 비용이 추가적으로 발생하며, [11]은 랜덤 키 셋을 사용하여 확률적인 인증 기법을 사용하기 때문에 랜덤 키 셋 관리(폐지목록 관리 및 주기적인 랜덤 키 셋 업데이트)를 위한 비용이 추가적으로 발생한다. 제안하는 프로토콜에서는 MAC-체인 기법을 사용함으로써 [10], [11]과 같이 추가적인 비용이 발생하지 않게 설계되었다. 제안하는 프로토콜에서는 초기 단계에서 AAA에 인증을 받아야 하는 추가적인 비용이 발생하나 이 과정은 차량이 시동을 거는 시점 혹은 최초로 네트워크에 접속하는 시점에만 발생하므로 차량이 운행되는 시점에서의 메시지 지연에 영향을 주지 않는다.

V. 결 론

본 논문에서는 차량 네트워크 환경에서의 보안과 프라이버시 문제에 관해서 다루었으며, 사고 발생 시의 추적성과 프라이버시 사이의 균형을 고려한 MAC-체인 기법을 사용하여 V2I에서 익명성, 비연결성, 추적성을 제공하는 인증 프로토콜을 제안하였다. 그러나 KDC 관리 모델과 수사기관, KDC, AAA 간의 모델이 정책적으로 다양한 형태로 구성될 수 있기 때문에 구체적인 프로토콜을 언급하지 않고 4.3절에서 분석 및 방법론을 제시하였다. 또한 차량이 빠르게 이동하는 시점에서 V의 통신량을 줄이기 위해서 새로운 메시지 전송 기법을 도입하였다. 마지막으로 제안하는 프로토콜을 분석하고 기존 연구[10, 11]와 비교함으로써 제안하는 프로토콜의 안전성과 효율성을 입증하였다.

참고문헌

[1] R. Bishop, "Survey of Intelligent Vehicle Applications Worldwide", in *Proc. of IEEE Intelligent Vehicles Symposium*, pp. 25-30, Oct. 2000.

[2] J. Choi, M. Jakobsson, S. Wetzel, "Balancing Auditability and Privacy in Vehicular Networks", In *Proc. of the 1st ACM International Workshop on QoSS in Wireless and Mobile Networks*, pp. 79-87, Oct. 2005.

[3] F. Dötzer, "Privacy Issues in Vehicular Ad Hoc Networks", in *Proc. of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks*, Sept. 2005.

[4] T. Mak, K. Laberteaux, R. Sengupta, "A Multichannel VANET Providing Concurrent Safety and Commercial Services", in *Proc. of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks*, Sept. 2005.

[5] M. Mauve, J. Widmer, H. Hartenstein, "A Survey on Position-Based Routing in Mobile Ad Hoc Networks", IEEE Network, 2001.

[6] P. Papadimitratos, V. Gligor, J-P. Hubaux, "Securing Vehicular Communications-Assumptions, Requirements, and Principles", in *Proc. of Workshop on Embedded Security in Cars (ESCAR)*, Nov. 2006.

[7] M. Raya, A. Aziz, J-P. Hubaux, "Efficient Secure Aggregation in VANETs", in *Proc. of 3rd International Workshop on Vehicular Ad Hoc Networks (VANET)*, pp. 67-75, Sep. 2006.

[8] M. Raya, J-P. Hubaux, "Securing Vehicular Ad Hoc Networks", in *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Netwroks*, pp. 39-68, vol. 15, 2007.

[9] M. Raya, P. Papadimitratos, J-P. Hubaux, "Securing Vehicular Communications", in *IEEE Wireless Communications Mag.*, vol. 13(5), pp. 8-15, Oct. 2006.

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

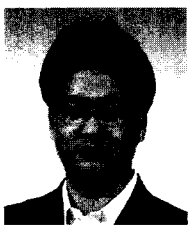
[11] Y. Xi, K. Sha, W. Shi, L. Schwiebert, "Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks", in *Autonomous Decentralized Systems, ISADS'07*, Mar. 2007.

[12] "Dedicated Short Range Communications (dsrc)", [Online]. Available : http://grouper.ieee.org/groups/scc32/dsrc/

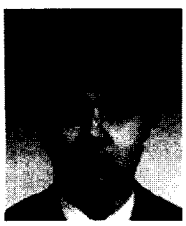
[13] "Event data recorder applications for highway and traffic safety", [Online]. Available : http://www-nrd.nhtsa.dot.gov/edr-site/

[14] "INter-Vehiclar Network Technologies (INVENT) home" [Online]. Available : http://web.njit.edu/borcea/invent/

〈著者紹介〉



김 성 훈 (Sung Hoon Kim) 학생회원
2006년 8월 : 서울시립대학교 수학과 졸업
2006년 9월~현재 : 고려대학교 정보경영공학전문대학운 석사과정
<관심분야> 암호프로토콜, 전자투표, VANET, IPTV 보안



김 범 한 (Bum Han Kim) 학생회원
2004 년 2월 : 숭실대학교 수학과 졸업
2006 년 2월 : 고려대학교 정보경영공학전문대학원 석사
2006 년 3월~현재 : 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 암호프로토콜, VANET, USIM 보안, 애드 혹 네트워크, 응용암호

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