ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

VANET 프라이버시 보장 아키텍처 설계☆

VANET Privacy Assurance Architecture Design

박 수 민[1] 홍 만 표[2] 손 태 식[2] 곽 진[2*]
Su-min Park Man-pyo Hong Tae-shik Shon Jin Kwak

요 약

VANET은 무선통신 기술을 이용하여 차량과 차량, 차량과 인프라와의 통신을 제공하는 네트워크 환경으로 자동차의 속도, 위치, 교통정보 등과 같은 데이터를 공유하여 차량 안전 주행 확보 및 교통 체증 등의 문제점을 해결할 수 있는 차세대 ITS 구현의 핵심 기술이다. 이처럼 VANET 환경을 통해 운전자의 안전성 증진과 효율성 및 이동성을 향상시킬 수 있지만, 끊임없이 차량 간 또는 차량과 인프라 간의 주고받는 데이터에는 차량 식별 정보 및 위치 정보 등의 프라이버시 정보가 포함되어 있어 프라이버시 보장을 위한 대책이 필요한 실정이다.

만약 VANET 환경에서 프라이버시 보장 방안이 제공되지 않는다면 식별 개인정보가 피해 받을 뿐만 아니라 개인의 위치 추적이 가능하여 공격자로부터 표적이 될 수 있으며, 정보의 오류 및 왜곡 등을 유발하여 생명과 재산에도 큰 피해를 안겨 줄 수 있다.

또한, 통신 환경에서의 도청을 통한 프라이버시 정보 노출 및 공격자의 악의적인 위장 공격을 통한 정보 갈취 등의 위협도 받을 수 있다. 따라서 본 논문에서는 이와 같은 위협으로부터 프라이버시를 보장하기 위해 VANET 프라이버시 보장 아키텍처를 제안한다.

☞ 주제어 : 차세대 지능형 교통 시스템, 커넥티드 카, 바넷, 프라이버시, 보안

ABSTRACT

VANET is one of the most developed technologies many people have considered a technology for the next generation. It basically utilizes the wireless technology and it can be used for measuring the speed of the vehicle, the location and even traffic control. With sharing those information, VANET can offer Cooperative ITS which can make a solution for a variety of traffic issues. In this way, safety for drivers, efficiency and mobility can be increased with VANET but data between vehicles or between vehicle and infrastructure are included with private information. Therefore alternatives are necessary to secure privacy.

If there is no alternative for privacy, it can not only cause some problems about identification information but also it allows attackers to get location tracking and makes a target. Besides, people's lives or property can be dangerous because of sending wrong information or forgery.

In addition to this, it is possible to be information stealing by attacker's impersonation or private information exposure through eavesdropping in communication environment. Therefore, in this paper we propose Privacy Assurance Architecture for VANET to ensure privacy from these threats.

☞ keyword : Cooperative Intelligent Transport Systems, Connected car, VANET, Privacy, Security

1. 서 론

전 세계적으로 도로 교통상황에서의 운전자 안전성 증진과 사고 경감을 위해 교통시스템과 ICT 융합을 통한 지능형 교통 서비스를 제공하고 있다 [1].

기존 서비스 제공 방식은 도로 기반의 지점 및 구간 중심 교통정보를 수집하여 제공하는 방식으로 사고 직전상황에 대비하는 방법이 아닌 일반적인 운전상황에서의 정보제공이나 소통관리, 사고 직후 피해경감 등의 대처가 가능했지만, 현재는 차세대 지능형 교통 시스템(C-ITS, Cooperative Intelligent Transport Systems)도입으로 차량에 장착한 단말기를 통해 차량 및 인프라와 상호 통신하여 교통정보를 공유함으로써 충돌 전에 제공받은 정보를 통해 인식 및 경고의 단계를 거쳐 사고 자체를 예방할 수 있도록 연구되고 있다 [2].

[1] Dept. of Computer Engineering, Ajou University, Gyeonggi-do, 16499, South Korea.
[2] Dept. of Cyber Security, Ajou University, Gyeonggi-do, 16499, South Korea.
* Corresponding author (security@ajou.ac.kr)
[Received 06 October 2016, Reviewed 24 October 2016, Accepted 01 November 2016]
☆ This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. NRF-2014R1A2A1A11050818). And This work was supported by the Ajou University research fund.

이처럼 차세대 지능형 교통 시스템은 차량이 주행하면서 도로 시설 및 다른 차량과 서로 통신하며 위험정보를 전파하고 공유하기 때문에 위험상황에 즉각 대응이 어려운 기존 ITS 서비스 보다 신속한 대응이 가능하다. 또한, 급정거 및 고장 등의 차량상태 뿐만 아니라 주변 사고 상황 등에 대한 정보를 서로 전파 및 공유하여 위험상황에 즉각 대응할 수 있어 획기적으로 교통사고 발생을 줄일 수 있다 [3].

이와 같이 자동차의 속도, 위치, 교통정보 등과 같은 데이터를 공유하여 차량 안전 주행 확보 및 교통 체증 등의 문제점을 해결할 수 있는 차세대 지능형 교통 시스템은 차량 간 통신인 V2V(Vehicle to Vehicle) 또는 차량과 인프라 간의 통신인 V2I(Vehicle to Infrastructure)를 제공하는 VANET (Vehicular Ad-hoc Network)을 핵심 기술로 이용한다.

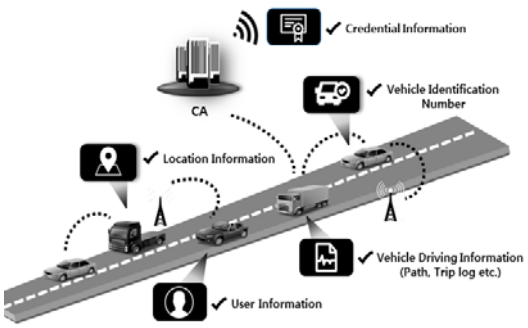
VANET은 이동하는 차량 사이에 무선 Ad-Hoc 네트워크 구축을 통해 운전자의 요구에 적합한 정보를 제공하여 이동 중에도 서비스 만족도를 향상시킬 수 있고, 차량 충돌 및 도로 교통 정체로 인한 비용을 감소시킬 수 있어 편안하고 안전한 운행을 가능하게 한다 [4]. 하지만 VANET 환경에서의 통신 데이터에는 차량의 식별 정보 및 위치 정보 등의 프라이버시가 드러나는 데이터가 포함되어 있어 프라이버시 보장을 위한 대책이 필요한 실정이다 [5].

