Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.2, Apr. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.2.411

IoT 관점에서의 차량 위협 탐지 방안*

곽 병 일,† 한 미 란, 강 아 름, 김 휘 강‡
고려대학교 정보보호대학원

A study on detection methodology of threat on cars from the viewpoint of IoT*

Byung Il Kwak,† Mi Ran Han, Ah Reum Kang, Huy Kang Kim‡
Graduate School of Information Security, Korea University

요 약

최근 빠르게 발전을 이룬 ICT (Information and Communications Technologies) 기술과 IoT (Internet of Things) 기술이 융합되어가고 있다. 그에 따라 ICT 환경에서 발생하였던 보안 위협들이 IoT 환경에서도 이어지고 있다. IoT의 사물로 간주되는 차량에 있어 보안 위협은 재산피해와 인명피해를 가져올 수 있다. 현재 차량 보안에 대한 대비는 미흡하고, 차량 자체에서 스스로 위협을 감지하고 대응하는 것에는 어려움이 존재하는 실정이다. 본 연구에서는 차량에서의 이상징후 탐지를 위한 의사결정 프레임워크를 제안하고, 이를 통해 IoT 관점에서 발생할 수 있는 차량 내 위협 요소들은 어떤 것이 있는지 알아보고자 한다. 차량을 대상으로 하는 공격에 대한 위협 요인과 위협 경로, 공격 형태 등을 인지하는 것은 자가 점검 기술과 디바이스 제어 공격에 대한 신속한 대처에 앞서 차량 보안 이슈를 해결하기 위한 전제가 될 것이다.

ABSTRACT

These days, a conversion of the fast-advancing ICT (Information and Communications Technologies) and the IoT (Internet of Things) has been in progress. However, these conversion Technology could lead to many of the security threat existing in the ICT environment. The security threats of car in the IoT environment could cause the property damage and casualty. There are the inadequate preparations for the car security and the difficulty of detection for the security threats by itself. In this paper, we proposed the decision-making framework for the anomaly detection and found out what are the threats of car in the IoT environment. The discrimination of the factor, path and type of threats from the attack against the car should take priority over the self-inspection and the swift handling of the attack on control system.

Keywords: IoT, Car Security, Hacking scenario, Data mining, Anomaly detection

I. 서 론

IoT (Internet of Things)는 각종 사물에 센서와 통신 기능을 내장하여 인터넷에 연결하는 기술을 의미한다[1]. 인터넷에 연결된 각종 사물과 사람 사이에서 발생하는 정보들의 상호작용으로 인해 사물과 사물, 사물과 사람 간에 통신할 수 있는 M2M의 개념이 사물은 물론, 현실과 가상세계의 정보들과 상호작용하는 개념으로 진화하였다. IoT에서의 사물은 가정에 있는 전자제품, 스마트폰 등과 같이 임베디드 시스템이 들어갈 수 있는 모든 제품을 의미 한다. IoT의 사

접수일(2015년 2월 12일), 수정일(2015년 4월 2일), 게재확정일(2015년 4월 2일)
* 이 논문은 삼성전자 미래기술육성센터의 지원을 받아 수행된 연구임 (과제번호 SRFC-TB1403-00)
† 주저자, kwacka12@korea.ac.kr
‡ 교신저자, cenda@korea.ac.kr(Corresponding author)

물들은 인터넷에 연결되어 통신이 가능하며, 센서를 통해 외부 환경으로부터 데이터들을 수집하고 교환한다[2]. M2M에서 사물인터넷으로의 진화는 일상생활에 혁신과 편리성을 가져다 줄 것이다.

세계적으로 IoT 시장의 규모가 크게 증가하고 있다. 해외 정보통신 분야의 시장조사 업체인 가트너(Gartner)에서는 2013년에 IoT 기기가 약 30억대에 도달했고, 2015년까지 약 49억대에 이를 것이며, 2020년에는 약 250억 대에 도달할 것이라고 밝혔다. 또한 IoT 기술을 활용한 경제적인 파급 효과도 커지면서 2015년 IoT 서비스 총 지출액이 약 695억 달러, 2020년에는 2,630억 달러에 이를 것으로 전망하고 있다. IoT 기기는 향후 제조, 공공사업, 교통 분야들이 IoT 기기 활용에 있어 두드러질 것이다[3].

텔레매틱스(Telematics)는 통신(TeleCommunication)과 정보과학(Informatics)의 합성어로, 카 내비게이션에 뉴스, 게임, 주식, 금융거래가 가능한 기능을 넣어 차 안에서 인터넷에 접속해 호텔 예약 및 영화 시청이 가능한 시스템을 의미한다[4]. 텔레매틱스와 IoT의 개념이 합쳐지며 커넥티드 카(Connected Car) 또는 스마트 카(Smart Car)와 같은 개념으로 확장되고 있다. 커넥티드 카 환경에서는 차량이 인터넷에 연결된 하나의 사물로 간주될 수 있다. 또한 차량안의 ECU (Electronic Control Unit)도 인터넷에 연결된 사물로 간주될 수 있다.

지금까지 자동차 해킹은 OBD (On-Board Diagnostic) 단자를 통한 직접적인 물리 접근 공격만 가능했었다. 그러나 Bluetooth와 Wi-Fi 등 인터넷과의 연결성이 확대된 IoT 차량은 공격자에 의한 원격 제어가 가능하고, Media Player를 통한 간접적인 물리 공격도 가능하며, 운전자 및 동승자의 안전과 사생활 노출의 위험성이 있다. 현재 차량 보안에 대한 대비는 상당히 미흡한 실정이고, 차량 자체에서 발생 가능한 위협도 대응하기 어려운 상황이다[5].

