정 보 보 호 학 회 지
제25권 제4호, 2015. 8

차량 통신 보안 기술 표준화 동향

이 상 우*, 이 병 길*, 나 재 훈*

요 약

오늘날 차량 교통 시스템은 지능형 교통 시스템(ITS, Information Transportation System) 으로 진화하고 있다. 특히 차량 간 통신 및 차량과 인프라 간 통신을 활용하여 차량 주행의 안전성을 높이고 교통 체계의 운영 및 관리를 과학화하고자 하는 연구가 활발히 진행 중이다. 그러나, 지능형 교통 시스템의 상용화를 위해서는 차량 통신 보안 기술의 확보가 필수적이다. 본 고에서는 차량 통신 보안 기술 표준화 동향을 살펴본다.

Ⅰ. 서 론

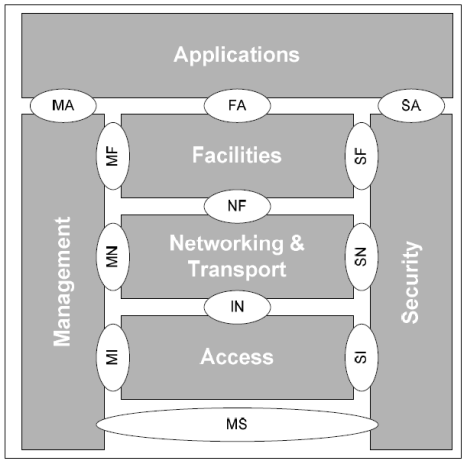
최근 들어, 자율 주행 차량의 상용화가 가시화 되고 있다. 자율 주행 차량은 차량의 주변 정보를 인식하는 레이더, 카메라 등의 센서 기술, 차량과 차량, 차량과 도로기지국 간의 통신 기술, 그리고, 주변 인식 정보와 통신 정보를 바탕으로 차량을 실시간 제어하는 기술로 구성된다. 특히, 레이더 등의 가시 거리 한계, 야간에서의 시각적 한계 상황을 보완하기 위하여 차량 간 통신 기술은 필수적인 기술이다. 그러나, 차량 간 통신 기술을 활용하기 위해서는 반드시 보안 기술의 확보가 선행되어야 한다[1]. 차량 네트워크 환경은 기존의 인터넷 등의 네트워크 환경과 달리 네트워크의 보안성 확보 여부가 운전자의 생명과 직결되는 위험 상황을 유발할 수 있기 때문이다. 이러한 상황을 반영하여, 현재 차량 통신 보안 표준화가 활발히 진행 중에 있다. 본 고에서는 차량 통신 보안 기술의 표준화 동향을 소개한다.

Ⅱ. 차량통신보안 기술 표준화 현황

차량 통신 보안 표준화는 IEEE, ETSI, ITU-T 등에서 추진 중이다. IEEE와 ETSI에서는 이미 1차 버전이 제정되어 개정이 추진 중인 상태이고, ITU-T에서는 새로이 표준화를 추진 중이다. 본 절에서는 표준화기구에 따른 표준화 활동을 살펴 본다.

2.1. ETSI ITS 통신 구조

그림 1은 ETSI의 ITS 기기의 참조 구조를 도시한 것이다. 이 구조는 일반적인 OSI 네트워크 계층 구조를 기초로 한다. Facilities 계층은 OSI 네트워크 계층 구조에서의 Session, Presentation 및 Application 계층을 의미한다. Access 계층은 OSI 구조의 Data link 및 Physical 계층을 의미한다. ITS 참조 모델에서 Applications 계층은 다른 ITS 기기와의 통신을 위한 응용 계층을 의미한다. 즉, OSI 구조에서의 Application



〔그림 1〕 ITS 참조 모델

본 연구는 미래창조과학부 및 정보통신기술연구진흥센터의 정보통신방송연구개발사업의 일환으로 수행되었음[R166-15-1018. 온라인 청소년 보호를 위한 ID검증기술 표준개발]

* 한국전자통신연구원

계층에서 차량 통신을 위하여 특별히 지정된 계층이라고 할 수 있다. Management 계층은 ITS 기기의 통신을 관리하는 계층을 의미하고, Security 계층은 방화벽, 침입 탐지, 인증 및 인가 등의 보안 서비스를 담당하는 계층을 의미한다. 각각의 계층 간은 고유의 인터페이스를 가지는데, 예를 들어, MA 인터페이스는 Management와 Application 계층 간의 인터페이스를 의미한다.