만약 VANET 환경에서 프라이버시 보장 방안이 제공되지 않는다면 차량 및 인프라 등과 통신하는 과정에서 여러 가지 다른 기기들에 의해 데이터가 수신되어 운전자 정보, 차량 식별 정보, 운전자 운전 패턴 및 과거 경로 등의 프라이버시 정보가 노출될 가능성이 높다 [6]. 또한, 공격자가 특정 대상의 프라이버시 정보를 얻어 위장 공격을 통해 차량들과 통신하는 정보를 얻을 수 있고, 도로 위의 차량들에게 가짜 교통상황 정보, 도로의 교통사고 경고 알림 등을 전송하여 운전자들에게 혼란을 야기해 교통사고를 유발하는 등의 2차적인 위협으로도 발전할 수 있다. 따라서 이와 같이 VANET 환경에서 프라이버시 정보를 안정적으로 보호 할 수 있는 방안이 필요함에 따라 본 논문에서는 VANET 프라이버시 보장 아키텍처를 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 VANET 환경에서의 프라이버시 정보에 대해 정의 및 구분하고 프라이버시 위협사항을 분석한다. 3장에서는 VANET 프라이버시 보장을 위한 관련 연구를 소개 및 요구사항을 분석하고, 4장에서 본 논문에서 제안하는 프라이버시 보장 아키텍처를 소개한다. 이 후, 5장에서 제안하는 프라이버시 보장 아키텍처에 대해 안전성 분석을 실시한 후, 6장에서 결론으로 마무리한다.

2. VANET 프라이버시

2.1 프라이버시 정보



(그림 1) VANET에서의 프라이버시 정보
(Figure 1) Privacy Information in VANET

IT기술의 발전이 자동차 기술에 접목됨에 따라 VANET 환경에서 발생되는 데이터양이 기하급수적으로 증가하고 있다. VANET 환경에서 발생하는 데이터를 활용한 커넥티드 카(Connected Car)는 자동차와 주변 사물이 양방향 네트워크로 연결되어 다양한 서비스를 제공함으로써 운전자의 안전성과 편리성을 제공한다.

VANET 환경의 커넥티드 카 서비스는 차량, 인프라, 스마트 디바이스 등과 실시간 데이터 공유를 통해 안전하고 편안한 운전 환경을 제공하지만, 데이터 공유 과정에서 수집 및 처리되는 데이터 내에 사용자 정보, 위치 정보, 차량 식별 번호 등의 프라이버시 정보가 포함되어 있어 데이터 오남용 및 정보 유출의 위험 요소를 가지고 있다. 이러한 위험을 예방하기 위해 프라이버시 정보 구분이 요구되고, 구분된 각 정보별 관리가 필요하다.

2.1.1 식별 프라이버시

VANET 환경에서는 차량을 식별하기 위한 차량 고유 정보와 운전자의 고유 정보를 식별 프라이버시로 구분할 수 있다. 차량 고유 정보는 VIN(Vehicle Identification Number)과 같은 차량 제조업체에서 지정한 정보와 차량 번호와 같은 차량 식별 정보 등을 뜻한다.

이를 통해 차량의 등록 및 소유권, 도난방지 뿐만 아니라 보험사의 사고여부 조회, 중고차 거래 등에 유용하게 쓰인다. 이와 같은 정보가 다른 데이터 시스템과 연관된다면 차량의 소유자 및 운전자의 정보를 추정할 수 있는 데이터가 될 수 있기 때문에 세심한 관리가 요구된다.

운전자 고유 정보는 운전자의 식별 및 접근통제를 위해 사용되는 얼굴 인식, 지문, 목소리와 같은 생체정보와 새로운 서비스에 가입하기 위해 수집되는 운전자의 이름, 성별 등의 기본적인 인적사항 정보가 해당된다.

2.1.2 위치 프라이버시

일반적인 프라이버시 정보를 이름, 주소, 전화번호 등과 같이 개인을 식별할 수 있는 정보라고 한다면 VANET 환경에서는 항상 동적으로 움직이는 차량을 주체로 전달되는 데이터 내의 정보를 통해 차량을 식별 및 구분할 수 있는 특성이 있기 때문에 일반적인 개인정보의 범위에서 좀 더 나아가서 개인을 식별시킬 수 있는 모든 정보를 프라이버시라고 정의해야한다 [7].

VANET을 활용한 차세대 ITS는 교통 효율 및 안전성을 위해 위치 정보가 포함된 메시지를 지속적으로 전송한다. 이 과정에서 차량의 위치, 속도, 이동 경로, GPS 정보 등의 민감한 정보가 수시로 V2V 및 V2I 통신에서 사용됨에 따라 누구나 수신할 수 있는 가능성이 있어 위치 프라이버시에 대한 보장 방안이 필요하다.

2.1.3 데이터 프라이버시

운전자의 다양한 개인정보가 수집 및 처리됨에 따라 미국의 프라이버시 미래 포럼에서는 커넥티드 카에서의 프라이버시 보호에 관련된 보고서를 발표하였다 [8]. 보고서에서는 식별 및 위치 프라이버시 뿐만 아니라 서비스 제공을 위해 자동차에 탑재된 센서로 감지 및 수집되는 주변 환경, 장애물, 차선 표시 등의 차량 외부 개인 정보를 프라이버시 정보로 정의하였고, 운전자의 평소 행동을 데이터화한 운전자의 운전 패턴(속도, 브레이크 습관) 등의 정보도 프라이버시 정보로 정의하였다.

이와 같은 정보를 수신하거나 노변 장치로부터 전달받아 실시간 상황 정보, 교통 위험 및 사고정보, 주변 차량 긴급 브레이크 및 메시지 알림 등의 서비스를 통해 운전자는 안전하고 편안한 운행이 가능하다. 이처럼 차량에서의 다양한 서비스 제공으로 사용자의 편리성 및 안전성을 보장하고, 사용자 데이터가 서비스에 활용됨에 따라 데이터에 대한 프라이버시 보호도 고려해야 한다.