2009년에 워싱턴 대학과 캘리포니아 대학 연구팀이 공항 활주로에서 테스트용으로 자동차의 전자 브레이크 시스템을 해킹하였다. 이 실험에서 운전자가 브레이크를 밟아도 브레이크가 말을 듣지 않는 상황이 발생했다[6]. 2010년 3월에는 텍사스 오스틴에서 100대 이상의 자동차 엔진에 시동이 걸리지 않거나, 경적이 계속 울리는 사건이 발생했다. 이 사건은 해커가 스마트 키를 이용하여 자동차의 도난 방지 기능을 원격으로 조작하여 해킹을 시도한 것이다[7]. 또한, 2011년 USENIX 컨퍼런스에서는 캘리포니아 대학의 연구팀이 실제 차량의 텔레매틱스 장비를 해킹하여 차량을 제어하는 시연을 하였으며[8], 2012년 영국의 차량 절도단은 OBD 단자를 이용해 리모콘 열쇠를 복제하여 3분 만에 BMW를 해킹하기도 하였다[9].

이처럼 IoT 관점에서의 차량 보안 위협은 ICT 기술의 접목으로 심각성과 피해 범위가 점점 더 커지고 있다. 차량 IoT의 보안 위협에 대비하기 위해서는 차량 IoT에 대한 보안 위협 요소가 어떤 것이 있는지 살펴보고, 위협 요소의 성격에 따라 탐지할 수 있는 방안을 마련해야 한다.

본 논문에서는 차량 IoT 환경에 적합한 위협 탐지 프레임워크를 제안하였으며, 차량 내 발생 가능한 위협 모델 및 요소를 제안하였다. 2장에서는 IoT 환경을 위한 보안기술과 차량 네트워크 정의에 대해서 설명하고, 3장에서는 차량 위협 탐지를 위한 전체적인 보안 프레임워크를 설명하였다. 4장에서는 차량 내 전송 및 수집 가능한 데이터와 통신 네트워크를 통한 차량 제어 시스템 공격 시나리오를 제시하고 5장에서 결론을 맺는다.

II. 관련 연구

자동차에서 추출 가능한 첫 번째 데이터로 자동차 내부의 CAN (Controller Area Network) 버스 데이터가 있다. Taylor, Phillip, et al. 은 차량의 CAN 버스 데이터를 수집하여 도로 종류, 신호등 종류 및 차선 종류에 대한 분류 문제 해결에 사용하였다[10].

추출 가능한 두 번째 데이터는 자동차에 내장된 센서를 통해 추출하는 데이터가 있다. Qichang, et al. 은 운전자의 피로도를 판단하기 위해서 운전 핸들의 각도를 데이터로 사용하였다. 가상 주행에서 운전자의 차선 이탈과 자동차 핸들 각도의 상관계수를 통해 서로의 관계성을 밝혔다. 가상 주행에서 운전자의 뇌전도 데이터와 차량 핸들 각도 데이터를 Bayesian Network에 적용하여 운전자의 피로도를 예측하였다[11]. McCall, et. al. 은 운전자 보조 시스템의 제동 동작 식별 및 지원을 위해 여러 운전자들을 대상으로 브레이크 페달 압력, 액셀 페달 위치, 핸들 각도, 가속도, 차량 회전 속도, 바퀴 속도 등의 정보를 수집하였다. 수집한 정보를 통해 운전자의 행동 패턴을 추출하였고 운전자 행동 예측 시스템을 제안하였다[12].

추출 가능한 세 번째 데이터는 운전자에 대한 데이터이다. Cuong, et al. 은 운전자의 페달 에러가 발

생하는 원인과 페달 에러의 완화 방법을 제안하였다. 페달 에러의 원인을 알아내기 위해 차량에 내장시킨 센서와 비디오 녹화 및 CAN 버스 데이터, 운전자의 나이, 성별, 시각 및 청각 정보, 자동차 업무 시퀀스를 사용하였다[13].

III. 차량 보안

3.1 IoT 환경을 위한 보안기술

기존 ICT 환경이 금융, 가전, 의료, 자동차 등 다양한 산업 영역과 결합되면서 보안의 필요성이 증가하고 있다. IoT 환경에서는 기존 ICT 환경 보다 더 많은 데이터가 발생하기 때문에 많은 저장 공간이 필요하다. 또한 네트워크 계층에서 대규모 서비스를 위한 이상징후 탐지 방법이 존재하지 않는다. 따라서 기존 ICT 환경에서의 보안기술을 그대로 IoT 환경에 접목하는 것은 비효율적이며, IoT 환경에 적합한 보안 기술의 고려가 필요하다.

국내에서는 ETRI에서 WAVE (Wireless Access in Vehicle Environment) 기반 멀티 홉 방식의 차량통신 기술에 관한 개발을 진행하였으나 해당 기술은 WAVE 내에서 구성되는 통신환경 구축을 연구 중점으로 두고 있고 보안 기술 개발이 주된 목표가 아니다[14]. 국외에서는 유럽을 중심으로 EVITA 프로젝트를 진행하여 차량 내부네트워크 보안을 위한 HSM (Hardware Security Module)을 제작하였지만, ECU의 암호 알고리즘의 성능 연구에만 치중하고 새로운 환경(IoT)을 위한 보안 프로토콜 및 이상징후 판단 알고리즘에 대한 연구가 미흡한 상황이다[15].

지능형 차량의 통신환경은 기존의 ICT 네트워크 환경과는 차이가 있다. 차량 IoT 디바이스들의 대량 증가로 디바이스들을 모니터링하고 분석하기 위해서는 빅데이터 분석 기술이 필요하며, 차량 IoT 환경에서 알려지지 않은 위협에 대한 전반적인 위협 대응 모델 연구도 필요하다. PC에서 사용하는 시그니쳐 기반 탐지 기법은 스마트 차량의 스펙이 기존 PC와 비슷한 경우에만 적용이 가능하다. 그렇기 때문에 PC가 아닌 스마트 차량을 대상으로 악성코드 탐지를 할 경우 기존 시그니쳐 기반 탐지 기법은 적용하기 힘들다. 또한 시간 제약 사항이 보다 엄격한 차량의 IoT 환경에서 기존의 정적인 정보를 기반으로 하는 이상징후 탐지기술의 적용은 한계가 있다.