2.2. IEEE WAVE (Wireless Access in Vehicular Environment) 구조

IEEE 1609에서는 차량 간 통신에 적합한 프로토콜인 WAVE(Wireless Access in Vehicular Environment)의 표준화를 진행 중이다 [4]. 그림 2는 WAVE 프로토콜의 계층 구조를 나타낸 것이다. IEEE 802.11p를 물리계층으로 활용하며, 5.85 ~ 5.925 GHz의 전용 주파수 대역을 사용한다. IEEE 802.11p 상위의 MAC 및 응용계층은 IEEE 1609에 정의되어 있다.

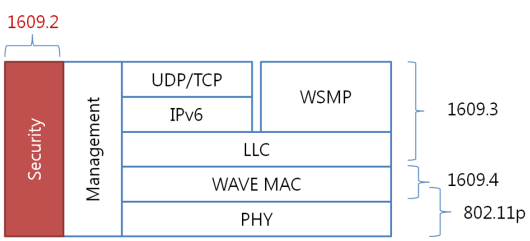
물리계층인 IEEE 802.11p의 특성은 차량의 고속 이동 환경에 적합하도록 기존의 무선 랜 규격에 비하여 좁아진 채널 대역폭(10MHz), 높은 RF 출력(최대 44.8 dBM)을 가진다. 또한, 교통 안전 메시지의 빠른 전송을 위한 제어 채널과 트래픽 메시지 전송을 위한 서비스 채널로 채널을 구분하여 사용하는 멀티 채널 스위칭 방식을 채택하고 있다. 또한, IEEE 802.11p에서는 무선 링크 접속 시간을 단축하기 위하여 기존 무선 랜에서의 링크 접속을 위한 인증 및 협상 단계를 생략한 것이 특징이다.

물리 계층 위에서 정의되는 WAVE 표준의 내용은 다음과 같다.

- 1609.0-2013 Architecture
  1609.0에서는 WAVE 통신 시스템 개요를 기술한다.
- 1609.1-2006 Resource Manager
  1609.1에서는 WAVE 자원 관리 어플리케이션의 서비스 및 인터페이스에 대하여 정의한다. WAVE 구조에서 제공되는 데이터 및 관리 서비스에 대하여 기술하고, 명령어 메시지 및 그에 대응되는 응답 메시지의 포맷을 정의하고, WAVE 규격 상의 개체 간 통신을 위한 어플리케이션의 데이터 저장 포맷에 대하여 정의한다. 현재는 철회 상태이다.
- 1609.2-2013 Security Services for Applications and Management Messages
  1609.2에서는 보안 메시지 규격과 보안 통신을 위한 처리 절차를 기술한다.
- 1609.3-2010 Networking Services
  1609.3에서는 WAVE 데이터 교환을 위한 주소 체계 및 라우팅 방법을 포함하는 네트워크/전송 계층 서비스를 정의한다. WAVE Short Message 프로토콜과 WAVE 프로토콜 스택을 위한 관리 정보를 기술한다.
- 1609.4-2010 Multi Channel Operation
  IEEE 1609.4에서는 제어 채널 및 서비스 채널로 구성되는 다중 채널을 지원하기 위한 MAC 계층을 정의한다.
- 1609.11-2010 Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)
  1609.11에서는 도로통행요금 징수를 위한 전자 지불 응용에 대한 규격을 정의한다.
- 1609.12-2012 Identifier Allocations
  WAVE 표준에서 정의하고 있는 ID인 PSID(Provider Service ID) 및 Object ID(OID)의 할당 규격을 정의한다.