2.2 프라이버시 위협

VANET에서는 안전한 메시지 구성을 위해 차량이 주기적으로 전송하는 메시지에 식별 정보, 현재 위치, 속도 등의 정보를 포함하고 있다 [9]. 이와 같은 정보가 포함된 안전 메시지 구성은 사고를 예방하는데 도움을 줄 수 있지만, 내포된 정보가 공격자로부터 유출 및 탈취되어 악의적인 의도로 사용될 수 있다. 따라서 프라이버시가 보장되지 않는다면 식별 개인정보가 피해 받을 뿐만 아니라 개인의 위치 추적이 가능하여 공격자로부터 표적이 될 수 있으며, 정보의 오류 및 왜곡 등을 유발하여 생명과 재산에도 큰 피해를 안겨 줄 수 있다. 예를 들어 공격자는 도청과 같은 공격으로 차량의 브로드캐스트 메시지를 수신하여 차량의 현재 위치뿐만 아니라 과거 이동 경로 및 목적지 예상 경로 등을 수집 및 분석함으로써 사용자의 프라이버시가 침해될 수 있다.

이와 같이 VANET 환경에서 프라이버시에 대한 노출 및 침해 문제점이 지속적으로 생겨날 것으로 예상됨에 따라 안전한 정보 활용과 서비스 활성화를 보장하는 프라이버시 보장 방안이 요구된다.

2.2.1 도청(Eavesdropping)

공격자가 VANET 환경에서 사용자의 프라이버시 정보를 탈취하기 위해 수행할 수 있는 일반적인 방법으로 V2V 통신에서의 차량과 차량 사이의 연결이나 V2I 통신에서 차량과 인프라 사이의 연결을 도청하는 것이다. 공격자는 도청을 통해 V2V 및 V2I 통신 과정의 메시지를 수집 및 분석하여 차량의 소유자를 분석하고 차량의 출발지, 경유지 및 목적지 등의 위치 정보를 수집할 수 있다.

2.2.2 위장(Impersonation)

공격자가 특정 노드로 위장하여 노드를 대신하는 공격으로 특정 노드의 실제 ID, 식별 정보 등을 이용해 특정 노드로 둔갑한다. 특정 노드의 신분이 공격 받는다면 신분 위장에 의해 프라이버시 주체의 정보뿐만 아니라 프라이버시 주체와 관련된 노드의 정보도 위협 받을 수 있다. 또한, 인증된 개체로 위장하여 기밀 정보 접근을 획득하거나, 인증된 개체의 식별 정보로 거짓 전송을 할 수도 있다. 예를 들면 특정 차량에게 전송되는 통신 메시지를 수신할 수 있고, 특정 차량의 위치 정보 등도 획득할 수

있을 뿐만 아니라 V2V 통신 과정에서 특정 차량에게 메시지를 전송하는 발신 차량의 인증서 및 디지털 서명 등의 인증 정보도 획득할 수 있다.

2.2.3 정보 분석(Information Gathering)

V2V 또는 V2I 통신 과정에서 프라이버시 정보 데이터가 도청 및 위장 공격 등에 의해 수집되는 양이 많아지면 공격자는 데이터 분석을 통해 프라이버시를 위협 할 수 있다. 예를 들어 익명 ID 및 인증서 분배 과정에서의 메시지를 획득하여 차량의 고유 ID와 익명의 연결 관계를 획득하거나 서로 다른 익명들이 동일한 차량임을 분석할 수 있다.

3. 관련 연구

3.1 기존 연구

3.1.1 Kamat 등의 Schme

Kamat의 제안 방법은 신뢰기관으로부터 인자값을 부여받아 식별 기반 공개키 암호화 기법을 이용한 익명 ID 생성 방법을 제안하였다 [10]. 제안 방법인 익명 ID 생성을 통해 익명성을 제공하고, 신뢰기관이 안전한 보안 통신망으로 차량 인증 후 익명 ID 생성 과정을 시작함으로써 인증을 제공하고 있다.

차량은 최초에 $ID_v = (vehicle \| identifier)$와 같은 고유 차량 식별자를 갖게 된다. 신뢰기관은 $Cert_v, TS_j, ID_v^i, rsaSignK_{pub}^v(ID_I \| ID_v^i)$의 구성으로 차량 ID를 생성하고, 인프라는 차량 ID 및 비밀키에 상수값을 더하고 타임스탬프와 연접한 값을 $rsaEncryptK_{pub}^v(ID_v^{i+1} \| d_v^{i+1} \| TS_j)$와 같이 RSA 암호화 알고리즘을 통해 차량의 공개키로 암호화하여 차량에게 제공하는 방법으로 익명 ID를 발급한다.

이처럼 익명 ID 생성 기법을 통해 익명성 및 인증을 제공하지만 차량 사고 발생 등으로 인한 신뢰기관의 추적이 필요할 때의 추적성은 고려하지 않았다. 또한, 신뢰기관이 생성하여 발급한 차량 ID에는 차량의 인증서가 포함되어 있어 공격자가 차량의 ID를 알게 된다면 차량 ID와 인증서의 관계를 통해 차량의 신원정보를 파악할 수 있다. 그 뿐만 아니라 익명 ID 생성 및 전달 과정에서 인프라에 상당히 의존적인 방법 또한 취약점으로 작용해 공격자의 위장 및 도청 공격에 취약할 수 있다.

3.1.2 Lai 등의 Schme

[11]의 제안 방법은 익명키 생성을 차량, 차량 제조업체, 키 생성 센터로 구분하고 서로 정보를 공유하여 익명키를 생성함으로써 익명키를 통한 익명성 동시에 추적성을 보장할 수 있도록 제안하였다. 그리고 각 기관과 통신할 때 개인키로 서명된 메시지를 사용하여 인증을 보장한다. 차량의 운전자는 임의의 난수값 r_1, r_2를 선택하고 $E_1 = IBE_{PU_M}(LA \| r_1) \| IBE_{PU_K}(r_2)$을 생성하여 차량 제조업체에게 전송한다. 차량 제조업체는 E_1 구성에 포함되어 있는 운전자가 생성한 r_1, r_2를 이용하여 $E_2 = IBE_{PU_M}(m_1 \| t_1 \| SMAC)$ 을 생성해 키 성생센터에게 전송한다.