3.2 IoT 관점에서의 차량 네트워크 정의

ICT 기술의 적용으로 인해 차량 시스템은 IoT 환경으로 변모해 가는 과정에 있다. Fig.1.은 차량의 네트워크를 Macro-view와 Micro-view의 관점에서 나타낸 것이다. Fig.1.의 Ⓐ는 차량 내부 네트워크로 차량 환경을 제어하는 수많은 저(低)사양 디바이스(ECU)들이 LIN (Local Interconnect Network), CAN, FlexRay와 같은 전용망으로 묶여있다. 기존 차량 네트워크 보안 연구는 Ⓑ의 차량 진단 포트(OBD)를 통한 취약점 분석 및 대응 방안만을 주로 다루었다. IoT 환경에서는 Ⓒ처럼 여러 연결점을 가지는 텔레매틱스 디바이스를 통해 다양한 텔레매틱스/인포테인먼트 서비스와 차량 내부로의 다양한 접근 방법이 제공될 것이다. Ⓓ에서 볼 수 있듯이 차량은 온라인으로 연결되어 다양한 텔레매틱스와 인포테인먼트 서비스를 받게 되기 때문에 단지 환경 내부에서만의 대응방법이나 정적 보안과 같은 방식은 악의적인 공격 대응에 한계가 있다. 따라서 변모해가는 차량 IoT 환경에 대한 보안은 차량 내부에서의 대응방법과 외부에서의 대응방법이 함께 고려되어야 한다.

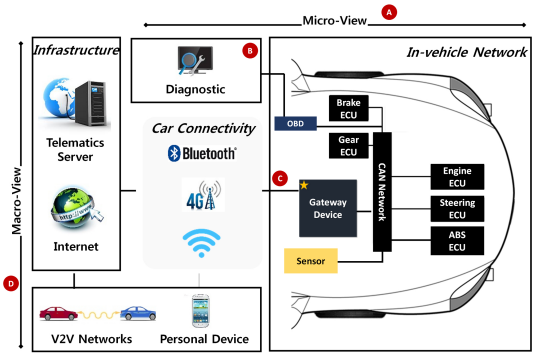

Fig. 1. Car network of the Micro & Macro view

IV. IoT 차량 위협 탐지

4.1 차량 위협 탐지를 위한 프레임워크

차량 IoT는 LIN, CAN, FlexRay와 같이 다양한 네트워크 구조를 가지며, 차량 내 디바이스마다 성능 차이가 존재한다. 따라서 기존 ICT 환경의 접목으로는 차량에서 발생하는 대규모의 혼합된 트래픽 처리에 한계가 있다. 이러한 한계를 보완하기 위해서 차

량 IoT 환경에 적절한 네트워크 구조와 디바이스 성능에 영향을 받지 않는 공격 탐지 기술이 필요하다.

Fig.2.는 본 논문에서 새롭게 제안한 프레임워크로 대규모 트래픽 처리와 신속한 공격 탐지가 가능한 DSE (Decision Support Engine)를 나타낸 것이다. 차량 내부에 존재하는 IoT 디바이스들은 낮은 성능으로 인해 자체적인 점검에 한계가 있다. 하지만 외부 시설에 존재하는 DSE는 대량의 상태 정보들을 신속하게 분석하기 때문에 IoT 디바이스의 점검을 가능하게 한다.

DSE는 Device Status Analyzer와 Device Maintenance Manager, Device Status DB, Decision Engine Core로 구성된다. Device Status Analyzer는 데이터 마이닝과 자기유사도를 통해 이상징후 탐지와 상태 점검을 수행하는 모듈이다. Device Maintenance Manager는 Device Status Analyzer에서 분석한 디바이스들의 상태 정보를 유지 및 관리하는 모듈이며, Device Status DB는 디바이스들의 상태 정보를 저장하는 장소이다. Decision Engine Core는 DSE에 있는 Device Status Analyzer, Device Maintenance Manager, Device Status DB 각각의 기능들을 통해서 의사결정을 내려주는 DSE의 핵심부분이다.

Security Monitor는 N-IDS (Network based Intrusion Detection System)와 H-IDS (Host based Intrusion Detection System)로 구성된다. N-IDS는 네트워크 단에서 비정상 트래픽을 실시간으로 탐지할 수 있는 시스템이다. H-IDS는 호스트 단에서 시스템 이벤트 로그 분석을 통해 내부 침입 행위를 탐지할 수 있는 시스템이다.

