ETRI

2013
Electronics and
Telecommunications
Trends

사이버 보안 기술 특집

지능형 차량·교통 보안 기술 동향

Security Trends in Intelligent Vehicle·Transport System

한종욱 (J.W. Han) 융합보안연구실 책임연구원
이병길 (B.G. Lee) 융합보안연구실 책임연구원
손명희 (M.H. Son) 융합보안연구실 선임연구원
최병철 (B.C. Choi) 융합보안연구실 선임연구원
김무섭 (M.S. Kim) 영상보안연구실 선임연구원
나중찬 (J.C. Na) 융합보안연구실 실장
조현숙 (H.S. Cho) 사이버보안연구단 단장

단순히 빠른 이동의 수단에서 안전하고 쾌적하게 이동할 수 있는 이동 수단으로 자동차 및 교통 인프라가 진화하고 있다. 이를 위한 IT 기술과의 융합으로 차량과 교통 인프라가 사이버 공격 등에 취약함이 다수의 사례를 통해 증명이 되고 있다. 본고에서는 차량과 교통 관점에서 발생 가능한 사이버/물리적 보안 취약점과 이에 대응하기 위한 보안 기술 현황을 살펴보고 향후 추가적으로 고려해야 할 보안 이슈들을 정리하였다.

Ⅰ. 서론

일상 생활에서 교통수단에 대한 의존도는 매우 높아지고 있으며, 단지 빠른 이동의 개념에서 쾌적하고 안전하게 이동하는 개념으로 사용자의 요구수준이 변화하고 있다. 이러한 사용자 요구수준 변화와 교통문제의 해결을 위해 지능형 교통체계인 ITS(Intelligent Transport System)가 도입되고 있으며 도로교통 혼잡, 교통사고, 물류비용 등 기존 교통관련 문제점을 획기적으로 개선할 수 있는 최적의 대안으로 주목받고 있다.

ITS의 세부 목표인 운전자 및 보행자, 차량 등의 안전을 위해 자동차 내장형 지능형 시스템들이 전 세계적으로 연구되고 있다. 주요 메이저 업체들은 보행자 안전을 위해 지능형 나이트 비전 시스템을 탑재한 상용차를 출시하고 있으며, 충돌 방지, 차선 변경 지원이나 차선 이탈 예방, 졸음운전 방지 등 다양한 지능형 시스템 등을 연구, 개발하고 있다.

또한, 교통 사고 발생 시 사고 원인 분석과 증거자료 확보를 위해 차량용 블랙박스 시장이 급격히 증가하고 있으며 상용차량에 대해서는 설치가 의무화되는 등 블랙박스 수요는 더욱 증가할 것으로 예상되고 있다.

본고에서는 교통 및 차량 분야의 보안 및 안전을 위해 국내외에서 연구, 개발되고 있는 ITS 분야, 차량용 지능형 시스템, 블랙박스 등에 대해 전반적으로 살펴보고 향후 보안 관점에서 고려해야 할 부분을 정리하였다.

자동차 · 도로 분야에서의 ITS는 도로교통 시스템의 구성 요소인 교통수단 및 시설에 첨단기술을 적용하여 교통운영 · 관리의 효율성을 극대화하고, 이용자 편의와 안 전성을 제공하며, 연료 소모 및 CO_2 배출량을 저감시키는 미래형 교통체계를 의미한다. ITS의 목표 달성