키 생성 센터는 SMAC의 유효성을 검증하고, 데이터베이스 내의 사용자 식별자와 익명키 쌍을 연접하여 m_2를 생성한다. 생성한 m_2를 이용해 암호문 $E_3 = IBE_{PU_M}(m_2 \| Sig_{PR_K}(m_2))$ 생성하여 차량 제조업체에게 전달한다. 차량 제조업체는 키 생성센터로부터 전달받은 정보의 유효성을 검증하고 차량에게 $E_4 = SE_{r_1}(m_3)$를 생성하여 전달한다. 차량은 수신 받은 E_4를 복호화하여 익명키 쌍을 제공받는다.

이와 같이 익명키 생성을 위한 각 단계마다 차량의 난수값 r_1, r_2를 공유하고 있어 차량 추적이 필요할 때 메시지, 정보 등을 수집 및 분석하여 추적성을 보장할 수 있다. 그리고 구분된 단계별 암호문을 통합해 익명키를 생성하여 도청 공격으로 인한 일부 정보 노출이 있어도 키를 보호할 수 있어 익명성을 보장하고 있고, 메시지 전달 시 개인키 서명을 통해 인증을 보장하고 있다.

하지만 결국 최초 차량이 생성한 난수값 r_1, r_2로 익명키를 생성하므로 메시지 수집을 통한 분석으로 차량의 신원을 파악할 수 있어 비연결성을 보장하지 못하고, 키 전달 및 업데이트를 RSU에 의존하는 모습은 위장 공격으로부터 취약함을 보인다.

3.1.3 Guo 등의 Schme

Guo의 제안 방법은 그룹서명 기법을 이용한 접근으로 그룹키와 그룹 공개키를 이용하여 메시지 서명 및 유효성 확인을 할 수 있다 [12].

그룹 매니저는 차량이 최초 가입 시, 차량의 신원 정보를 신뢰기관으로부터 인증 받아 그룹 가입을 승인하고

그룹원의 신원 정보를 저장한 후, 차량에게 그룹키를 발급한다.

메시지 발신 차량은 메시지 서명 시 그룹키를 사용하여 신원 정보가 드러나지 않기 때문에 자신의 실제 ID는 알리지 않고 수신자로부터 서명의 정당성을 그룹 공개키로 검증하게 함으로써 익명성을 보장받을 수 있다. 그러나 그룹 매니저는 gmsk(group manager secret key)를 이용해 그룹 차량들의 신원 정보를 알 수 있어 차량은 조건부 익명성을 보장 받는다고 할 수 있다.

이처럼 차량은 그룹키를 사용하여 그룹 매니저 외의 차량에게는 익명성을 보장받는 조건부 익명성을 보장받고, 그룹 매니저는 gmsk를 사용하여 추적이 필요할 때 추적성을 보장할 수 있다.

또한, 각 차량에게 다량의 그룹키를 발급하여 같은 차량으로부터 생성된 메시지의 비연결성이 보장한다.

하지만 그룹 매니저의 gmsk로 그룹원의 신원 정보를 알 수 있어 공격자의 그룹 매니저 위장 공격에 매우 큰 취약점을 갖고 있다.

3.1.4 Raya 등의 Schme

PKI 기반의 익명 인증서 방식 시스템을 제안하였다 [13]. 각 차량은 주기가 짧은 다량의 익명인증서와 본인 인증을 위한 장기간 인증서를 갖고 있다. 주기적으로 다량의 익명인증서를 발급 및 갱신 받아 사용하고, 익명성과 비연결성 보장을 위해 익명인증서는 오직 한 번 사용 후 폐기된다.

또한, 차량의 식별 정보를 포함하고 있는 장기간 인증서를 CA로부터 발급받아 인증을 보장한다.

그러나 추적성 보장을 위한 방안이 따로 고려되지 않아 사고 발생과 같은 상황에서의 특정 차량의 추적이 불가능하다.

3.2 프라이버시 보장을 위한 요구사항

3.2.1 익명성

익명 정보는 차량 인프라 환경에서 수집 및 노출되는 데이터로서 식별정보 노출로 인한 사용자의 프라이버시 위협을 보호하기 위해 기본적으로 제공되어야 하는 특성이다. VANET에서 프라이버시를 보장하기 위해서는 발신자에 대한 익명성을 보장하는 것이 중요하다.

익명 식별 정보 및 인증서를 발급한 개체가 공격자에게 공격당하더라도 익명 정보를 통해 사용자의 식별정보를 추출할 수 없어야 한다. 익명정보는 대표적으로 익명 ID 및 인증서가 있다.

3.2.2 인증

차량은 실시간으로 데이터를 수집하고 수신함에 따라 인가된 사용자와의 통신을 보장하기 위해 차량 및 인프라, 이동 단말기에 대한 인증이 필요하다. 만약 인증이 이뤄지지 않아 악의적인 공격자의 위장 공격을 받는다면, 공격당한 노드의 프라이버시 정보는 물론, 공격자로부터 공격당한 노드가 발신하는 노드의 프라이버시 또한 위협당할 수 있으므로 인증이 요구된다.

3.2.3 추적성

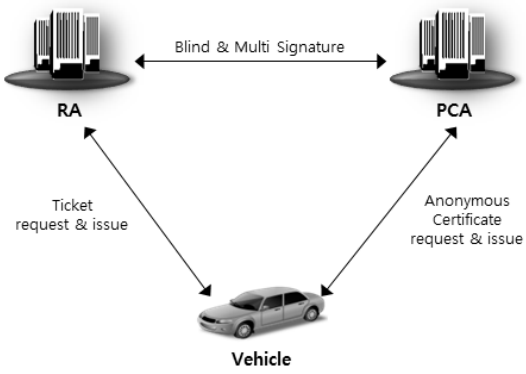
만약 도로 위에 사고가 VANET 메시지로부터 발생했다면, 경찰과 같은 신뢰기관(Trust Authority)은 메시지를 보낸 발신자를 알아야 하고 메시지 이동 경로를 추적할 수 있어야 한다.

이처럼 VANET 환경에서는 주행 안전과 관련해서 차량에 대한 유사 시 및 긴급 문제 발생 시, 신뢰 기관이 서비스 데이터와 메시지들을 수집 및 분석하여 차량을 추적할 수 있어야 한다. 하지만 추적성을 보장하기 위해 차량의 식별정보, 차량의 주행정보, 운전자의 식별정도 등을 수집하는 과정에서 프라이버시 및 개인정보 문제가 발생할 수 있다. 따라서 차량 프라이버시 정보가 보호되면서 추적성이 보장되어야 한다.