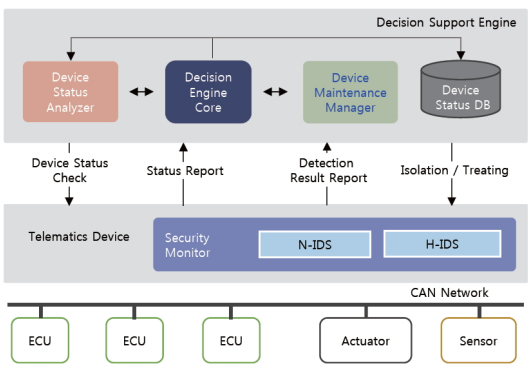

Fig. 2. Decision Support Engine Framework

Fig.2.에서 Security Monitor가 수집한 디바이스 상태 정보는 Telematics Device를 통해 DSE에 전달된다. Device Status Analyzer는 데이터 마이닝 알고리즘을 적용하여 전달된 상태 정보들을 분석한다. Device Status Analyzer는 분석한 정보들을 정상 및 비정상 상태 정보로 분류하여 Device Status DB에 저장하고, 데이터 마이닝 수행 시 Training, Testing, Validation 단계를 통해 Detection rule을 생성하고 업데이트한다. Security Monitor는 업데이트된 Detection rule을 통해 차량 IoT 디바이스에서 발생하는 시스템 이벤트와 네트워크 트래픽에 대한 비정상 트래픽을 탐지한다. Security Monitor는 통신이 가능한 경우 실시간으로 Rule의 업데이트를 수행하고, 외부 네트워크 단으로부터 침입 행위 발생 시 N-IDS와 H-IDS를 통해 침입 행위를 탐지한다. 통신이 불가능한 경우 외부 네트워크 단으로부터 침입 행위가 일어날 수 없으므로 경량화된 H-IDS를 통해 시스템 내부 침입 행위를 탐지한다. 통신 및 처리 지연이 생길 경우 기존에 유지하고 있는 Rule을 통해 침입 행위를 탐지하고 지연 문제가 해결 되었을 경우 정상적으로 업데이트와 함께 침입 행위를 탐지한다.

4.2 Macro-view Security

앞서 Fig.1.에서 제안한 차량 네트워크의 두 가지 관점 중 Macro-view는 서버와 주고받는 디바이스의 상태 정보를 분석하여 차량 외부로부터 발생하는 공격이나 이상징후를 탐지한다. Macro-view의 관점에서는 각각의 차량을 하나의 사물로 간주할 수 있다. DSE로 전달된 많은 차량들의 디바이스 상태 정보는 효율적으로 기록되고, DSE는 이 정보를 분석하여 신뢰할 수 있는 의사결정을 하여 공격이나 이상징후를 탐지한다.

Macro-view단에서는 원격 제어를 통해 차량안의 각 디바이스들이 운전자에 대한 직접적인 피해를 입히는 것뿐만이 아닌 차량 외부에서 발생 가능한 교통사고나 테러와 같은 위험을 빠르게 탐지하여 신속한 대응이 필요하다.

4.3 Micro-view Security

Micro-view는 차량 내부의 시스템과 CAN 네트

워크에서 발생하는 정보들을 분석하여 차량 내부에서 공격이나 이상징후를 탐지한다. Micro-view의 관점에서 ECU는 텔레매틱스 디바이스와 같이 IoT의 사물로 간주할 수 있다. 차량 내부에 들어가는 ECU는 디바이스의 낮은 H/W 성능으로 인해 기존 보안 솔루션의 적용이 어렵다. 그렇기 때문에 차량 IoT 환경에 적합하고 성능 저하를 최소화할 수 있는 경량화된 IDS가 필요하다. 차량 내부의 경량화된 IDS는 텔레매틱스 디바이스에 대한 공격이나 이상징후를 탐지한다.

Micro-view단에서는 원격에서 제어하기 위해 차량 내부의 텔레매틱스 디바이스들에 대한 공격을 탐지하고 빠르게 대응하여 운전자와 운전자 차량을 외부 원격 제어로부터 보호하는 것이 필요하다.

V. 차량 위협 모델

최근 스마트폰을 이용한 차량 운전자에게 편의성을 제공하는 서비스가 활발하다. 안드로이드 마켓에서 제공하는 차량 진단 어플리케이션은 OBD-2 단자와 스마트 폰을 유/무선으로 연결하여 사용자가 차량의 상태를 확인 가능하도록 해준다. 그러나 공격자는 이런 어플리케이션을 통해 LIN이나 CAN과 같은 차량 통신 네트워크에 메시지를 생산하는 악의적인 목적의 차량 진단용 어플리케이션을 배포할 수 있다. 공격자는 배포된 어플리케이션을 통해서 자동차를 원격 제어하거나, 과도하게 메시지 생성함으로써 차량 내 버스 네트워크를 마비시킬 수 있다.

5.1 차량 전송 데이터 및 수집 가능 데이터

최근 스마트폰 사용의 대중화에 따라 스마트폰 어플리케이션과 결합해 다양한 서비스를 제공하는 텔레매틱스가 주목받고 있다. Table 1.은 현대 자동차에서 서비스하는 Blue Link와 GM대우에서 서비스하는 OnStar로 두 가지 텔레매틱스 서비스에서 전송되는 정보를 정리한 것이다.

Table 1. The transmitted information from telematics services

Telematics services	The transmitted information
Blue Link	Car starting, Temperature inside vehicle, Door status, Destination information, Airbag status, SOS request, Accelerator status, Departure, Anomaly detection, Engine oil status, Filter status, Driving information, Driving speed, Sudden unintended acceleration , Car idling time
GM OnStar	Vehicle crash information, SOS request, Location information, Departure, Destination, Engine, Directional control information, Airbag status, Exhaust gas, Brake information, OnStar vehicle status, Fuel level, Tire pressure, Hands-free phone list, Remote command, Location information

Table 2.는 Table 1.의 수집 가능한 정보 중 안드로이드 서비스 해킹을 통해 악용될 수 있는 개인 정보들을 서비스 형태에 따라 정리하였다.

Table 2. The collected information via hacking

Services	The collected information
Financial app	Certificate, Account number, Transactional information, Regular transactional account, etc.
Navigation	Search location List, Vehicle route, Departure, Destination, etc.
Messenger	Friend list, Message contents, Exchange file, etc.
Car black box	Recording video, Recording voice, etc.

5.2 차량내 오작동 및 이상징후 탐지 방안

IoT 차량은 외부로부터 공격이 들어오는 경우 CAN 네트워크 통신의 이상징후를 통해 탐지가 가능하다. 주행 중인 차량의 CAN 버스 안에는 전송 메시지들이 존재한다. 정상적인 차량 주행 시 CAN 메시지들의 빈도수 평균과 표준편차를 구할 수 있다. CAN 네트워크를 통한 메시지 공격은 CAN 네트워크 외부에서 내부로 메시지를 주입해야 하므로 메시지들의 빈도수가 정상분포에서 벗어난다. 메시지의 빈도수가 정상분포를 벗어날 경우 이상점이 발생하기 때문에 주행 중인 상황에서 공격 여부를 탐지할 수 있다.

