자율주행 자동차 통신기술 보안을 위한 Recovery Partition ECU 보안 솔루션 제안

박현성, 이상근, 서정택

순천향대학교 정보보호학과

A proposal of security communication technology self-driving car using Recovery Partition ECU

Hyeon-Seong Park, Sang-Geun Lee, Jung-Taek Seo

Department of Information Security Engineering, Soonchunhyang University.

요 약

최근 자동차업체들이 고수준의 자율주행기술을 선보이고 있다. 하지만 자율주행기술의 급격한 발전이 진행되는 것에 비하여 자율주행 시스템이 보안에 취약하다는 사례가 발견되고 있다. 대표적으로 자율주행 기술에 있어 차량 내부 ECU간 통신, 차량과 외부의 시스템 간의 통신이 악의적인 접근으로부터 도청 또는 위·변조가 가능하다는 문제점이 제기되고 있다. 이러한 문제점은 운전자와 그 주변 차량들에 막대한 피해를 입힐 수 있는 가능성이 크다. 본 논문에서는 이러한 문제점에 실시간으로 대응하여 통신 구간의 위·변조 공격에 대응할 수 있는 Recovery Partition ECU 보안 솔루션을 제안한다.

I. 서론

기존자동차는 운전자의 의사결정을 통해 목적지까지 운전을 했다. 하지만, 최근에는 자동차에 ICT 기술을 접목시켜, 인공지능이 사람을 대신하여 목적지까지 주행하는 자율주행시스템이 개발 및 적용되고 있다. 자율주행 환경에서 운행되는 자율주행 자동차는 사람의 의사결정을 반영하여 동작하지 않으므로 보안성 및 안전성이 더욱 중요하다. 최근 테슬라의 자율주행 자동차가 자율주행 모드로 운행하던 중 기계의 잘못된 감지 및 동작으로 인하여 인명사고가 발생하였다. 이 사고로 자율주행 자동차에 대한 안전성이 더욱 큰 이슈가 되고 있다. 또한, 자동차 내 통신 프로토콜인 CAN(Controller Area Network) Bus 취약점이 각종 해킹관련 컨퍼런스에 발표되면서 자동차 보안이 더욱 이슈가 되고 있다. 본 논문에서는 자율주행 자동차 운영 환경에 대한 보안성과 안전성을 확보하기 위하여 자동차 통신기술인 CAB Bus 통신방식을 보완하는 Recovery Partition ECU 보안 솔루션을 제안한다.

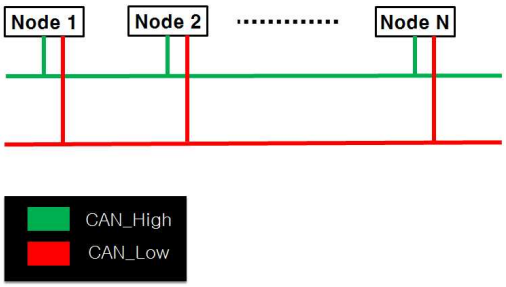
II. 자율주행 자동차 구조

2.1 ECU(Engine Control Unit)

ECU란 자동차 내부 장치들의 동작을 컴퓨터로 제어하는 전자제어 장치로서 센서로부터 입력되는 신호를 변환하는 입력 인터페이스, 정해진 순서에 따라 입력 데이터의 산술 연산 및 논리 연산을 행하는 컴퓨터(Micro Computer)와 산술 및 논리 연산 결과를 작동 신호로 전환하는 출력 인터페이스로 구성된다. 초기 ECU의 개발 목적은 엔진의 효율과 연비 향상을 위해 엔진을 정밀하게 제어하는 목적이었으나 이후 자동차에 각종 편의 장치, 안전장치 등을 탑재하기 위해 ECU의 활용 범위를 조향, 차체제어, 에어백 등 다양한 분야로 확대되었다[1].

2.2 CAN Bus

CAN Bus는 각각의 ECU의 통신을 위해 쓰이는 차량 제어 프로토콜이다. 이는 메시지 전송속도에 따라 High-Speed CAN과 Low-Speed CAN으로 나누어진다. High-Speed CAN방식은 빠른 속도를 요구하고 세밀한 제어를 하는 엔진이나 브레이크의 제어를 위해 사용되어지며, Low-Speed CAN방식은 High-Speed보다 조금 느린 방식이며 전조등이나 멀티미디어 기기의 조작과 같은 편의 사항을 제어하는데 사용된다[2].