3.2.4 비연결성

V2X(Vehicle to Things) 통신으로 주고받는 메시지 및 데이터에는 위치 정보가 포함되어 있어 차량의 위치 정보가 공격자에게 쉽게 노출될 가능성이 있다. 만약 공격자가 RSU와 차량 간의 통신 데이터를 도청 공격과 같은 기법을 이용하여 탈취하더라도, 공격자가 차량 통신상의 메시지를 분석하여 차량의 식별정보 및 위치정보, 경로를 유추할 수 없도록 데이터와 차량 정보 간의 연결성이 있어서는 안 된다. 예를 들어, 전송되는 2개 또는 그 이상의 서명된 메시지를 분석하여 발신자와 관련된 정보를 얻을 수 있어서는 안 된다.

4. 프라이버시 보장 아키텍처



(그림 2) 프라이버시 보장 아키텍처
(Figure 2) Privacy Assurance Architecture

본 아키텍처에서 신뢰기관은 단일 기간이 아닌 책임을 분담하여 2개의 신뢰기관으로 구성한다.

차량의 신원을 확인 및 등록하는 역할을 수행하는 Registration Authority(RA)와 익명인증서 발급을 담당하는 Pseudonym CA(PCA)로 구성한다. 신뢰기관을 분담함에 따라 RA는 차량 사용자에 대한 실제 신원은 알고 있지만 사용자에게 발행된 인증서에 대해서는 알 수 없고, PCA는 차량 사용자에게 발행된 인증서에 대해 알고 있지만 사용자에 대한 실제 신원에 대해서는 알 수 없다.

따라서 사용자의 신원정보를 알기 위해서는 RA와 PCA가 협력해야 차량 사용자에게 발행된 인증서와 실제 신원을 연결시켜 차량 사용자에 대한 정보를 획득할 수 있다.

RA는 차량 사용자 신원 확인 및 데이터베이스 기록 및 유지, PCA에게 익명인증서 발급을 요청할 수 있는 티켓 발급을 담당하고, PCA는 차량 사용자의 인증서 요청을 확인 및 검증하여 차량 사용자에게 익명인증서를 발급하는 역할을 한다. 이 과정에서 익명인증서에 필요한 서명은 RA와 PCA의 다중서명 값으로 구성되고 RA와 PCA는 익명인증서 주체의 프라이버시를 보장하기 위해 블라인드 서명 기법을 이용한다 [14].

4.1 익명인증서 발급 프로토콜

모든 차량은 최초 생산될 때 제조업체로부터 부여받은 시리얼 번호 등의 고유 식별정보를 갖고 있다. 차량은 CA에 신원정보를 등록하고, CA는 차량의 고유 식별정보를 이용해 차량의 가명 ID를 생성하여 안전한 보안 통신망으로 차량에게 가명 ID를 전달한다. 이 때, CA는 차량 신원정보 및 고유 식별정보와 가명 ID 정보를 데이터베이스에 저장한다.

(표 1) 프로토콜 표기법
(Table 1) Protocol Notation

표기법	내용
$Cert_i$	인증서
$PseCert_i$	익명인증서
Sig_i	전자서명
$[T_s, T_e]$	인증서 유효기간
ID_i	식별자
$PseID_v$	가명 ID
$PubK_i$	공개키
request $ticket_i$	티켓 요청
PseCertificate request	익명인증서 요청
$ticket_i$	티켓
$EncPK_i$	공개키 암호화

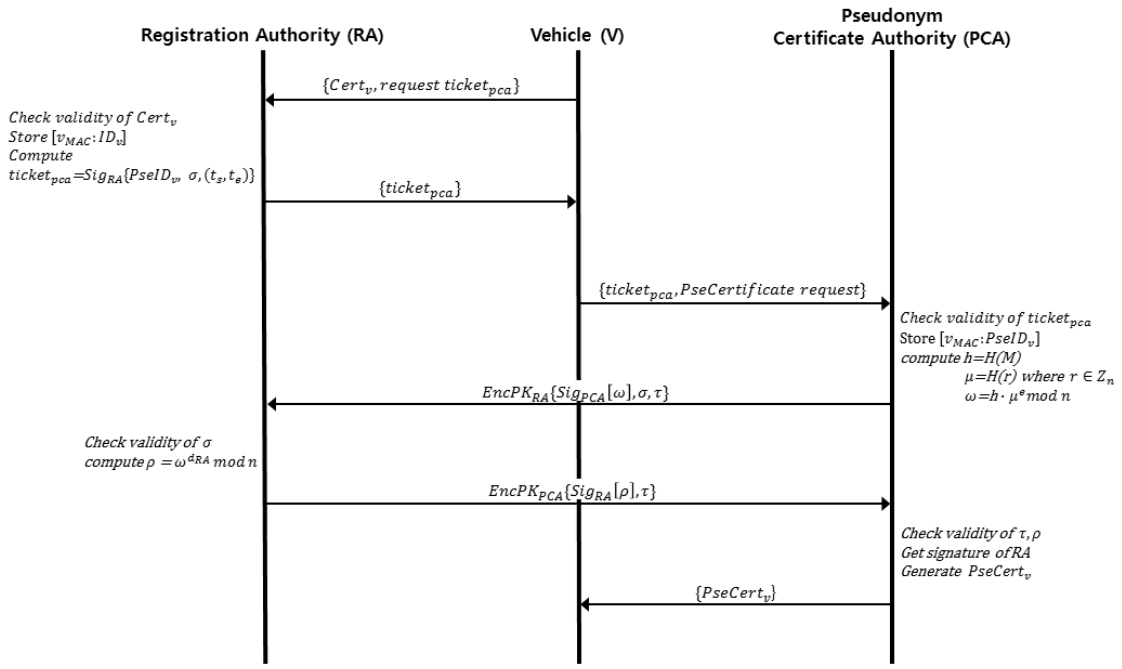
차량은 VANET 환경에서 차량의 실제 신원을 나타내는 인증서와 개인/공개키 쌍을 CA로부터 발급받아 HSM(Hardware Security Module)와 같은 차량 내부의 안전한 저장소에 저장한다. 인증서는 차량의 가명 ID, CA의 식별자, 인증서 유효기간이 CA의 서명으로 전자서명 되어 있고, 개인/공개키 쌍은 차량의 가명 ID 정보로 생성된다.

$$Cert_v = Sig_{CA}[PseID_v, ID_{CA}, (t_s, t_e)]$$

먼저 차량 사용자는 익명인증서를 발급받기 위해 RA에 토큰을 요청한다. 토큰은 RA로부터 신원을 검증 받아야 발급 받을 수 있는 것으로 토큰을 통해 PCA에게 유효한 사용자임을 인증 받는다. 차량은 RA에게 신원을 등록 및 인증 받고 PCA와의 통신을 위해 토큰을 발급받는다.