(그림 1) 지능형 교통체계 개념

〈표 1〉 지능형 교통체계 서비스

서비스	내용
교통관리	실시간 교통 제어, 광역 교통류 제어, 고속도로 교통류 제어, 교통 제어 정보 제공, 돌발상황 감지 및 대응조치, 긴급차량 운행관리 지원, 위반차량 단속
대중교통	시내 · 시외 · 고속버스 정보 제공, 대중교통 안전관리, 시내 · 시외 · 고속버스 운행관리, 대중교통 시설관리, 환승요금 관리
전자지불	유료도로 통행료 전자지불, 혼잡통행료 전자지불, 주차요금 전자지불, 대중교통요금 전자지불
교통정보 유통	기본 교통정보 제공, 교통정보 관리 · 연계
지능형 차량 · 도로	차량 전 · 후 · 측방 충돌 예방, 교차로 충돌 예방, 철도건널목 안전 관리, 감속도로구간 안전 관리, 차량안전 자동진단, 운전자 시계 향상, 위험운전 방지, 차량간격 자동제어, 자동조향운전, 군집 운행
부가교통 정보 제공	여행자 정보 제공, 출발 전 여행정보 제공, 운전 중 교통정보 제공, 주차정보 제공, 주행안내
화물운송	화물추적 관리, 화물차량 운행관리, 화물차량 경로안내, 화물차량 안전관리 지원, 위험물 관리 및 사고 처리, 위험물 차량경로 안내 및 관리, 화물전자통관 · 전자행정

을 위해서는 (그림 1)과 같이 교통수단, 교통시설, 서비스 인프라 등이 첨단화, 최적화되어야 이동성, 안전성, 편리성의 향상이 가능해진다.

이미 선진국에서는 ITS의 대표기구를 설치하고 조기 정착을 위하여 민간 및 정부기관에서 다양한 연구가 수행 중에 있다. EU에서는 63개 산학협동으로 CVIS 프로젝트를 진행하고 있으며, 첨단차량과 첨단도로의 효율적 운영을 통해 도로 안전과 잠재적인 위험 요소를 인지하고 안전거리 유지와 주변 환경에 따른 운전자의 시공간적 상황을 인지시켜 사고를 예방하기 위한 기술을 개발하는 SAFESPOT 프로젝트도 진행하고 있다. 미국의 경우는 PATH, IVBSS 등의 프로젝트가 진행 중에 있으며, 일본에서도 ITS-Safety 2010이란 프로젝트가 진행되는 등 세계 각국은 ITS 추진에 많은 노력을 기울이고 있다[1]. 우리나라에서도 구 건설교통부(현, 국토교통부)에서 2000년 12월 '지능형 교통체계 기본계획 21'을 수립하였으며, 수정 보완하여 2011년 12월 '지능형 교통체계 기본계획 21'의 하위 계획인 자동차 · 도로 ITS 계획을 10년의 범위에서 수립하였다. 현재 한국도로공사와 각 지자체별로 ITS 센터를 구축하고 실시간 교통상황, 버스도착 정보, 정체구간 등 운전에 필요한 정보를 제공하고 있다. 또한 이와 함께 자동차 회사들에서도 좀 더 안전하고 편리한 운전을 지원하기 위한 지능형 자동차 연구개발이 이루어지고 있다.

ITS의 기본 서비스를 정리하면 〈표 1〉과 같다.

ITS를 기반으로 한 지능형 교통체계 서비스 성공을 위해서는 보안 기술이 반드시 적용이 되어야 한다. 미국 샌디에이고 대학과 위싱턴 대학 연구진이 시속 40마일로 주행 중인 차량을 해킹하여 전자제어장치를 무력화함으로써 운전자가 차량을 통제하지 못하게 하는 시연에 성공한 사례에서 보듯이 차량 자체에 대한 보안 대책 수립이 필요하다. 또한, 인텔이 인수한 맥아피 소속 해커들이 미국 캘리포니아에서 수출용 차량을 선적하기 전에 차량 내부에 바이러스가 침투하지 않았는지 일일이 점검한 사례에서 볼 수 있듯이 자동차 업계는 해킹 문제에 대한 심각성을 인식하고 있다. 차량뿐 아니라 교통시설에 대한 해킹을 통해 제어권을 확보할 경우 불법적으로 교통신호기를 제어하여 대형 교통사고를 유도할 수도 있는 등, 〈표 1〉에서 목표로 하고 있는 서비스를 중단시키거나 또는 악용하는 경우 경제적 · 사회적 피해뿐 아니라 생명과 직결되는 인적 피해가 예상되므로 불특정 다수를 대상으로 하는 물리적 테러 수준에 준하는 보안 이슈로 인식하고 대응책 마련이 필요하다[2]. 따라서, 안전한 ITS 실현을 위해 국내외에서 다양한 보안 기술 개발 및 도입이 이루어지고 있다. 본고에서는 ITS, 차량용 지능형 시스템, 블랙박스기술 등 차량과 교통 전반에 걸쳐 관련 보안 기술 개발 및 상용화 현황을 정리하였고, 궁극적으로 안전한 차량·교통체계 구축을 위해 요구되는 보안 요구사항을 정리하였다.