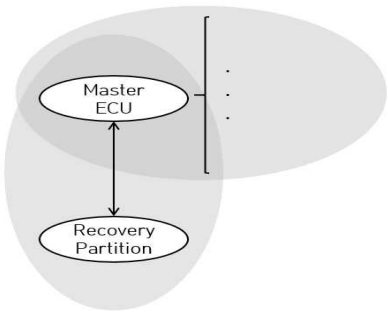
[그림 1] CAN BUS 구조

III. CAN Bus 보안 취약점

CAN Bus는 브로드캐스트 통신을 수행한다. 하지만 브로드캐스팅 통신임에도 불구하고 데이터 암호화나 인증기능을 전혀 제공하지 않는다. 그래서 공격자는 쉽게 모든 노드에서 메시지를 수신이 가능하며 공격자가 쉽게 메시지를 도청 및 변조가 가능하다[3]. 또한 ECU간의 인증 필드가 없는 부분을 이용하여 해커가 ECU의 제어영역까지 진입할 수 있는 것이 발견되었다. 최근에는 크라이슬러 지프를 해킹하여 원격 제어를 했다. 이러한 문제점 중 패킷의 위·변조의 취약점을 이용한 해킹에 실시간으로 대응하기 위해 본 논문에는 CAN Bus 취약점을 대응하기 위한 Recovery Partition을 제시한다[4,5].

IV. Recovery Partition ECU 제안

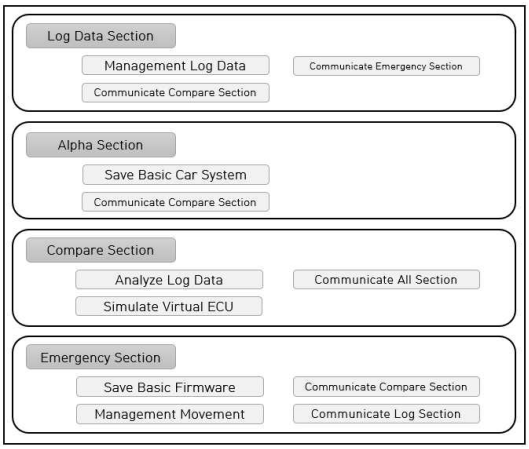
자율주행 자동차의 통신과 보안에 있어서 가장 근본적이고 핵심이 되는 부분인 중앙 ECU가 기존의 자율주행 자동차 내에 존재하고 추가로 각각의 ECU의 통신에 따른 오작동 및 해킹에 대응하기 위해 고안된 보안 ECU(Recovery Partition)를 추가한다. Recovery Partition은 기존의 중앙 ECU보다 관리자 권한이 높게 설정되어 긴급 시 차량 내의 모든 ECU를 통제할 수 있는 권한을 가진다. 또한 기존의 ECU와 양방향 통신을 하지 않고 Recovery Partition의 각각의 섹션마다 통신 방향이 다르며 외부의 접속을 차단한다. Recovery Partition을 [그림2]와 같이 설정한다.



[그림 2] Recovery Partition ECU 구조

V. Recovery Partition Section 제안

Recovery Partition은 [그림3]과 같이 4개의 동작 영역으로 이루어져 있으며 각각의 섹션을 Log Data 섹션(Log Section), Alpha ECU Recovery Data 섹션(Alpha Section), ECU Simulator & Compare 섹션(Compare Section) 마지막으로 Emergency 섹션(Emergency Section)이라고 한다.



[그림 3] Recovery Partition 섹션 구조

5.1 Log Data 섹션

Log Data 섹션은 실시간으로 차량 내 각각의 ECU끼리 주고받는 모든 패킷들을 수신한다. 그러나 단방향 통신만으로 중앙 ECU에서 오는 패킷을 수신한다. 그러므로 수신되었던 모든 데이터는 Log섹션이 직접적으로 Recovery Partition의 밖으로 보낼 수 없다. 해커에 의한 도청이 불가능하다. 수신한 패킷들은 Log Data 섹션의 저장 공간에 시간 순에 따라 순서대로 저장된다. 저장된 데이터(Log)는 Compare 섹션과 Emergency 섹션으로의 전송만이 허용된다.