이 때, RA는 차량의 신원정보를 데이터베이스에 저장한다. PCA에 토큰을 전달하면 PCA는 토큰을 검증하고 블라인드 서명값을 RA의 공개키로 암호화하여 RA에게 전달한다.

RA는 PCA로부터 전달받은 블라인드 서명값을 자신의 개인키로 복호화하고 PCA의 공개된 값을 이용하여 블라인드 서명값을 검증한다. 검증이 유효할 경우, RA는 자신의 개인키로 전자서명하고 PCA의 공개키로 암호화하여 PCA에게 전송한다. PCA는 RA로부터 받은 블라인드 서



(그림 3) 익명인증서 발급 프로토콜
(figure 3) Pseudonym Certificate issue Protocol

명값을 자신의 개인키로 복호화하여 RA의 서명을 획득할 수 있다. 획득한 RA의 서명과 PCA의 서명을 이용하여 하나의 서명으로 생성해 차량에게 익명인증서 발급 시, 서명으로 사용한다.

• Step 1. 차량 V는 RA에게 자신의 신원을 증명하는 $Cert_v$와 익명인증서 발급 기관인 PCA에 인증받기 위한 티켓을 요청하는 $Request\ ticket_{pca}$을 전송한다.

• Step 2. RA는 차량 V로부터 수신 받은 $Cert_v$을 검증하고 검증이 유효할 경우, 기록 유지를 위해 MAC 값을 계산하여 $[v_{MAC} : ID_v]$ 형태로 데이터베이스에 저장하고, 차량 V의 익명 ID $PseID_v$와 티켓이 유효함을 뜻하는 식별자 σ, 티켓 유효기간으로 계산한 값을 전자서명한 $ticket_{pca}$를 발급하여 전송한다.

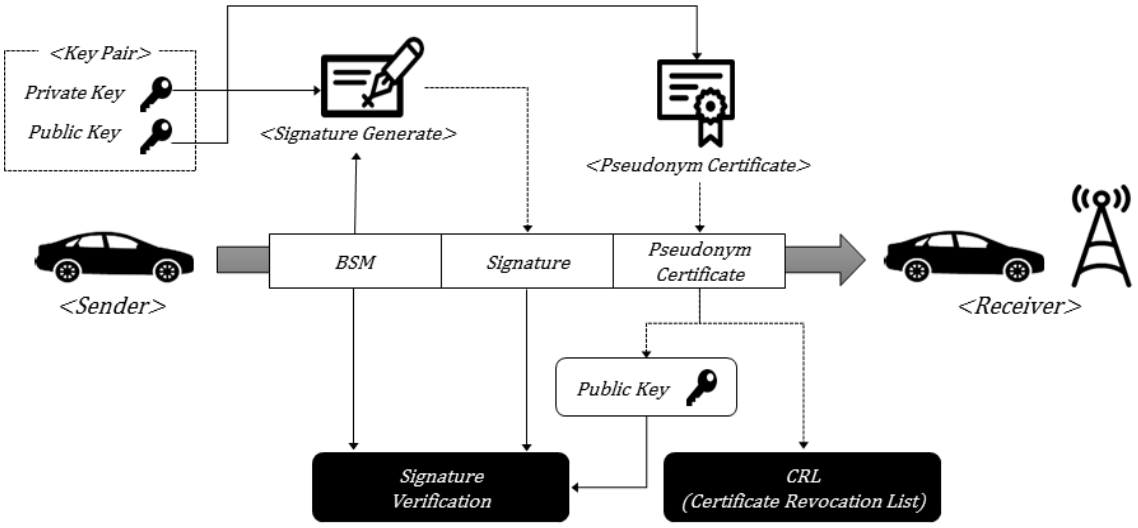
• Step 3. 차량 V는 익명인증서를 발급받기 위해 PCA에 RA로부터 발급받은 $ticket_{pca}$와 익명인증서를 요청하는 $Psecertificate\ Request$를 전송한다.

• Step 4. PCA는 차량 V로부터 수신 받은 $ticket_{pca}$를 검증하고 검증이 유효할 경우, 기록 유지를 위해 MAC 값을 계산하여 $[v_{MAC} : PseID_v]$ 형태로 데이터베이스에 저장하고, 익명인증서 서명에 필요한 RA와의 다중서명 구성을 위해 블라인드 서명값을 생성한다.

서명에 필요한 항목을 M에 구성하여 해쉬값 $h = H(M)$을 구하고, 난수 r을 $r \in Z_n$ 범위 내에서 임의로 선정하여 $\mu = H(r)$으로 구한다.

그리고 h와 μ를 이용한 블라인드 서명을 수행하여 $\omega = h \cdot \mu^e \bmod n$을 구한다. 구한 ω값을 자신의 개인키로 서명하고, RA의 공개키로 암호화하여 전송한다. 이 때, 올바른 송수신 확인을 위해 식별자 τ를 첨부한다.

• Step 5. RA는 PCA로부터 수신 받은 값을 자신의 개인키로 복호화하여 자신이 생성했던 식별자 σ의 유효성을 검증한다. σ의 검증이 유효하면 $\omega = h \cdot \mu^e \bmod n$에 자신의 개인키 (d_{RA}, n)으로 전자서명 한 후, $\rho = \omega^{d_{RA}} \bmod n$으로 계산하여 자신의 개인키로 서명하고 τ와 함께 PCA의 공개키로 암호화하여 전송한다.