II. 보안 및 안전 기술 개발 현황

1. 차량 통신 보안 기술

ITS 실현을 위해서는 차량을 중심으로 한 통신 네트워크 환경 구축이 반드시 필요하다. 하지만 지능형 서비스 제공을 위한 네트워크 환경이 역으로 해킹 공격을 가능하게 하는 통로를 제공하게 되므로 이를 해결하기 위해 국내외의 많은 연구가 진행되고 있다. 차량 통신 네트워크는 차량을 중심으로 내부망과 외부망으로 구분할 수 있는데 차량 내부망은 IVN(In-Vehicle Networking)이라 부르며, IVN은 차량의 오디오, 앰프, CDP 등 멀티미디어 기기 접속을 위한 MOST, 그리고 브레이크나 조향 장치를 연결하고 제어하는 X-by-Wire가 있다.

차량 외부망은 차량 간 통신망인 V2V(Vehicle-to-Vehicle)와 차량과 인프라 통신망인 V2I(Vehicle-to-Infrastructure), 그리고 차량과 사용자 단말 간 V2N(Vehicle-to-Nomadic Device)으로 분류된다. V2I 네트워킹은 차량과 유무선 통신망이 접속되어 단말과 서버 간에 통신을 지원할 수 있는 통신망으로 텔레매틱스 서비스, 자동요금 징수 서비스, 교통정보 수집 및 제공 서비스를 제공할 수 있다. V2V 네트워킹은 차량 간 통신을 기반으로 인프라 도움 없이 구성될 수 있는 차량 통신망으로 차량 안전 서비스를 제공하며 차량 간 실시간으로 정보를 전달하여 협력 주행 서비스를 제공할 수 있다. V2N 네트워킹은 휴대 단말과 차량을 직접 접속하여 차량 진단 및 제어 서비스를 제공할 수 있다. 이러한 V2I, V2V, V2N, IVN을 종합하여 V2X 네트워킹이라고 부른다[3].

미국 IntelliDrive 프로젝트는 V2V, V2I 통신 시스템 및 인프라를 구축하여 안전성, 이동성을 극대화하기 위한 목적으로 2003년부터 미국 DOT(Departments of Transportation)에서 지원을 하고 각 주의 DOT와 Ⅶ 컨소시엄의 주도로 진행되고 있다. 이를 위해 개발된 Vehicle IntelliDrive Module의 경우 유연하고 개방된 플랫폼을 제공하여 WAVE(Wireless Access in Vehicular Environments) 기반의 다양한 V2X 통신 및 애플리케이션 개발을 지원하며 현재는 Connected Vehicle로 이름이 변경되어 추진 중에 있다[4]. WAVE 통신 기술의 보안을 위해 IEEE 1609.2에 보안 메시지 규격과 보안 통신을 위한 절차가 표준화되어 있다. IEEE1609.2에서는 WAVE 메시지에 대한 인증 메커니즘 및 사용자에 대한 인증 메커니즘을 제공하고 있으며, 사용자 보호를 위한 익명 인증 메커니즘에 대해서도 표준에 포함이 되어 있다. WAVE 보안구조는 암호화, 디지털 서명 등을 통해 데이터 등을 안전하게 전송하는 데이터 처리부와 인증서 관리기능을 담당하는 관리 처리부로 구분이 된다. 인증서는 인증 대상에 따라 차량을 인증하기 위한 개체 인증서와 개체 인증서를 인증하기 위한 CA 인증서로 구분된다. IEEE 1609.2에서 사용하는 암호 알고리즘은 〈표 2〉와 같다[5].