차량 내 공격이 아닌 기기상의 문제로 기능 오작동이 일어날 수 있다. 차량 기능의 오작동인 경우 차량 내부에 설치된 센서를 통해 탐지할 수 있다. 예를 들어, 차량 내부 액셀에 내장된 센서가 액셀 페달의 상태 정보를 수집한다. 추가로 CAN 네트워크에서 액셀 페달과 관련성 있는 메시지의 빈도수를 검사한다. 페달의 상태 정보와 메시지의 빈도수 체크를 통해 현재 오작동이 기기상 문제인지 공격으로 인해 발생한 것인지를 탐지할 수 있다.

5.3 차량 제어 공격 시나리오 및 탐지 방안

5.3.1 차량 속도 제어 오작동

5.3.1.1 공격 시나리오

Fig.3.은 차량 속도 제어 오작동에 관한 공격 시나리오를 순서도로 나타낸 것이다. 공격자는 정지 상태인 차량 또는 주행 중인 차량을 원격 제어하여 급발진이나 급감속 또는 급후진 시킨다. 급발진, 급감속 및 급후진을 통해 운전자 및 차량 탑승자에게 직접적인 피해를 입히거나 교통사고를 유발하고, 또한 차량 외부에 있는 사람이나 차량에게도 큰 피해를 입힐 수 있다. 차량주행중인 경우 급가속 및 급감속이 발생할 경우 대형 교통사고가 발생할 수 있다.

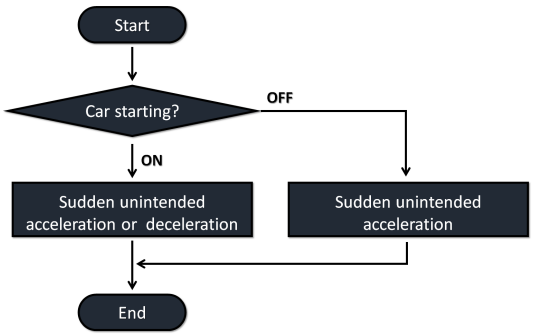

Fig.3. Flowchart of speed control malfunction scenario

5.3.1.2 공격 탐지 방안

차량 속도 제어 오작동 시나리오는 시동 상태에 대한 정보와 액셀 상태, 브레이크 상태, 가속도 등과 같은 속도와 관련된 정보를 통해 탐지한다.

Table 3. The information for IoT car speed control malfunction detection

Information	Range
Car starting	1(ON), 0(OFF)
Accelerator status	1(ON), 0(OFF)
Brake status	1(ON), 0(OFF)
Acceleration	(-)50 ~ (+)50

Table 3.은 차량 속도 제어 오작동을 탐지하기 위한 정보들을 나타낸 것이다. 차량이 주행 중일 경우 시동 상태의 정보는 '1', 정지 상태일 경우에는 '0'으로 나타난다. 차량이 속도를 높이기 위해 액셀을 밟았을 때 '1', 액셀을 밟지 않았을 때 '0'으로 나타난다. 차량의 브레이크를 밟았을 때 '1', 밟지 않았을 때 '0'으로 나타난다. 가속도가 높을 경우 급발진 또는 급가속으로 볼 수 있고, 가속도가 낮을 경우에는 급후진 또는 급감속으로 볼 수 있다.

공격에 대한 탐지는 Fig.3.의 공격 시나리오 순서도를 따른다. Table 3.의 정보들을 통해 차량의 시동 상태, 액셀 상태, 브레이크 상태, 가속도를 통해서 차량의 속도가 급격하게 증가 또는 감소시킬 때 탐지가 가능하다. 차량의 시동 상태를 통해 주행 여부를 확인한다. 주행 중인 경우는 차량의 속도가 급격하게 증가하거나 급격하게 감소하는지를 확인하고 차량이 정지 상태인 경우는 차량이 급발진 하는지를 확인하여 탐지한다.

5.3.2 차량 방향 제어 오작동

5.3.2.1 공격 시나리오

Fig.4.는 차량 방향 제어 오작동에 관한 공격 시나리오를 순서도로 나타낸 것이다. 공격자는 고속 주행 중인 차량의 방향을 원격으로 제어하여 오작동을 일으킨다. 차량 방향 제어 오작동을 통해 운전자 및 차량 내부에 있는 탑승자에 대한 직접적인 피해를 입히거나 교통사고를 유발한다. 공격자는 차량이 고속 주행(120km 이상)인지를 확인한다. 고속 주행 중일 경우 방향 제어를 통해서 차량의 방향을 오른쪽이나 왼쪽으로 급격하게 변화시켜 차량의 전복 사고를 유발한다. 또한 차량이나 사람이 많이 모여 있는 곳에서는 큰 인명피해와 재산피해를 입힐 수 있다.

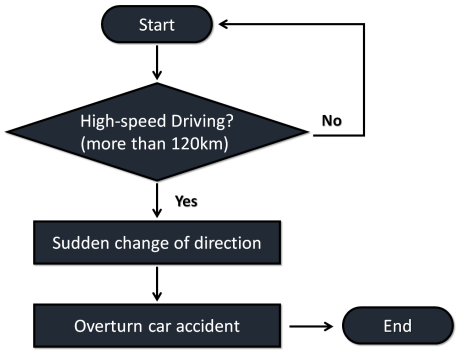

Fig.4. Flowchart of direction control malfunction scenario

5.3.2.2 공격 탐지 방안

차량 방향 제어 오작동 시나리오는 주행속도, 방향 제어와 관련된 정보를 통해 탐지한다. Table 4.는 차량 속도 제어 오작동을 탐지하기 위한 정보들을 나타낸 것이다. 차량의 주행속도 정보는 '0' ~ '250' 사이의 값으로 나타난다. 방향 제어는 '(-)55' ~ '(+)55' 사이의 값으로 나타난다.