(그림 4) V2X 통신 인증
(figure 4) V2X Communication Authentication

• Step 6. PCA는 RA로부터 수신 받은 값을 자신의 개인키로 복호화하여 자신이 생성했던 식별자 τ의 유효성을 검증한다. τ의 검증이 유효할 경우, RA의 블라인드 서명을 획득한다. 이 후, 획득한 RA의 서명값과 PCA가 생성한 서명값으로 익명인증서의 서명값을 구성하여 익명인증서를 차량 V에게 발급한다. 익명인증서는 차량의 가명ID, PCA의 식별자, 차량의 공개키, 인증서 유효기간이 PCA의 전자서명으로 구성되어 있다.

$$PseCert_v = Sig_{PCA}[PseID_v, ID_{PCA}, PubK_v, (t_s, t_e)]$$

4.2 V2X 통신 인증

차량 V가 통신하고자 하는 대상 차량이 근거리에 있을 경우 및 RSU의 통신범위에 접근했을 경우에 V2X 통신 인증을 실시한다. 통신 과정에서 사용되는 BSM(Basic Safety Message)은 주행하는 차량의 안전성을 높이기 위해 차량 및 RSU로부터 빈번하게 브로드캐스팅 되는 메시지를 뜻한다. 그림 4는 V2X 통신 인증 과정을 나타낸다.

4.2.1 발신 노드

발신 차량은 BSM과 차량의 전자서명, 차량의 가명인증서를 수신 차량에게 전송한다. 이 때, 차량의 전자서명은 BSM을 개인키로 암호화하여 생성되고, 익명인증서에는 개인키에 대응하는 공개키가 포함되어 있다.

4.2.2 수신 노드

발신 차량으로부터 BSM, 전자서명, 가명인증서를 전달 받은 차량 및 RSU는 가명인증서에서 차량의 공개키를 추출하여 전자서명을 검증하고 인증서에 대한 검증은 CA로부터 주기적으로 전송받는 CRL(Certificate Revocation List)로 차량 가명인증서의 유효성을 검증한다. 발신 차량의 전자서명과 익명인증서의 유효성이 검증되면 발신 차량은 유효한 차량으로 인증된다.

5. 안전성 분석

5.1 익명성

V2X 통신할 때 차량 V는 CA로부터 발급받은 익명인증서를 사용한다. 인증서에 포함된 식별정보를 익명 ID로 대체하고, 동일 차량이라도 익명인증서를 주기적으로 변경하여 V2X 통신에 사용한다.

이를 통해 인증서의 식별정보가 주기적으로 변경되는 효과가 있으며, 동일한 차량인지 확인할 수 없기 때문에 차량의 식별정보가 보호된다.

(표 2) 비교 분석
(Table 2) Comparison Analysis

요구사항 \ 논문	제안 방식	[10]	[11]	[12]	[13]
익명성	○	○	○	△	○
인증	○	○	○	○	○
추적성	○	X	○	○	X
비연결성	○	X	X	○	○

5.2 인증

V2X 통신 과정에서 상대방에게 전송하는 익명인증서에는 차량의 공개키가 포함되어 있다.

수신 차량 및 RSU는 익명인증서에 포함된 공개키를 이용해 차량의 전자서명 유효성을 검증할 수 있고, CRL로 수신 받은 익명인증서의 유효성을 검증함으로써 인증을 보장할 수 있다.

또한 익명인증서 발급 과정이 역할을 분담하여 운영함에 따라 단일기관에 의한 익명인증서 발급보다 신뢰도가 높다.

5.3 추적성

RA는 차량 사용자에 대한 실제 신원은 알고 있고, PCA는 차량 사용자에게 발행된 인증서에 대해 알고 있으므로 특정 차량의 추적이 필요할 경우 RA와 PCA의 협력하여 차량의 신원정보를 알아낼 수 있다.

추적하고자 하는 차량으로부터 얻은 익명인증서로 차량의 익명ID를 알 수 있다. 익명인증서를 발급한 PCA는 차량으로부터 익명인증서 발급 요청을 받고 검증할 때, 검증이 유효하면 익명 ID를 발급하고 익명ID와 차량의 신원정보를 매칭하여 $[v_{MAC} : PseID_v]$를 저장한다.

따라서 특정 차량의 익명인증서로부터 얻은 익명 ID의 차량 신원정보를 찾을 수 있다. 이 후에, 찾은 차량 신원정보를 차량의 신원을 검증하고 등록하는 RA와 협력한다.

RA는 차량의 신원을 검증하고 등록하는 과정에서 $[v_{MAC} : ID_v]$를 저장한다. 이를 통해 차량의 실제 신원정보를 알아낼 수 있어 PCA와 RA의 협력을 통해 차량의 추적성을 보장할 수 있다.

5.4 비연결성

제안한 아키텍처는 사용자에게 각기 다른 다량의 익명인증서를 발급하여 공격자가 인증서를 획득한 경우에도 차량의 정보를 유추할 수 없도록 비연결성을 보장한다.

익명인증서 구성에는 차량을 식별할 수 있는 직접적인 정보가 없으며, 만약 위장 및 도청 공격에 익명인증서 내에 포함되어 있는 익명ID가 이용되더라도 익명 ID는 차량의 실제 신원정보와 연결성이 없다. 그리고 차량과 익명 ID 사이의 비연결성을 보장하기 위해 차량의 가명 ID 및 인증서의 교체 주기를 짧게 하여 연결성을 최소화한다.

따라서 동일 차량이라도 익명 ID 및 익명인증서를 주기적으로 자주 변경하여 V2X 통신에 사용하므로 전달되는 인증서의 식별 정보가 랜덤하게 변경되기 때문에 공격자는 동일한 차량인지 확인할 수 없다.

6. 결 론

운전자 안전성 증진과 사고 경감을 위한 차세대 지능형 교통 시스템, 커넥티드 카 개발 등 전 세계적으로 교통안전과 관리에 대한 관심과 노력이 높아져가고 있다.

하지만 VANET 환경에서의 데이터에는 운전자 정보, 차량 식별 정보, 위치 정보, 운전자 운전 패턴 및 과거 경로 등의 프라이버시 정보가 포함되어 있어 안정적으로 보호할 수 있는 방안이 필요함에 따라 본 논문에서는 VANET 환경에서의 프라이버시 정보에 대해 구분 및 정의하고, 프라이버시를 위협하는 요소를 분석하였으며, 프라이버시를 보장하기 위한 요구사항을 정의하여 이에 충족하는 프라이버시 보장 아키텍처를 제안하였다.

