지능형 차량 보안 기술 동향

A Survey of Intelligent Vehicle Security

u-IT839의 정보보호 이슈 특집

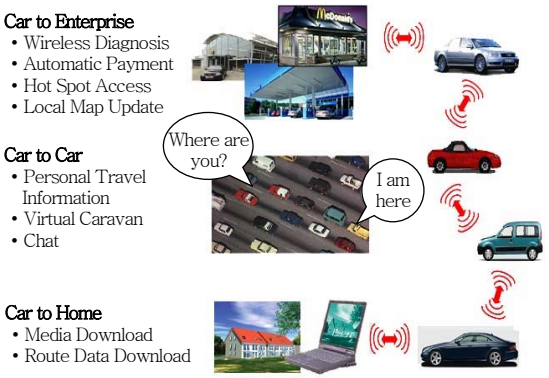
최병철 (B.C. Choi) 정보보호원천연구팀 선임연구원
한승완 (S.W. Han) 정보보호원천연구팀 선임연구원
정병호 (B.H. Chung) 정보보호원천연구팀 선임연구원
김정녀 (J.N. Kim) 정보보호원천연구팀 팀장

목 차

국내외적으로 지능형 차량 및 텔레매틱스/ITS 연구 개발을 통해서 차량에 IT 기술 접목을 위한 노력을 가속화하고 있다. 우리나라의 경우 산업자원부가 미래 10대 전략품목으로 자동차 부분에서 지능형 차량을 선정하였으며, 정보통신부는 u-IT839의 핵심 서비스로 텔레매틱스/ITS 서비스를 추진하고 있다. EU는 i2010 Flagship에서 intelligent car initiative 프로젝트를 통해 지능형 차량 및 보안을 위한 전략 수립과 세부 과제를 수행하고 있다. 또한, IEEE 802.11p/P1609(WAVE)와 ISO TC204/WG16 CALM에서는 차량 통신 보안 및 서비스에 대해서 고려하고 있다. 현재 지능형 차량과 관련하여서는 다양한 사업 모델이 제시되고 있으며, 자동차 업계의 BM과 이동통신 업계의 AM이 동반 성장하고 있다. 본 기고문은 지능형 차량 및 텔레매틱스/ITS와 관련한 보안 기술 동향을 살펴본다.

Ⅰ. 서론

IT 기술은 우리의 생활 속에서 다양한 형태로 컨버전스가 되어 현실화되고 있다. 디지털 홈, 텔레매틱스, 지능형 로봇 등에 접목되어 네트워킹 및 인포테인먼트가 가능한 형태로 진화되고 있다. 특히, 차량의 경우 IT와의 컨버전스를 통해서 BM 뿐만 아니라 AM 시장을 확대하고 있으며, 이는 차량을 이용한 다양한 신규 서비스를 창출할 수 있기 때문이다. 현재까지는 휴대 단말에 국한되었던 다양한 서비스들이 향후에는 차량의 지능화에 의해서 실현될 것으로 전망된다[1]. (그림 1)은 차량을 통한 다양한 서비스 시나리오에 관한 것이다[2]. C2E, C2C, C2H