공격에 대한 탐지는 Fig.4.의 공격 시나리오 순서도를 따른다. 주행 시 일정속도마다 방향 제어 각도의 범위가 한정되어 있으므로 주행속도가 높고, 방향의 변화폭이 정상 범위 '(-)55 ~ (+)55'를 넘어가게 되면 이상행위로 간주한다. 또한, 시간 정보를 함께 계산하여, 정상 범위가 일정시간 이상 지속될 경우 이상행위로 간주할 수 있다.

Table 4. The information for IoT car direction control malfunction detection

Information	Range
Driving speed	0~250
Directional control	(-)50~(+)50

5.3.3 에어백 오작동

5.3.3.1 공격 시나리오

Fig.5.는 에어백 오작동에 관한 공격 시나리오를 순서도로 나타낸 것이다. 공격자는 주행 중인 차량의 에어백을 원격으로 제어하여 오작동을 일으킨다. 공격자는 에어백 오작동을 일으켜 운전자에게 직접적인 피해를 입히거나 교통사고를 유발한다. 차량의 원격 제어를 통해서 차량 주행속도, 충돌여부와 같은 운행정보를 획득한 공격자는 획득한 정보를 통해 고속 주행인지 커브길 주행 중인지 확인한다. 차량이 고속 주행이거나 커브길 주행 중일 경우 공격자는 에어백을 오작동 시키고 에어백 오작동으로 인한 충격과 시야 방해로 빠른 대응을 하지 못하도록 하여 교통사고를 유발한다.

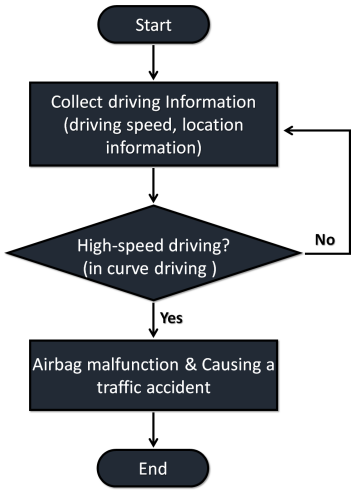

Fig.5. Flowchart of airbag malfunction scenario

5.3.3.2 공격 탐지 방안

에어백 오작동 시나리오를 수행할 방법은 주행속도, 방향 제어와 관련된 정보를 통해서 탐지한다. Table 5.는 에어백 오작동을 탐지하기 위한 정보를 나타낸 것이다. 에어백 전개 여부는 에어백이 전개되어 있을 경우 '1', 전개 되지 않았을 경우 '0'으로 나타난다. 위치정보는 위도, 경도, 고도에 따라 '0' ~ '360' 사이의 값으로 나타내며, 차량의 주행속도 정보는 '0' ~ '250' 사이의 값으로 나타난다. 충돌여부는 충돌했을 경우 '1', 충돌하지 않았을 경우 '0'으로 나타난다. 브레이크 상태는 브레이크를 밟았을 때 '1', 밟지 않았을 때 '0'으로 나타내며, 액셀 상태는 액셀을 밟았을 때 '1', 액셀을 밟지 않았을 때 '0'으로 나타난다. 기어 상태는 상태에 따라 '0' ~ '8' 사이의 값으로 나타난다.

공격에 대한 탐지는 Fig.5.의 공격 시나리오 순서도를 따른다. 차량의 주행속도와 위치정보, 브레이크 상태, 액셀 상태, 기어 상태와 같은 운행정보를 통해 고속 주행 중이거나 커브길에서 주행 중인지를 확인

Table 5. The information for IoT car air bag malfunction detection

Information	Range
Airbag status	1(ON), 0(OFF)
Location(latitude, longitude, altitude)	0~360
Driving speed	0~250
Car collision	1(ON), 0(OFF)
Brake status	1(ON), 0(OFF)
Accelerator status	1(ON), 0(OFF)
Gear position	0~8 (1~6 level, 0:N, 7:R, 8:P)

한다. 이 때 충돌여부와 에어백 전개 여부를 확인할 수 있는데, 충돌여부가 OFF인 상태에서 에어백 전개 여부가 ON으로 되어 있는지를 확인을 통해 공격이나 이상징후가 있는지를 탐지할 수 있다.

5.3.4 시야 확보 방해 사고

5.3.4.1 공격 시나리오

Fig.6.은 시야 확보 방해 사고에 관한 공격 시나리오를 순서도로 나타낸 것이다. 공격자는 비오는 날 야간에 고속 주행 중인 차량을 원격 제어하여 차량 내부 온도를 상승시켜 습기가 생성되도록 유발시킨다. 공격자는 차량의 와이퍼 작동을 일시 정지시키고, 사이드 미러를 강제로 접어 교통사고를 유발시킬 수 있다.

5.3.4.2 공격 탐지 방안

시야 확보 방해 사고 시나리오로 인한 결과 정보는 와이퍼, 사이드 미러, 유리 열선 상태, 히터, 에어컨 상태, 전조등과 관련된 정보를 통해서 탐지가 가능하다.

Table 6.은 시야 확보 방해 사고를 탐지하기 위한 정보들을 나타낸 것이다. 와이퍼는 작동 중일 경우 '1', 정지 상태에 있을 경우 '0'으로 나타난다. 사이드 미러는 펼쳐져 있을 때는 '1', 접혀 있을 때는 '0'으로 나타난다. 유리 열선 상태는 켜진 상태일 경우 '1', 꺼진 상태일 경우 '0'으로 나타난다. 히터는 켜진 상태일 경우 '1', 꺼진 상태일 경우 '0'으로 나타난다. 에어컨은 켜진 상태일 경우 '1', 꺼진 상태일

Table 6. The information for IoT visibility disturbance detection

Information	Range
Wiper	1(ON), 0(OFF)
Side mirror	1(ON), 0(OFF)
Heating wire status	1(ON), 0(OFF)
Heater	1(ON), 0(OFF)
Air conditioner status	1(ON), 0(OFF)
Headlight	1(ON), 0(OFF)

경우 '0'으로 나타난다. 전조등은 켜진 상태일 경우 '1', 꺼진 상태일 경우 '0'으로 나타난다.