WAVE 표준 규격에는 OSI 계층 구조의 Application 계층을 명시적으로 표현하지 않고 있다. 도로 통행료 과금을 위한 응용 예는 1609.1에서 다룬다.

WAVE 통신 기술을 이용한 어플리케이션은 차량 주행의 안전성과 직결된 문제이므로, 도청, 스푸핑, 변조, replay 공격 등으로부터 메시지를 보호하는 것이 필수적이다. 또한, WAVE 기술은 개인의 차량에 적용되는 기술이므로, 운전자의 프라이버시 보장 또한 필수적으로 제공되어야 한다. WAVE 보안 기술의 가장 큰 제약사항은 보안 기능으로 인한 메시지 전송 시간의 지연을 줄이는 것이다. 즉, WAVE의 특성 상 고속 이동 중인 차량 간에 전송되는 메시지를 보호하게 되므로, 패킷 손



〔그림 2〕 WAVE 개념도

실이 발생하지 않도록 보안 기능에 의한 처리 지연 시간이 최소화되어야 한다.

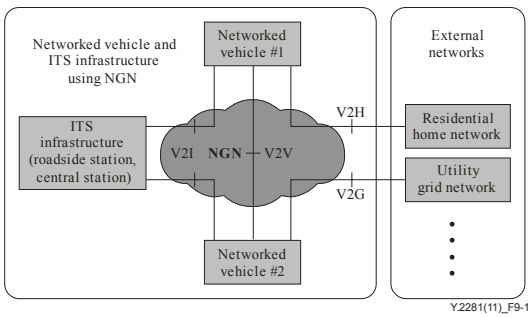
IEEE 1609.2 에서는 WAVE 기술을 위한 보안 서비스를 정의한다[4]. WAVE 메시지에 대한 인증 메커니즘 및 사용자에 대한 인증 메커니즘을 제공한다. 주목할 사항은 사용자 보호를 위한 익명 인증 메커니즘에 관해서는 여전히 표준화가 진행 중이며, 현재 버전의 표준에서는 포함하고 있지 않다.

2.3. ITU-T NGN 기반 네트워크 차량 프레임워크

ITU-T 의 Y.2281은 차세대 네트워크(NGN, Next Generation Networks)에서의 네트워크에 접속되는 차량의 응용 및 서비스에 대한 프레임워크를 기술한다. Y.2281은 NGN을 이용하여 네트워크를 형성하는 차량과 NGN과의 관계성을 정의한다. 또한, NGN을 이용하여 네트워크를 형성하는 차량과 NGN 및 이를 이용하는 ITS의 서비스에 대하여 기술하고 있다. 그림 3은 Y.2281의 참조 모델을 나타낸 것이다. 그림에서는 차량이 NGN을 통한 차량 간 통신, 그리고 차량과 인프라 간의 통신을 이용한 ITS 서비스를 모델링하고 있다. 또한, 기존의 홈 네트워크 및 전기차를 고려한 스마트 그리드와의 연결성 또한 모델링 하고 있다.

다른 ITS 표준과 비교할 때, Y.2281은 ITS 환경에 NGN을 적용하는 것에 초점이 맞추어져 있다. Y.2281에서는 peer-to-peer ITS통신과 NGN과 같은 공개 네트워크 간의 호환성 문제를 최소화하기 위한 NGN의 적용 방법을 정의한다.

NGN은 사용자 기능 계층, 서비스 계층, 전송 계층, 관리 계층, 그리고 NGN 기반 응용 계층으로 구성된다. NGN의 관점에서는 NGN 기반 차량과 ITS 기반 구조는 사용자 기능 계층에 존재하게 된다. Y.2281에서는 차량에 특화되는 NGN 응용으로 차량 응급 전화 서비스 등을 예로 들고 있다.