WAVE 보안에서 해결해야 할 가장 큰 기술적인 이슈는 고속 이동 중인 차량 간에 전송되는 메시지를 보호하기 위해 패킷 손실이 발생하지 않도록 보안 처리 지연시간을 최소화하는 것으로 하드웨어적인 방법으로 해결하고 있다.

국내의 경우, 기존 도로에 비해 안전성, 이동성, 편리성 등이 개선된 도로를 구축하는 구 국토해양부의 스마트 하이웨이 프로젝트에서 WAVE 기반의 V2X 통신 및 보안 기술을 개발하고 있으며, 구 지경부의 자율안전주행을 위한 협력제어통신기술 개발 사업에서 WAVE 기반의 V2X 통신 및 보안 기술을 개발하고 있으며, 고속 보안 처리 구현이 핵심 목표이다.

〈표 2〉 IEEE 1609.2에 적용되는 암호 알고리즘

암호명	기능	참조 표준
ECDSA	디지털 서명	FIPS 186-3
ECIES	공개키 암호화	IEEE 1363a
AES-CCM	대칭키 암호화	FIPS 197 NIST SP 800-38C
SHA-256	해시	FIPS 180-3

국토교통부에서는 OBD, 디지털 운행기록계, 블랙박스 등 사업용 차량에 장착된 약 13여 종류의 차내 장치를 통합하는 표준 플랫폼을 개발하고 이로부터 수집되는 다양한 운행 정보를 교통관리공단에서 수집하여 운전자 맞춤형 서비스를 개발하는 과제를 수행하고 있다. 본 과제에서는 수집 정보의 무결성을 보장하고, 차량 통합 단말과 센터 간의 안전한 정보 전송을 위한 경량 VPN 기술, 임베디드 단말 환경을 고려한 암호 기술 등이 연구 내용에 포함되어 있다.

2. 차량용 블랙박스 보안 기술

최근 교통 사고 발생 시 사고 발생의 책임 소재에 대한 판단을 용이하게 하고 사고 예방의 효과를 높이기 위해 차량 주변의 상황을 영상으로 기록하는 차량용 블랙박스의 장착이 증가하고 있다. 일반적으로 EDR(Event Data Recorder)로 알려져 있는 블랙박스 장치는 비행기에 장착되어 항공기의 추락이나 대형 참사 등으로 동체가 거의 소멸되었을 때 사고의 원인 규명에 결정적인 역할을 하는 장치로 사용되어 왔다. 이러한 블랙박스의 개념을 차량에 의한 교통사고 해결에 적용한 것이 차량용 블랙박스이다. 차량용 블랙박스는 차량 충돌 사고 시점의 전 · 후 일정 시간 동안의 상황을 기록하여 피해자와 가해자의 주장이 서로 상반될 때 시시비비를 가리기 위한 증거자료를 제공한다는 점에서 최근 각광받고 있다. 특히, 택시, 버스 등 대중교통에서의 사고 발생 시 블랙박스 영상이 증거자료로 활용되는 사례가 증가하고 있어 상용차량에 블랙박스 설치를 의무화하는 추세로 진행되고 있다. 미국과 유럽 등 선진국들을 중심으로 블랙박스의 도입을 확대하고 있다. 미국은 2006년 도로교통안전국(NHTSA)이 자동차 제조업체에 차량 내 블랙박스 장착을 권고한 데 이어 도요타 리콜 사태를 계기로 '자동차 안전법안'을 마련하였다. 차량용 블랙박스는 항공기 블랙박스처럼 어떠한 사고에도 파손되지 않을 만큼 내구성이 뛰어나야 하고 방수·방화기능이 반드시 추가돼야 한다는 것이다. 또한 블랙박스에 기록된 운행정보는 교통사고 확인조사와 관련한 법원의 요구나 NHTSA의 요청이 있을 시에는 그 내용을 즉각 공개토록 했다. 미국 내 2005년형 승용차의 64%는 이미 블랙박스를 장착했으며 지금은 대부분의 완성차업체들이 차량에 블랙박스를 장착하고 있다. 특히 이 법안에 따라 2013년 이후부터는 대형급을 제외한다면 모든 승용차와 트럭에 블랙박스가 의무적으로 장착될 예정이다. 유럽은 2006년 사업용 차량에 이어 지난해 모든 차량에 블랙박스 장착을 의무화했다. 중국은 도로교통법을 개정해 모든 트럭과 버스, 택시에 블랙박스 장착을 의무화했으며 일본은 2004년부터 상업용 차량 등에 도입을 실시했다.