공격에 대한 탐지는 Fig.6.의 공격 시나리오 순서도를 따른다. 비오는 날 고속 주행 여부를 확인하고 고속 주행일 경우 와이퍼, 전조등, 히터, 유리 열선, 에어컨의 사용 여부를 확인하여 공격이나 이상징후에 대해 탐지한다.

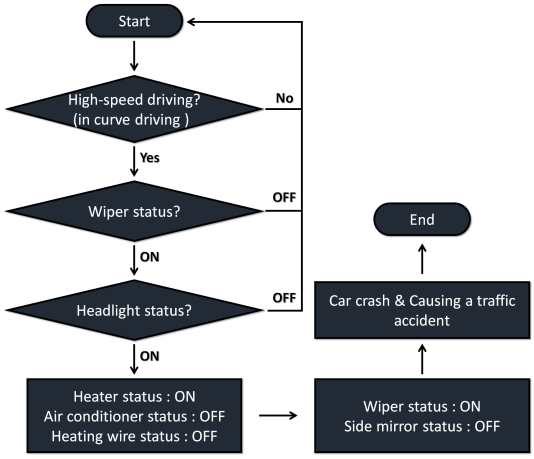

Fig.6. Flowchart of visibility disturbance scenario

5.4 공격 탐지 알고리즘

Fig. 7.은 차량 내 침입 탐지를 위한 알고리즘이다. CAN Message Collecting 모듈은 CAN 메시지를 수집하여 분석이 용이하도록 가공한다. Message structure checking 모듈은 이전 모듈에서 전달받은 메시지의 구조적인 이상 여부를 검사한다. CAN 메시지의 구조, 플래그 정보, ID 등 주행 중 나올 수 없는 메시지 포맷에 대해 검사한다. Attack message detecting 모듈은 탐지 이전 모듈에서 전달받은 메시지를 Rule 기반으로 탐지한다.

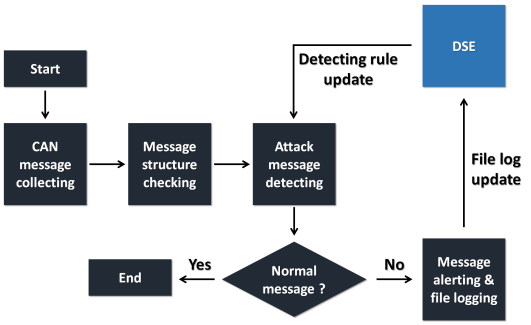

Fig. 7. Flowchart of detection for attack in vehicle

탐지 메시지가 비정상일 경우 Message alerting & file logging 모듈에서 이상징후 탐지 경고와 메시지 정보를 로그 파일로 남긴다. 비정상 메시지 관련 로그파일은 통신이 가능한 지역에서 실시간으로 DSE에 전송된다. DSE는 전송받은 로그 파일을 추가 분석하여 기존 Rule을 수정하거나 새로운 Rule을 생성한다. DSE는 차량이 통신 가능할 경우 생성한 Rule을 차량의 Attack message detecting 모듈로 업데이트 한다.

예를 들어 차량 방향 제어 오작동의 경우 CAN message collecting 모듈이 CAN message를 수집하면 가공 처리하여 Message structure checking 모듈로 전송한다. Message structure checking 모듈은 전송받은 메시지의 구조적인 이상 여부를 검사한다. 일반적인 주행 중 발생 가능한 CAN message ID인지 검사하고, 이후 데이터 영역의 비정상 여부를 확인한다. Message의 구조적 이상이 있을 경우 비정상으로 체크한 후 Attack message detecting 모듈로 전송한다. 기존에 가지고 있던 Rule과 DSE로부터 업데이트된 Rule을 통해 Attack message detecting 모듈은 메시지의 이상징후를 탐지한다. 이상징후 탐지 시 Rule은 공격 시나리오에서 탐지 방안으로 제시했던 주행속도, 방향 제어 정보를 이용한다. 방향 제어 오작동 탐지 Rule의 조건으로 주행속도가 120km 이상, 핸들의 각도가 (-)50 이하 또는 (+)50 이상을 설정한다. 추가로 CAN message의 탐지 시 CAN message의 빈도수 분포가 정상에서 벗어났는지를 검사한다. Rule에서 차량 방향 제어 오작동으로 탐지되고, CAN message의 빈도수가 정상 분포에서 벗어났다면 공격으로 분류한 후 경고 메시지와 함께 Log file로 저장한다. 저장된 Log File은 통신이 가능한 경우 DSE로 전송하여 업데이트한다. 통신이 불가능한 경우 저장된 Log File을 계속해서 유지하고 통신 가능 지역에서 DSE로 전송하여 업데이트를 종료한다. DSE는 많은 차량으로부터 업데이트된 Log file들을 분석하여 탐지 가능한 Rule을 수정 및 생성한다. 새로운 Rule은 차량과 통신이 가능할 경우 차량의 Attack message detecting 모듈에 업데이트한다.

제시한 차량 방향 제어 오작동 탐지 Rule은 기본 Rule 이지만 상황에 맞춰 여러 조건들을 추가할 수 있다. 현재 차량의 GPS정보, 차량의 경사면 각도, 전조등의 사용 유무 등 공격 탐지에 도움이 될 수 있는 여러 조건들을 추가한다면 공격들을 더 정확하게 탐지할 수 있다.