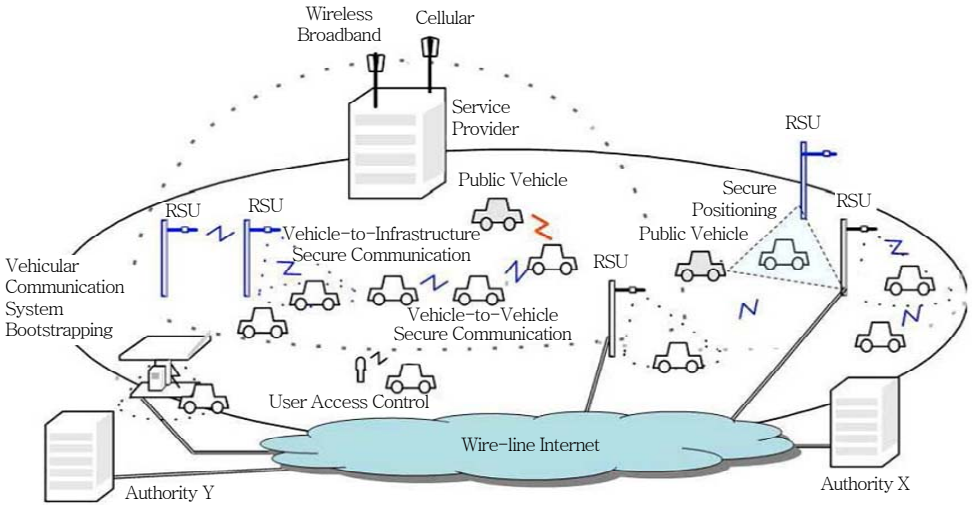
(그림 1) 지능형 차량 서비스 시나리오

간의 다양한 서비스 모델을 제시하고 있다. 이 중에서 현재도 가능한 서비스도 있지만 아직 현실화되지 않은 서비스로 있다. 이를 위해서는 지능형 차량 서비스를 위한 인프라가 확충되어야 가능하다. 중요한 것은 이러한 서비스 시나리오는 자동차 제조 업체뿐만 아니라 통신 사업자 및 포털 사업자에게도 많은 사업 기회를 줄 것으로 예상한다. 다만 이러한 서비스 활성화를 위한 기반 기술 개발 및 법제도의 정비도 반드시 필요할 것이다. 또한, 이러한 서비스에 의한 역기능, 즉 개인정보 및 프라이버시 침해, 차량 정보/통신 메시지/트래픽 정보 등의 위변조 위협 등을 해결해야 할 것이다[3].

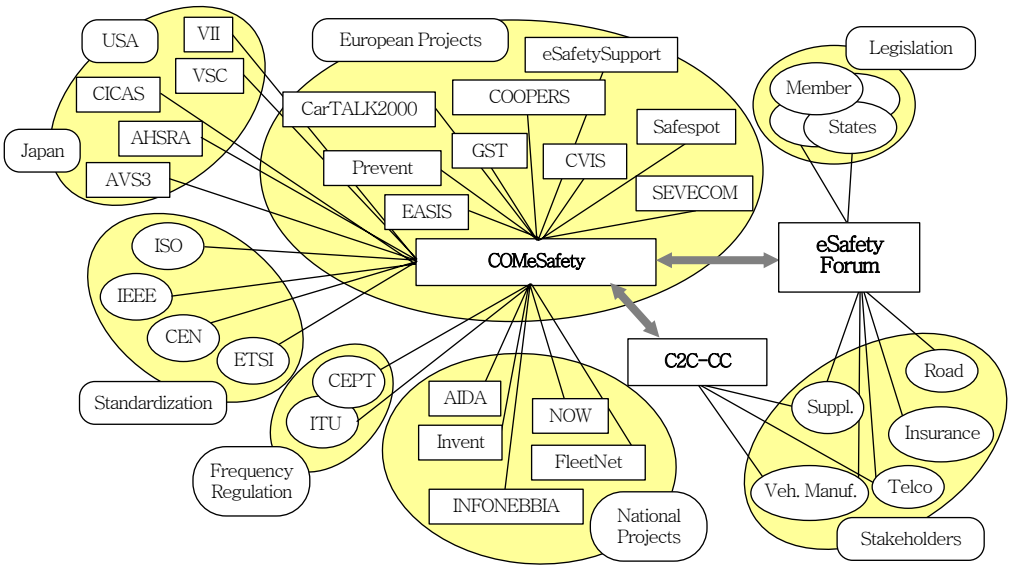
(그림 2)는 안전한 차량 서비스 및 통신을 위한 보안 프레임워크이다. Secure Positioning, Vehicle-to-Infrastructure Secure Communication, Vehicle-to-Vehicle Secure Communication, User Access Control, VPKI 등을 포함하고 있다[3].

Ⅱ. 연구 동향

국내외적으로 지능형 차량을 이용한 다양한 서비스를 위해서 차량 통신(vehicle communication) 및 관련 보안 기술을 연구 개발하고 있으며, 대부분 아



(그림 2) 지능형 차량 통신 보안 개념도



(그림 3) 국외 지능형 차량 연구 동향

직 초기 단계에 머무르고 있다. 그러나, 유럽의 경우 국가적인 지원을 받아 i2010 Flagship의 intelligent car initiative 프로젝트를 통해서 연구에 박차를 가하고 있다[4]. 학계에서는 스웨덴의 EPFL(연방공과대학)에서 차량 통신에서의 보안 및 프라이버시, 키 관리 문제 등에 대해서 많은 연구 결과를 산출하고 있다. 산업계에서는 미국의 IEEE 802.11p/P1609 (WAVE)에서 VSCC (U.S. Vehicle Safety Communication Consortium)의 지원을 받아서 차량 통신용 키 관리(폐기 및 갱신)를 위한 익명성 지원 비대칭 암호 기술을 연구하고 있다[1],[3],[5]. 유럽은 차량 통신 보안에 대해서 C2C-CC의 지원을 받아 NoW 및 GST 등의 프로젝트를 통해서 차량 통신 보안에 대해서 연구를 해왔으며, 현재는 EU의 SEVECOM을 포함한 COMeSafety 프로젝트를 통해서 차량 통신 보안에 대해서 연구 개발을 추진하고 있다. 이와 관련하여 전체 국외 지능형 차량 연구 동향은 (그림 3)과 같다[2],[3],[6].