국내에서는 2013년까지 버스와 택시 등 사업용 차량에 블랙박스를 의무적으로 장착하도록 교통안전법을 개정, 공포해 현재 추진 중이다. 이에 따라 일부 지방자치단체 주도 아래 개인 및 법인택시 등에 대한 블랙박스 장착이 확산되고 있으며 민간에서는 여러 자동차 보험회사들이 블랙박스를 장착한 차량에 대해 3~4%의 보험료를 할인해주고 있다.

차량용 블랙박스에서 발생할 수 있는 보안 이슈는 저장된 사고 데이터의 위·변조 문제이다. 블랙박스의 특성상 법적인 증거자료로 활용되는 경우가 대부분이고 항공기용 블랙박스와는 달리 용이하게 접근할 수 있어 이해관계 당사자에 의한 위 · 변조 또는 파손 등의 가능성이 매우 높다고 할 수 있다. 따라서, 블랙박스 데이터에 대하여 원본 데이터의 진위 여부를 판단할 수 있는 무결성과 데이터의 위 · 변조 여부를 판별할 수 있는 보안 기술 대책이 요구되고 있다. 이러한 요구를 반영하여 2011년 에 "KS-R-5078: 차량용 영상 사고기록 장치" 국가표준에 제정되어 증거자료로서의 신뢰성을 가질 수 있는 기준을 마련하였다. ETRI, 고려대학교 등에서는 차량용 블랙박스 데이터의 신뢰성을 보장하는 표준 규격을 만족하는 보안 기술을 개발하였으며, 추후 상용차량을 중심으로 국가표준을 준용한 블랙박스 보급이 예

상되고 있다.

3. 차량 안전용 지능형 인식 기술

운전자 및 보행자의 안전 보장을 위해 컴퓨터 비전 기술에 기반한 지능형 차량안전 기술이 연구되고 있으며 이미 주요 메이저 업체에서는 지능형 비전 기술을 탑재한 차량을 출시하고 있다.

지능형 차량 비전 기술은 차선 유지 및 차선 이탈 경고, 전방 차량 충돌 방지 등을 위한 차선 및 전방 차 인식기능, 차선 변경 지원, 후면 충돌 경고, 사각지역 상황 전달 등을 위한 측/후방 차량 인식기능, 야간 주행 시 전방의 동물이나 보행자를 감지하여 경고를 주는 보행자 인식기능, 졸음운전 등 운전자의 비정상 상태를 감시하는 운전자 감시기능 등이 있다.

차선이탈 경보 시스템은 유럽의 시트로엥, 닛산, 도요타, GM 등의 상용차량에 탑재되어 판매되고 있으며, 운전자 감시기능은 아직 연구 단계로 상용화까지는 시간이 소요될 것으로 생각된다.

나이트 비전 시스템은 야간 주행 시 운전자에 개선된 시야를 제공해 주고 전방의 동물 및 보행자를 감지하여 운전자에게 주의를 줌과 동시에 충돌 예상 시 후속조치가 가능한 신호를 차량에 보내주는 시스템을 말한다. 지능형 나이트 비전 시스템은 외국에서는 이미 10여 년 전부터 첨단 안전 차량의 주요 기술로써 연구되어 왔으며, 현재 미국, 일본, 유럽의 많은 대학과 연구소 및 관련 업체를 중심으로 활발한 연구가 진행 중이고 주요 메이저 업체를 중심으로 나이트 비전 시스템이 탑재된 상용차량이 판매되고 있다. 연구 방향도 보행자나 동물의 존재 여부를 표시하는 기능에서 주행도로 상의 차선 이탈이나 사전 충돌 경보 등 전방 카메라로 구현 가능한 안전 관련 기능들이 추가되고 있는 추세이다.