5.2 Alpha ECU Recover Data 섹션

Alpha ECU Recover Data 섹션은 자율주행 자동차의 출고 직전 테스트에서 발생한 데이터 값과 ECU 통신의 프로토콜의 원칙이 저장되어 있다. Log Data 섹션과는 통신하지 않으며 나머지 섹션들에게 정보를 보내는 역할을 한다. Compare 섹션과는 정보를 보내는 발신만을 수행하며 Emergency 섹션과는 양방향 통신이 가능하다. 연결된 섹션들과 Alpha Data(섹션내의 저장된 각종 정보)를 주고받는다.

5.3 ECU Simulator & Compare 섹션

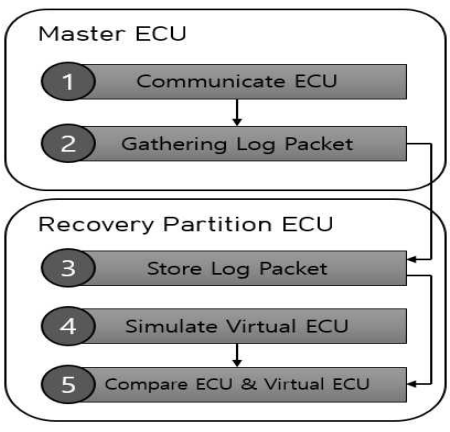
ECU Simulator & Compare 섹션은 전송받은 Log Data와 Alpha Data를 바탕으로 가상 구동을 시뮬레이터 값을 산출한다. 산출된 값을 바탕으로 현재의 차량 상태의 값과 정상일 때의 작동 값을 비교하는 역할을 한다. Log 섹션, Alpha 섹션과 수신만 수행하는 단방향 통신이며 Emergency 섹션과는 비교를 통한 결과데이터를 발신만 수행하는 단방향 통신이다.

5.4 Emergency 섹션

Emergency 섹션은 비교분석 섹션을 통한 분석에서 일정 오차를 넘어선 값이 발견되거나 해킹으로 인한 조작되고 있다는 결과를 수신했을 때 긴급 모드로 차량 전체를 제어할 수 있는 관리자 권한을 가진다. 또한 이 섹션 저장 공간 안에는 자율주행 자동차의 기본 펌웨어가 내장되어 있다. 이 섹션은 모든 섹션에 접근할 수 있으나 일반적인 주행 중에는 작동하지 않는다.

VI. Recovery Partition 작동 원리

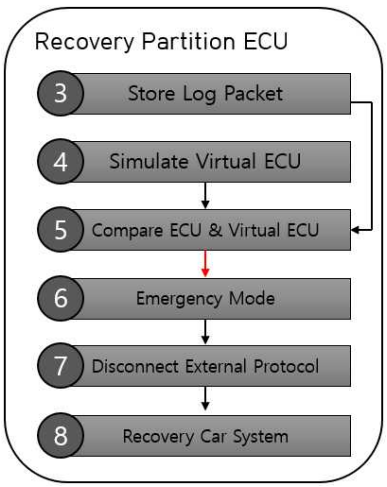
CAN 프로토콜은 다양한 ECU 간 브로드캐스트 방식으로 메시지를 전송하게 된다. 이때 Recovery Partition은 하나의 독립적인 ECU에 해당하게 되며 이는 중앙처리 역할을 하는 마스터 ECU만이 연결 된다. 이후 폐쇄 망이 구축되어 있다는 가정을 두고 그 외의 모든 접근을 방지한다. 자율주행 자동차의 엔진 구동과 동시에 Recovery Partition이 동시에 동작 한다. 자율주행 모드에 들어가게 되면 차량의 동작에서 발생하는 모든 ECU통신 패킷들은 Recovery Partition의 Log 섹션으로 보내진다. 전송되어진 Log 데이터들은 2가지로 나뉜다. 차량의 주변 상태와 그에 따른 ECU의 작동 상태로 나뉜다. Log 섹션에 시간 순으로 저장된 모든 패킷들은 저장됨과 동시에 Compare 섹션으로 보내진다. Compare 섹션에서 Log데이터를 받기 시작하면 Alpha 섹션에서 Compare 섹션으로 순정 정보를 보낸다. Compare 섹션은 차량 주변 상태에 관한 Log 데이터와 순정 작동 정보인 Alpha 데이터를 바탕으로 가상의 시뮬레이터 값을 산출한다. 산출된 값들은 현재의 차량에 대한 가상 ECU의 작동상태이며, 실제 ECU의 작동 상태와 비교분석을 실시한다.