〔그림 3〕 Y.2281의 네트워크 모델 개념도

Y.2281의 보안 고려 사항은 Y.2201에 기반하여 정의한다. 차량에 네트워크가 연결되므로 보안 고려사항이 존재한다는 의미이다. 그러나, Y.2281에서는 차량이 NGN과 연결될 때의 보안 고려사항만 다룰 뿐, 기타 네트워크를 통한 차량의 네트워크 형성에 관해서는 다루지 않고 있다.

2.4. ITU-T 차량 게이트웨이 플랫폼 구조

ITU-T SG16에서는 차량 게이트웨이 플랫폼에 대한 표준화가 진행 중이다. 차량 게이트웨이는 차량 내부의 개체와 물리적으로 차량 내부 또는 차량 외부에 존재하는 다른 개체와의 실시간 통신을 지원하는 디바이스라고 정의한다[5]. 차량 게이트웨이 플랫폼은 차량 게이트웨이의 통신 서비스를 실현하기 위한 소프트웨어 및 하드웨어의 구현 형태를 의미한다. 차량 게이트웨이의 큰 특징 중 하나는 개방형 구조를 취하고 있다는 것이다. 차량 게이트웨이는 차량 내부 네트워크와 차량의 외부 네트워크를 연결하는 브리지 역할을 수행한다. 즉, 차량 게이트웨이는 차량의 센서들로부터 차량의 정보를 수집하고, 차량 외부 네트워크를 상기한 정보를 외부 네트워크에서 적용하고 있는 프로토콜로 변환하는 기능을 수행한다.

2.5. ITU-T SG17에서의 표준화 활동

SG17에서는 2014년부터 ITS 보안 분야의 표준화가 진행되었다. 기존의 차량통신보안 표준화는 차량 통신을 표준화하는 단체에서 전체 표준의 일부 항목으로 표준화가 진행되었다. 따라서, SG17같은 보안 분야를 담당하는 전문 표준화 기구에서 차량 통신 보안 분야에 대한 표준화를 진행하고 있다는 것이 그 의의가 크다고 할 수 있다. ITU-T SG17에서는 지난 2014년 9월 회의에서 차량 통신 보안 및 ITS 보안을 주제로 2개의 신규 워크 아이템을 선정하고 이에 대한 표준화가 진행 중이다. 한 건은 ITS 보안을 포괄적으로 접근하는 표준안(X.itssec-2)[7]이고, 또 다른 한 건은 ITS 보안 분야 중 특정 분야에 대한 표준(X.itssec-1)[6]을 제정하는 것이다.

X.itssec-1, Software update capability for ITS communications devices의 표준화 범위는 안전한 차량의 소프트웨어 업데이트 절차를 정의하는 것이다. 오늘날 차량에서는 다수의 ECU(Electronic Control Unit)를 적용하고 있고, 리콜이 요구되는 차량의 약 30%가 ECU 소프트웨어의 업데이트로 인한 문제라고 보고되고 있는 현상을 반영하고, 안전한 소프트웨어 업데이트 절차를 표준화하고자 하는 것이 X.itssec-1의 목적이다. X.itssec-1에서는 차량의 원거리 소프트웨어 업데이트 개요, 위협 요소 및 위협 분석, 기능 요구사항, 안전한 소프트웨어 업데이트 구조를 정의한다.

X.itssec-2, Security Guidelines for V2X communication Systems에서는 차량통신시스템에 대한 보안 가이드라인을 표준의 범위로 설정하고 있다. V2X 통신 시스템은 차량 통신 시스템을 통칭하는 것으로 차량과 차량(V2V), 차량과 인프라(V2I) 및 차량과 노매딕 디바이스(V2N) 간의 통신 환경을 의미한다. X.itssec-2에서는 V2V, V2I, V2N 통신 환경에서의 보안 위협 및 보안 요구 사항을 정의하고, 차량 등록 및 인증 서비스 모델 등의 유즈 케이스를 표준화 범위로 지정하고 있다. X.itssec-1과 X.itssec-2에 대하여 미국과 일본이 적극적으로 표준화를 추진 중이므로, 이에 대응하여 한국 또한 국내 기술을 반영하여 적극적으로 표준화를 추진할 필요가 있다.