나이트 비전 기술은 크게 근적외선을 이용하는 방법과 원적외선을 이용하는 방법으로 나누어지며, 현재 근적외선 방식은 원적외선 방식에 비해 적용이 용이하여 치열한 시장 경쟁이 예상되며, 벤츠의 S, E class 등에 적용되고 있다. 원적외선 방식은 BMW 5, 6, 7 시리즈 및 혼다의 Legend, Audi A8에 이 방식이 채택되어 있으나, 시장 형성은 아직 초기 단계이다.

Raytheon사에서 개발된 원적외선 기술을 응용한 나이트 비전인 Thermal-eye Series는 경찰, 소방서, 해양 구조대뿐 아니라 군대에 이르기까지 광범위하게 채택되어 야간 운전 시 시야 확보에 사용되고 있으며, 이를 이용하여 검지된 장애물을 위험성이 있는 장애물로 분류하여 경고하는 능동적 보행자 보호 시스템에 적용하고 있다. 혼다도 원적외선 기술을 적용하여 앞 범퍼에 2개의 원적외선 카메라를 장착하여 운전자의 야간 시야 확보는 물론 장애물의 검지 및 경고하는 지능화된 시스템을 개발하였다. 도요타는 근적외선 기술을 적용하여 헤드램프에서 근적외선 라이트를 조사하고, 룸미러 반대편에 위치한 카메라로 감지하여 클러스터 LCD 창에 디스플레이하며, 운전자의 야간 시야 확보는 물론 보행자 감지와 장애물의 변화를 감지 및 경고하는 시스템을 개발하였다. BMW는 5, 6, 7 시리즈에 원적외선 카메라를 적용하였으며, 앞 범퍼에 위치한 원적외선 카메라로 컨트롤 디스플레이 창에 나이트 비전 화면이 표시되며, 보행자 감지 시에 HUD에 보행자 아이콘을 표시하여 운전자에게 경고하는 시스템을 적용하였다. 벤츠는 근적외선 기술을 적용하여 헤드램프에서 근적외선 라이트를 조사하고 룸미러 반대편에 위치한 카메라로 감지하여 클러스터 LCD 창에 디스플레이하며, 운전자의 야간 시야 확보는 물론 보행자 감지와 장애물의 변화를 감지 및 경고하는 지능화된 시스템을 개발하였다.

Ⅲ. 향후 고려 사항

1. ITS 표준 보안 프레임워크

미국 및 국내 등 현재 ITS 관련 통신 보안은 차량을 중심으로 한 V2X 통신에 주력하고 있다. 진정한 ITS 서비스를 제공하기 위해서는 서비스 제공 서버부터 자동

차까지 전체 통신 보안이 중요하므로 ITS 전체를 아우르는 보안 프레임워크 정립이 필요하겠다. 아직 ITS 전체를 포괄하는 표준 프레임워크가 정립되지 않고 다양한 시도가 이루어지고 있는 상황이지만 보안전문가들이 적극 참여하여 발생 가능한 다양한 보안 취약점을 해결하는 보안 프레임워크 정립에 대한 연구를 주도할 필요가 있다. 차량 인증센터의 부재문제, 교통정보 메시지 무결성 보장, 차량 위치 기반 서비스에 따른 프라이버시 침해문제, 차량 전용 인증서 부재 문제, 노메딕 장비 인증 및 해킹 위협 등 다양한 보안 취약성 및 보안대책 부재 등을 고려한 프레임워크 정립이 필요하며, 특히 제공 서비스에 따라 다양한 취약점들이 존재할 수 있으므로 서비스 레벨의 보안문제까지 고려한 보안기능이 제공될 수 있도록 향후 연구가 필요하다.