제안하는 프라이버시 보장 아키텍처는 등록 기관과 익명인증서 발급기관 2개의 신뢰기관으로 역할을 분담하여 블라인드 및 다중 서명 기법을 통한 익명인증서 발급 프

로토콜과 V2X 통신 상황에서의 인증 방법으로 프라이버시 보안 위협을 해결하고, 프라이버시 보장 요구사항을 충족한다.

이를 통해 향후 차세대 지능형 교통 시스템 및 커넥티드카 개발 등에서 VANET 환경 프라이버시 관련 연구에 도움이 될 것으로 기대된다.

참 고 문 헌 (Reference)

[1] C. Campolo, A. Molinaro, R. Scopigno, “Vehicular ad hoc Networks: Standards, Solutions, and Research,” Springer, 2015. http://dx.doi.org/10.1007/978-3-319-15497-8

[2] Tubbene, Halvard, “Performance Evaluation of V2V and V2I Messages in C-ITS”, NTUN-Trondheim, 2015. https://core.ac.uk/download/pdf/30876037.pdf

[3] Yousefi, Saleh, Mahmoud Siadat Mousavi, and Mahmood Fathy, “Vehicular ad hoc networks (VANETs): challenges and perspectives,” 2006 6th International Conference on ITS Telecommunications, IEEE, 2006. http://dx.doi.org/10.1109/ITST.2006.289012

[4] H. Hartenstein, K. Laberteaux, “VANET: vehicular applications and inter-networking technologies,” Wiley Online Library, 2010. http://samples.sainsburysebooks.co.uk/9780470740620_sample_390070.pdf

[5] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, K. Sezaki, “CARAVAN: Providing location privacy for VANET,” Proceedings of Embedded Security in Cars (ESCAR), 2005. http://www2.ee.washington.edu/research/nsl/papers/ESCAR-05.pdf

[6] M. Raya, J. Hubaux, “The security of vehicular ad hoc networks,” 3rd ACM Workshop Security Ad Hoc Sensor Network, pp.11－21, Alexandria, 2005. http://dx.doi.org/10.1145/1102219.1102223

[7] H-J. Lim, T-M. Chung, “A Survey on Privacy Problems and Solutions for VANET Based on Network Model,” 11th ICA3PP, pp. 74－88, Australia, 2011. http://dx.doi.org/10.1007/978-3-642-24669-2_8

[8] J. Jerome, “The Connected Car And Privacy Navigating New Data Issues”, Future of Privacy Forum, 2014. https://fpf.org/wp-content/uploads/FPF_Data-Collection-and-the-Connected-Car_November2014.pdf

[9] R. Sumner, B. Eisenhard, J. Baker, “SAE J2735 Standard: Applying the Systems Engineering Process,” U.S Department of Transportation, 2013. http://ntl.bts.gov/lib/51000/51100/51167/DE156ECC.pdf

[10] Kamat, P., Baliga, A., Trappe, W, “An Identity Based Security Framework for VANET,” 3rd International Workshop on Vehicular Ad Hoc Networks, pp.94-95, Los Angeles, USA, 2006. http://dx.doi.org/10.1145/1161064.1161083

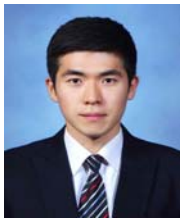
[11] Lai, C., Chang, H., Lu, C. C, “Secure Anonymous Key Mechanism for Privacy Protection in VANET,” 9th International Conference ITS Telecommunications, pp. 635－640, France, 2009. http://dx.doi.org/10.1109/ITST.2009.5399278

[12] Guo, J., Baugh, J.P., Wang, S, “A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework,“ the Mobile Networking for Vehicular Environments workshop in conjunction with IEEE INFOCOM, Alaska, 2007. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4300813

[13] Raya, M., Papadimitratos, P., Hubaux, J.-P, “Securing Vehicular Communications,” Wireless Communications, IEEE, pp.8-15, 2006. https://people.kth.se/~papadim/publications/fulltext/sevecom-early-3.pdf

[14] Chaum, David. ″Blind signature system.″ Advances in cryptology. Springer US, 1984. http://dx.doi.org/10.1007/978-1-4684-4730-9_14

◐ 저 자 소 개 ◑



박 수 민 (Su-min Park)
2012년 세명대학교 정보통신학부 졸업(학사)
2014년~현재 아주대학교 컴퓨터공학과 재학(석사)
관심분야 : IoT 보안, 자동차 보안, 암호프로토콜, 개인정보보호
E-mail : smpark.isaa@gmail.com

홍 만 표 (Man-pyo Hong)
1981년 서울대학교 계산통계학 졸업(학사)
1983년 서울대학교 계산통계학 졸업(석사)
1991년 서울대학교 전산과학 졸업(박사)
1983년~1985년 울산공과대학 전임강사
1985년~현재 아주대학교 사이버보안학과 교수
관심분야 : 악성코드 및 바이너리 분석, 핀테크 보안, 차량 네트워크 보안, 영상 프라이버시 보안
E-mail : mphong@ajou.ac.kr

손 태 식 (Tae-Shik Shon)
2000년 아주대학교 정보컴퓨터공학부 졸업(학사)
2002년 아주대학교 정보통신공학과 졸업(석사)
2005년 고려대학교 정보보호대학원 졸업(박사)
2004년~2005년 Research Scholar, University of Minnesota
2005년~2011년 삼성전자 통신/DMC 연구소 책임연구원
2011년~현재 아주대학교 사이버보안학과 교수
관심분야 : 산업제어시스템 보안, 비정상행위탐지, 디지털 포렌식
E-mail : tsshon@ajou.ac.kr

곽 진 (Jin Kwak)
2000년 성균관대학교 졸업(학사)
2003년 성균관대학교 졸업(석사)
2006년 성균관대학교 졸업(박사)
2007~2015년 순천향대학교 정보보호학과 교수
2015년~현재 아주대학교 사이버보안학과 교수
관심분야 : 암호프로토콜, 개인정보보호, 정보보호제품평가, 클라우드 보안, 자동차 보안
E-mail : security@ajou.ac.kr