[그림 4] Recovery Partition 구조

가상 ECU의 작동 상태와 실제 ECU의 작동 상태가 오차범위 안에서 일치하거나 정상상태라면 자율주행 모드는 유지된다. 하지만 일정

수준 이상의 오차가 발견되거나 차량내부에 결함이 발견되는 결과가 나타나면 Compare 섹션에서 Emergency 섹션으로 차량의 이상이 있다는 메시지를 보내게 된다. 이때의 Emergency 섹션은 차량의 일반적인 운행 중에는 작동하지 않는다. 하지만 Compare 섹션에서 차량의 이상이 있다는 메시지를 받게 되면 즉각적으로 외부의 악의적인 접근을 차단하기 위해 차량과 차량 외부를 연결하는 모든 통신을 차단하고 운전자에게 차량에 문제가 발생함을 알린다. 운전자가 이를 인식하여 차량이 수동운전 모드에 들어가게 되면 Emergency 섹션은 Compare 섹션과의 통신으로 원인분석을 실시한다. 차량 자체의 고장이 아닌 해커의 공격에 의해 자율주행 펌웨어의 조작이 원인이 되었다면 섹션에 저장되어 있던 관리자 모드로 진입하여 기본 펌웨어를 차량에 적용하여 악의적으로 수정되었던 펌웨어를 덮어씌운 클린 상태로 만든다. Recovery Partition이 차량 내부에서 할 수 있는 모든 조취를 수행한 후, 차량과 차량 외부의 연결을 허용한다. 외부의 연결이 성립되면 차량의 셀룰러 네트워크를 이용하여 해당 운전자의 차량에 문제가 발생했다는 메시지와 문제가 발생한 시점의 Log 데이터들을 자동차회사 또는 차량의 보험회사로 전송하여 차량 문제를 알린다.



[그림 5] Recovery Partition ECU 순서

VII. 결론 및 기대효과

CAN Protocol은 모든 메시지를 브로드캐스트 하지만 데이터를 암호화 하지 않는다는 취약점이 존재한다. 하지만, 본 논문에서 제안하는 Recovery Partition은 실시간으로 데이터를 분석이 가능하기 때문에 자율주행 모드에서 발생하는 모든 사건들에 대해 즉각적으로 대처할 수 있다는 것이 가장 큰 장점이다. 실시간이라는 이점을 사용하여 데이터 위·변조뿐만 아니라 차량의 고장을 발견하고 예방할 수 있는 기능을 갖춘다. 이상이 발견되었을 때는 문제를 외부로 빠르게 전송하여 공격에 대한 분석과 대응을 가능하게 한다. 또한 Recovery Partition 자체가 독립적인 동작을 수행하며 외부의 접근으로부터 통신 방향이 각기 다른 섹션을 4개를 보유하고 있기 때문에 외부로부터의 접근이 어려워 해커의 공격으로부터 보호된다.

자율주행 자동차의 상용화는 아직 준비가 부족하다. 상용화가 되기 전에 이미 여러 취약점과 해킹 사례가 공표되었고 이에 따라 보안적 측면에서 더욱 연구가 필요하다. 앞서 말한 것처럼 본 논문에서 CAN Protocol의 취약점에 대한 대응으로 Recovery Partition을 제안하였다. 자율주행 자동차의 전반적인 부분에서 악의적 접근과 조작에 대한 보안 서비스를 제공한다.

[참고문헌]

[1] 손영섭, 김원희, 정정주, 자율주행 자동차의 전기적 파워 조향 시스템을 위한 제어 기법의 개관, 기술특집, 2015

[2] 석종수, 김종서, 진현욱, CAN(Controller Area Network) 기반의 분산 환경을 위한 IEEE 1588 시간 동기화 프로토콜 구현, 가을 학술발표논문집, 2011

[3] Automotive Security Best Practices, intel security, 2016

[4] H UEDA, Security Authentication System for In-Vehicle Network, AUTOMOTIVE, 2015

[5] Miller, Charlie, Chris Valasek, Remote exploitation of an unaltered passenger vehicle, Black Hat USA 2015