2. 차량 내 임베디드 시스템 해킹 대응 기술

자동차는 해커들에게 단지 바퀴 달린 컴퓨터에 불과하며 사고 발생 시 피해 규모는 매우 크지만 상대적으로 대응책 마련이 매우 미흡하여 공격 가능성이 매우 높은 목표가 될 수 있다. OBD, ECU 통신 등을 이용한 차량 해킹으로 고의적 급발진을 유도하거나, 급제동, 임의 불법 조작 등이 차량 내부 통신망에 대한 해킹 공격을 통해 발생될 수 있음이 이미 다양한 사례를 통해 입증이 되었다. 미국 샌디에이고 대학과 워싱턴 대학 연구진에 의한 주행 차량 해킹 성공 사례, 국내에서 개최되었던 자동차 내부 네트워크의 취약점을 이용한 해킹 시연회 등의 사례에서와 같이 더 이상 자동차는 해킹에 안전하다고 할 수 없는 상황이 되었다.

주요 선진 자동차 업계는 해킹 문제에 대한 심각성을 인식하고 다양한 대응 방안을 내놓고 있다. 포드사에서는 제동장치 제어와 인터넷 접속을 담당하는 네트워크를 구분해 사이버 공격을 받더라도 차량 운행에 지장이 없도록 하고 있으며, 도요타사, 크라이슬러사 등에서는 앱을 통한 바이러스 침입을 막기 위해 자사 전용 앱스토어만 이용하도록 하고 있다. 보쉬사는 차량 안전을 위한 보안 전문업체를 인수하는 등 자동차 업계에서도 차량 안전을 위해 사이버보안대책 수립에 관심이 증가하고 있는 상황이다.

이와 같이 주요 선진 업체를 중심으로 자동차 해킹에 대한 대응책이 마련되고 있으므로, 자동차 융합보안시장 창출을 선점할 수 있도록 기 보유하고 있는 시스템 보안 및 네트워크 보안 기술을 기반으로 커넥티드카 도래를 고려하여, OBD 포트, CD, 셀룰러, 블루투스 등 다양한 접속 통로를 통해 웜 바이러스나 트로이 목마가 차량으로 옮겨질 수 있음이 증명되었듯이, 임베디드 차량 환경에 적합한 해킹 대응 기술을 개발할 필요가 있다.

3. Mass Transit 중심 보안 기술

미국에서 발생되었던 버스 연료탱크를 이용한 테러 시도와 같이 고속 및 시내외 버스 등 대형 대중교통에 대한 사이버 공격이나 물리적 위협이 발생될 경우 대형 인명피해가 발생될 수 있으므로 집중적인 보안대책 수립이 필요하다. 미국의 경우 버스를 비롯한 지하철, 기차, 항공기 등 mass transit에 대한 테러 대책을 마련하고 있으며, 중국에서는 공항 등에서 사용하는 보안 검색기를 지하철에서 사용하여 테러 발생을 미연에 방지하고 있다. Mass transit에 대한 보안대책은 사이버보안뿐 아니라 물리보안 기술까지 적용하여 대형 사고 발생을 방지할 수 있는 융합형 보안 기술 개발이 필요하다.

4. 블랙박스 사생활 보호기술

택시 등 상용차량용 블랙박스는 전방 영상뿐 아니라 차량 내부의 영상과 음성까지 기록하는 2채널 이상의 블랙박스를 장착하고 있다. 택시 내부의 영상 및 음성 촬영은 승객들의 전화 통화부터 사적인 대화 및 무의식

중에 행동하는 개인 습관까지 기록할 수 있다. 따라서 블랙박스에 저장된 데이터가 인터넷에 유출되거나 협박 도구로 사용될 수 있는 부작용이 발생할 수 있다. 최근 한 정치인이 택시 안에서 나눈 농도 짙은 대화가 저장된 블랙박스 영상이 외부로 공개돼 이슈화가 되었던 사례와 같이 블랙박스의 사생활 침해문제 해결을 위한 기술적인 보안대책 마련이 필요하다. 구 국토해양부에서는 사생활 보장을 위해 실내 영상 촬영을 하지 못하도록 권고하고 있으나, 버스 및 택시 등 상용차량 업체에서는 운행 중 발생하는 분쟁의 시시비비를 가리기 위해 실내 촬영을 강력히 요구하고 있는 상황이다.