Ⅲ. 취약성 및 보안 프레임워크

지능형 차량을 이용한 다양한 서비스를 하려면 통신(V2V, V2I) 기술이 필요하며, 이러한 차량 통신 환경에서의 보안 취약성, 주요 고려사항 및 제약사항, 그리고 보안 프레임워크를 아래와 같이 분석하였다.

다음은 취약성에 대한 설명이다.

1. 취약성

• Jamming (like DoS Attack)

일정 네트워크 영역 내에서 다른 차량의 통신에 장애를 초래하는 신호를 발생시키는 공격

• Forgery

거짓 정보를 발생하는 공격 차량에 의해 일정 네트워크 영역 내의 다른 차량들을 거짓 정보로 오염시키는 위협

• In-transit Traffic Tampering

주행중에 메시지 또는 정보의 전달 과정에서 drop, corrupt, 또는 modify를 통한 정보의 위변조 공격

• Impersonation

차량의 상태 정보를 변경하여 다른 차량으로 하

여금 오인하도록 하는 공격

• Privacy Violation

시간, 위치, 차량 ID, 이동 정보 등의 차량과 관련된 개인 프라이버시 정보에 대한 침해

• On-board Tampering

차량 내부의 정보(속도, 위치, 차량 전장 부분의 상태, 각종 센싱 정보 등)에 대한 위변조 공격

또한, 이러한 지능형 차량은 고속(약 시속 180km 이하) 이동 환경에 의한 제약사항을 고려하여야 한다. 다음은 차량 통신 및 서비스에서의 주요 제약사항 및 고려사항이다.

2. 고려사항 및 제약사항

• Network Volatility

차량 네트워크(VANET)는 고속 주행으로 인하여 빠르게 토폴로지가 변화되는 네트워크 휘발성을 내재

• Liability vs. Privacy

차량 정보를 이용한 사고 처리 등에서 책임 및 법적 자료 제공에 따른 개인 정보 침해 가능성 존재

• Delay-sensitive Applications

VANET의 특성상 실시간성으로 정보 처리가 이루어져야 함(차량용 AAA 프레임워크 필요)

• Network Scale

전세계에는 수십억 대의 차량이 존재하며 이들간의 안전한 관리 및 키 분배 등에 제한이 따름

• Heterogeneity

서로 다른 국가, 제조 업체, 서비스 업체에 따라서 차량을 이용한 서비스의 이질성이 존재

지능형 차량 통신 및 서비스를 위한 보안 인프라는 AAA 프레임워크를 사용하며, 다음과 같은 보안 요소 기술들이 필요하다.

3. 보안 프레임워크

• Security Hardware

차량 통신 보안을 위한 하드웨어로는 ELP(전자번호판), EDR(차량용 블랙박스), TPD(차량용 TPM, Advanced EDR) 등이 있음

• VPKI

VANET 차량 통신 인프라에 적용할 수 있는 PKI 인증 인프라

• Authentication

보안 처리에 의한 오버헤드를 줄이기 위해 ECC를 사용하고 있으며, 좀더 빠른 인증 처리를 위한 기술을 연구 개발 진행중임

• Certificate Revocation

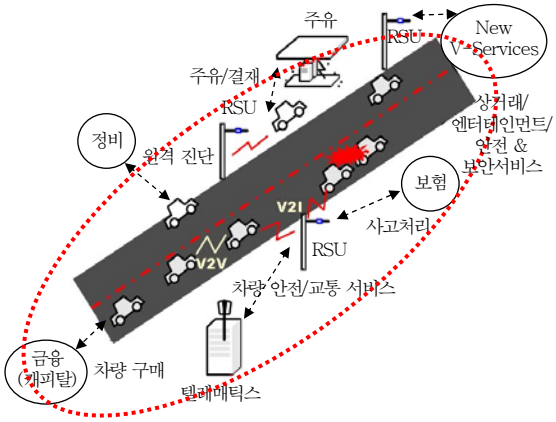
VPKI 인증 인프라에서 키 폐기 및 갱신은 매우 중요한 요소이며, 일반적으로 CRLs를 이용하지만, 보다 효율적인 키 폐기 및 갱신을 위한 연구가 진행중임