Ⅲ. 결 론

본 논문에서는 차량 통신 보안 표준화가 활발히 진행되고 있는 다양한 표준화 단체의 표준화 내용과 ITU-T SG17에서 새롭게 추진 중인 표준안에 대하여 살펴보았다. ITU Y.2281은 차량 통신 네트워크로서 NGN을 적용하는 측면에 대한 표준이다. IEEE 1609.2는 5.9GHz DSRC 통신을 위한 구현 측면에서의 보안 기술을 표준화하고 있다. 반면에, ETSI에서는 5.9GHz DSRC 뿐만 아니라, 이동통신 망 등도 고려한 통신 구조를 표준화하고 있는 실정이다. ITU SG16에서는 다양한 통신 환경에 적용될 수 있는 차량 게이트웨이 플랫폼에 대한 표준을 진행 중이며, ITU-T SG17에서는 차량 소프트웨어 업데이트라는 특정 응용으로부터 접근을 취하는 표준안(X.itssec-1)과 포괄적인 접근을 취하는 표준안(X.itssec-2)에 대한 표준화가 진행 중이다.

현재 대두되고 있는 IoT 보안의 실제적인 적용 사례라고 할 수 있는 차량 통신 보안 표준화가 국제적으로 활발히 진행되고 있는 만큼, 정부, 학계, 연구기관의 적극적인 참여를 통한 국제 표준화의 주도권 선점이 필요한 시점이다.

참 고 문 헌

[1] 이상우 외, “차량 통신 보안 기술 동향,” 주간기술동향, vol. 1556, 2012.

[2] ITU-T Y.2281, Framework of networked vehicle services and applications using NGN, 2011.

[3] ETSI EN 302 665, Intelligent Transport Systems (ITS); Communications Architecture, 2010.

[4] IEEE Std 1609.2, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Security Services for Applications and Management Messages, 2013.

[5] ITU-T SG16 draft Recommendation, H.VGP-ARCH, Architecture of Vehicle Gateway Platform.

[6] ITU-T SG17 draft Recommendation, X.itssec-1, Software update capability for ITS communications devices.

[7] ITU-T SG17 draft Recommendation, X.itssec-2, Security Guidelines for V2X communication Systemsoftware update capability for ITS communications devices.

〈저 자 소 개〉

이 상 우 (Sang-Woo Lee)
정회원

1999년 2월 : 경북대학교 전자공학과 학사
2001년 2월 : 경북대학교 전자공학과 석사
2009년 2월 : 경북대학교 전자공학과 박사
2001년 1월~현재 : 한국전자통신연구원 사이버보안연구본부 선임연구원
2014년~현재 : ITU-T SG17 editor
관심분야 : 임베디드 보안, 차량통신보안, 융합보안

이 병 길 (Byung-Gil Lee)
정회원

1991년 2월 : 경북대학교 전자공학과 학사
1993년 2월 : 경북대학교 전자공학과 석사
2003년 2월 : 경북대학교 전자공학과 박사
2001년 1월~현재 : 한국전자통신연구원 사이버보안연구본부 책임연구원
관심분야 : IT융합보안기술, 보안 관제

나 재 훈 (Jae Hoon Nah)
종신회원

1985년 2월 : 중앙대학교 컴퓨터공학과 졸업
1987년 2월 : 중앙대학교 컴퓨터공학과 석사
2005년 2월 : 한국외국어대학교 전자정보공학과 박사
1987년~현재 : 한국전자통신연구원 사이버보안연구본부 전문위원/책임연구원
2009년~현재 : ITU-T SG17 Q7 Rapporteur
2011년~2012년 : 한국정보보호학회 학회지 편집위원장
<관심분야> IPv6/MIPv6, P2P, IPTV, 웹메시업 보안