상용차량뿐 아니라 개인 차량에 사용되는 블랙박스도 차량의 운행정보 및 운전자의 개인정보가 담긴다는 점에서 프라이버시 문제가 발생할 수 있다. 미국은 'California Assembly Bill 2133' 등과 같이 10개 주가 연이어 차량용 블랙박스와 관련한 사생활 보호법률을 제정하였으며, 일리노이 등 20개 주는 이와 유사한 법률 제정을 추진 중에 있다. 이들 법안들의 주요 내용은 블랙박스에 담긴 정보는 법원이 명령할 때만 공개할 수 있으며, 운전자와 차량 번호 등 신상 정보는 공개 대상에서 제외하는 등 프라이버시를 보호하면서도 차량용 블랙박스를 보급할 수 있는 법률적 조치들을 제안하고 있다. 국내에서도 '개인정보보호법'과 '택시 내 CCTV 설치 관련 개인정보보호 가이드라인' 등의 제도적 조치들이 진행되고 있으나, 개인 프라이버시 보호를 위해 필요한 기술적인 내용에 대해서는 아직 명시되지 않고 있다. 향후에는 현재 국제적으로 진행되는 법률과 시장에서 발생하는 프라이버시 보호 문제를 해결하기 위해서는 법률과 제도의 보완과 함께, 블랙박스에 저장되는 영상 데이터에 보안 기술과 지능형 영상인식 기술을 접목하여 실시간으로 사용자의 얼굴이나 신체의 일정 영역에 대하여 마스킹 기능을 적용하는 등의 프라이버시 보호 기술을 제공하는 지능형 블랙박스 제품 개발이 필요하다.

Ⅵ. 결론

ITS를 기반으로 한 지능형 교통체계 서비스 성공을 위해서는 보안 기술이 반드시 적용이 되어야 한다. 차량 및 교통 시스템에 대한 해킹은 더 이상 소설 속의 이야기가 아니고 실제로 생활 중에 발생될 수 있는 일이 되었다. 자동차 업계에서 보안 필요성을 인식하고 보안 대책을 수립해 나간다는 점이 그나마 다행이라고 생각이 되지만, 보안 특성상 사소한 한군데의 보안 취약점이 전체 서비스의 안전을 좌우할 수 있으므로 체계적이고 종합적인 접근이 반드시 이루어져야 할 것이다. 안전하고 쾌적한 이동수단을 기대하는 사용자들이 증가함에 따라 차량 및 교통 분야의 보안 기술 수준이 관련 제품 및 서비스의 시장 경쟁력을 좌우하는 핵심 요인이 될 수 밖에 없으므로 보안 기술 개발에 대한 꾸준한 관심이 필요하겠다.

용어해설

ITS 자동차 · 도로 분야에서의 ITS는 도로교통 시스템의 구성요소인 교통수단 및 시설에 첨단기술을 적용하여 교통운영 · 관리의 효율성을 극대화하고, 이용자 편의와 안전성을 제공하며, 연료 소모 및 CO2 배출량을 저감시키는 미래형 교통체계를 의미

약어 정리

DOT	Departments of Transportation
EDR	Event Data Recorder
ITS	Intelligent Transport System
IVN	In-Vehicle Networking
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Nomadic Device
WAVE	Wireless Access in Vehicular Environments

참고문헌

[1] 최병철, "EU 지능형 차량 프로젝트 소개," Automotive

Mag., 2007. 6.

[2] M. Wolf, A. Weimerskirch, and T.Wollinger, “State of the Art: Embedding Security in Vehicles,” EURASIP J. Embedded Syst., Article ID 74706, 2007.

[3] 황태욱, “IT융합 기반 V2X 차량 통신 기술개발 현황,” 방송통신전파저널, vol. 54, 2012. 10.

[4] 오현서, 박종현, “차량 통신 네트워크 기술 동향,” 전자통신동향분석, vol. 23, no. 5, 2008. 10.

[5] 이상우, 이병길, “차량 통신 보안 기술 동향,” 주간기술동향, vol. 1556, 2012. 7.