• Privacy

차량 보안을 위한 하드웨어로 ELP(전자번호판)과 EDR(차량용 블랙박스) 등이 연구 개발되고 있지만, 이는 프라이버시 문제 때문에 TPD와 같은 차량용 하드웨어가 요구되고 있음. 또한, 차량 통신에 사용되는 다양한 정보(시간, 위치, 차량 ID 등)가 실시간으로 노출되고 있기 때문에 개인 정보 및 프라이버시 침해 대응 기술이 연구되고 있음

Ⅳ. 결론

국내외적으로 지능형 차량 및 텔레매틱스/ITS에 대한 연구 개발이 활발하게 이루어지고 있다. 현재 미국, 유럽, 일본은 자동차 업계 중심으로 사업 모델을 진행하고 있으며, 국내의 경우는 자동차 업계와 통신 업계가 동반 주도하는 형태를 취하고 있다. 차량과 관련한 서비스 및 연구개발 수준은 아직 선진



(그림 4) 지능형 차량을 이용한 V-서비스 모델

국에 비해서 미흡하지만, 정부(산하연구기관 포함)의 의지와 차량 업계 및 통신 업계에서 꾸준히 노력하고 있기 때문에 그 전망은 밝을 것으로 예상한다.

(그림 4)는 향후 중장기적으로 구축될 지능형 차량을 이용한 서비스 사업 모델에 대해서 예시한 것이다. Car to ITS/텔레매틱스와 V2V/V2I 통신 인프라(VANET, VPKI)를 이용한 V-Commerce, V-Entertainment, V-Safety 등의 서비스, 그리고 차량 안전 및 보안 관리를 위한 다양한 하드웨어 장치(Advanced EDR, ELP, TPD 등)가 개발되어 사용될 것으로 전망된다.

약 어 정 리

AAA	Authentication, Authorization, Accounting
AM	After Market
BM	Before Market
C2C-CC	Car2Car Communication Consortium
C2C	Car to Car
C2E	Car to Enterprise
C2H	Car to Home
CALM	Communication Air-interface Long and Medium range
CRLs	Certificate Revocation Lists
DoS	Denial of Service
ECC	Elliptic Curve Cryptography
EDR	Event Data Recorder
ELP	Electronic License Plate
GST	Global System for Telematics
ITS	Intelligent Transport Systems
NoW	Network on Wheels
RTPD	Revocation protocol of the Tamper-Proof Device
SEVECOM	Secure Vehicular Communication
TPD	Tamper-Proof Device
TPM	Trusted Platform Module
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VANET	Vehicular Ad Hoc Networks
VPKI	Vehicular PKI (Public Key Infrastructure)
WAVE	Wireless Access in Vehicular Environments

● 용 어 해 설 ●

텔레매틱스(Telematics): 자동차에 위치 측정 시스템(GPS)과 지리 정보 시스템(GIS)을 장착하고 운전자와 탑승자에게 교통 정보, 응급 상황 대처, 원격 차량 진단, 인터넷 이용 등을 제공하는 모바일 서비스

ITS (Intelligent Transport System, 지능형 교통 시스템): 전기, 전자, 정보, 통신, 자동차 기술을 교통에 적용하여 교통 체증과 비경제 등 심각한 교통 문제에 효과적으로 대응하기 위해 선진 각국에서 추진하고 있는 종합 교통 정보의 수집/가공/전파 시스템

참 고 문 헌

[1] TTA, "Standardization Roadmap for IT839 Strategy – Telematics/ITS," 2006.

[2] Rudy Mietzner, "COMeSafety," *In Proc. of SEVECOM Workshop*, BMW Group, Feb. 2006.

[3] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux, "Securing Vehicular Communications," *In Magazine of IEEE Wireless Communications – IVC Specials*, EPFL, Oct. 2006, pp.8-15.

[4] EU i2010 Flagship – intelligent car initiative (http://europa.eu.int/information_society/activities/poicy_link/brochures_2006/documents/intelligent_car.pdf), 2006.

[5] Daniel Jiang, Vikas Taliwal, Andreas Meier, Wieland Holfelder, and DaimlerChrysler AG, "Design of 5.9GHz DSRC-based Vehicular Safety Communication," *In Magazine of IEEE Wireless Communications – IVC Specials*, Oct. 2006, pp.36-43.

[6] Knut Evensen, "CALM – Continuous Communications for Vehicles," *In Proc. of SEVECOM Workshop*, Q-Free, Feb. 2006.