VI. 결 론

IoT 차량의 보안 위협은 운전자와 동승자뿐만 아니라 차량 외부에 있는 사람들에게까지 큰 인명피해를 입힐 수 있다. 급격히 발전하고 진화하고 있는 IoT 환경에서, 자동차를 보다 안전하고 편리하게 사용하기 위해서는 무엇보다 보안성 확보가 전제되어야 한다.

본 논문에서는 일반적인 PC환경에서 발생 가능한 공격 및 위협을 IoT 자동차 환경에서 탐지할 수 있는 프레임워크를 Macro-view 관점과 Micro-view 관점에서 제안하였다. 제안한 프레임워크는 자동차 내부에서 데이터를 추출하고 데이터마이닝을 이용하여 발생 가능한 공격 탐지한다. 또한 차량의 오작동 상황과 공격받고 있는 상황에 대한 탐지 방안을 제시하였다. 프레임워크에서 탐지 가능한 공격 시나리오 및 대응 방안을 살펴보았으며, 차량 IoT 환경에서 발생할 수 있는 위협 요소를 고려하여 차량 내에서 수집 가능한 데이터 정보를 제시하였다.

향후 연구에서는 앞서 제시했던 DSE 구축 방안을 통해 차량 내부에서 발생하는 정상 및 비정상 데이터를 센서 및 통신 모듈로부터 수집할 예정이다. 또한 비정상 정보의 유입을 이상징후로 탐지할 수 있는 알고리즘 설계와 Macro-view 및 Micro-view의 관점에서 이상징후 탐지를 수행할 예정이다.

References

[1] Wikipedia, http://en.wikipedia.org/wiki/Internet_of_Things

[2] Ho won Kim and Dong Kyue Kim "IoT technologies and security," Review of KIISC, 22(1), pp. 7-13, Feb. 2012

[3] Gartner, http://www.gartner.com/newsroom/id/2905717, Nov. 2014

[4] D.K.Jang, Y.U.Shin, and M.G.Choe, W.G.Nam, T.H.Hong, PCB/SMT/PACKAGE/DIGITAL Glossary, Publishing Gold, Apr. 2005

[5] Woo, Samuel, Hyo Jin Jo, and Dong Hoon Lee. "A practical wireless attack on the connected car and security protocol for in-vehicle can," Intelligent Transportation Systems, vol. 16, no. 2, pp. 993-1006, Sep. 2014

[6] TechHive, http://www.techhive.com/article/196293/car_hackers_can_kill_brakes_engine_and_more.html, May 2010

[7] WIRED, http://www.wired.com/2010/03/hacker-bricks-cars/, Mar. 2010

[8] S.Checkoway, D.McCoy, and B.Kantor, D.Anderson, H.Shacham, S.Savage, K.Koscher, A.Czeskis, F.Roesner, T.Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," USENIX conference on Security, Aug. 2011

[9] YouTube, https://www.youtube.com/watch?v=DshK4ZXPU9o, July 2012

[10] Taylor, P. Anand, S. S., and Griffiths, N., Adamu-Fika, F., Dunoyer, A., & Popham, T, "Road type classification through data mining," Proceedings of the 4th International Conference on Automotive User Interfaces and Interactive Vehicular Applications, pp. 233-240, Oct. 2012

[11] He, Qichang, Wei Li, and Xiumin Fan, "Estimation of driver's fatigue based on steering wheel angle," Engineering Psychology and Cognitive Ergonomics, pp. 145-155, July 2011

[12] McCall, Joel C., and Mohan M. Trivedi, "Human behavior based predictive brake assistance," Intelligent Vehicles Symposium, pp. 8-12, June 2006

[13] Tran, Cuong, and Anup Doshi, Mohan M. Trivedi, "Pedal error prediction by driver foot gesture analysis: A vision-based inquiry," Intelligent Vehicles Symposium (IV), pp. 577-582, June 2011

[14] Sang Woo Lee and Byung Gil Lee "Security technology trends for car network," National IT Industry Promotion Agency, The weekly publication for technology trends, 1556, pp. 12-36, July 2012

[15] Henniger, O., Ruddle, A., and Seudié, H., Weyl, B., Wolf, M., & Wollinger, "Securing vehicular on-board it systems: The evita project," VDI/VW Automotive Security Conference, Oct. 2009

〈저자소개〉

곽 병 일 (Byung Il Kwak) 일반회원
2013년 2월: 세종대학교 컴퓨터공학과 졸업
2013년 9월~현재: 고려대학교 정보보호학과 석·박사통합과정
〈관심분야〉 온라인게임 보안, 데이터 마이닝, 네트워크 보안, IoT 보안

한 미 란 (Mi Ran Han) 학생회원
2002년 2월: 동덕여자대학교 컴퓨터공학 학사
2014년 8월: 고려대학교 정보보호학과 석사
2014년 9월: 고려대학교 정보보호학과 박사과정
2004년 5월~2012년 3월: NEXON 해외사업 개발본부
〈관심분야〉 온라인게임 보안, 네트워크 보안, 데이터 마이닝, 시각화, 빅데이터, IoT 보안

강 아 름 (Ah Reum Kang) 학생회원
2006년 2월: 서울여자대학교 컴퓨터공학과 학사
2012년 2월: 고려대학교 정보보호학과 석사
2012년 3월~현재: 고려대학교 정보보호학과 박사과정
〈관심분야〉 온라인게임 보안, 소셜 네트워크, 데이터 마이닝, 네트워크 보안, IoT 보안

김 휘 강 (Huy Kang Kim), 종신회원
1998년 2월: KAIST 산업경영학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년 5월~2010년 2월: 엔씨소프트 정보보안실장, Technical Director
2010년 3월~2014년 12월: 고려대학교 정보보호대학원 조교수
2015년 1월~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌식