Journal of The Korea Society of Computer and Information
Vol. 18, No. 11, November 2013
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2013.18.11.039

자동차용 ECU의 CAN 메시지를 통한 자동차 공격 방법 연구

이 혜 련*, 김 경 진**, 정 기 현**, 최 경 희*, 박 승 규***, 권 도 근****

Studies of the possibility of external threats of the automotive ECU through simulation test environment

Hye-ryun Lee*, Kyoung-jin Kim**, Gi-hyun Jung**, Kyung-hee Choi*,
Seung-kyu Park***, Do-keun Kwon****

요 약

본 논문에서는 자동차의 내부 통신망(CAN)에 대한 보안 매커니즘이 매우 미비하여 외부로부터 위협 가능성이 높은 점을 검증하기 위한 방법으로 시중에서 쉽게 구입할 수 있는 자동차의 ECU(Electric Control Unit)을 이용하여 테스트 환경을 구축하여 CAN 메시지를 획득한 다음 자동차의 실제 ECU에 적용시켜 공격을 시도하는 방법을 제안한다. 최근 연구들 중에서는 자동차에서 누구나 쉽게 평문 상태의 CAN 메시지를 볼 수 있어 외부로부터 공격에 취약한 것을 보이기 위하여 실제 자동차에서 데이터를 분석한 내용을 가지고 공격을 성공시켰으나 차를 구입하여 고정시킨 상태에서 CAN 메시지를 추출하고, 이를 분석하여 공격을 시도함으로 공간적, 금전적, 시간적 비용을 발생시키는 단점을 가진다. 본 논문에서는 자동차의 외부 위협 가능성을 검증하기 위한 실험을 수행하기 위해 자동차의 ECU를 통해 찾아낸 CAN 메시지를 실제 자동차에 적용하되 무선 네트워크 환경을 갖추어 실험한 결과 제안한 방법을 통해 자동차에 공격이 가능함을 확인한다. 그 결과 기존 연구에서 발생하는 비용을 줄임과 동시에 자동차의 정보가 전혀 없는 상태에서 자동차 ECU의 공격 가능성을 보인다.

▸ Keywords : ECU, 보안, 자동차 공격, CAN message

Abstract

In this paper, security mechanism of internal network(CAN) of vehicle is a very incomplete state and the possibility of external threats as a way to build a test environment that you can easily buy from the market by the vehicle's ECU(Electric Control Unit) to verify and obtain a CAN

•제1저자 : 이혜련 •교신저자 : 정기현
•투고일 : 2013. 9. 3, 심사일 : 2013. 9. 11, 게재확정일 : 2013. 9. 24.
* 아주대학교 컴퓨터공학과(Dept. of Computer Science, Ajou University)
** 아주대학교 전자공학과((Dept. of Electronic Science, Ajou University)
*** 아주대학교 소프트웨어융합학과(Dept. of Software Convergence Technology, Ajou University)
**** 아주대학교 전자공학과((Dept. of Electronic Science, Ajou University) & The attached institute of ETRI

message. Then, by applying it to ECU of the real car to try to attack is proposed. A recent study, Anyone can see plain-text status of the CAN message in the vehicle. so that in order to verify the information is vulnerable to attack from outside, analyze the data in a vehicle has had a successful attack, but attack to reverse engineering in the stationary state and buying a car should attempt has disadvantages that spatial, financial, and time costs occurs. Found through the car's ECU CAN message is applied to a real car for Potential threats outside of the car to perform an experiment to verify and equipped with a wireless network environment, the experimental results, proposed method through in the car to make sure the attack is possible. As a result, reduce the costs incurred in previous studies and in the information absence state of the car, potential of vehicle's ECU attack looks.

▸ Keywords : ECU, security, vehicle attack, CAN message

I. 서 론

최근 자동차는 수많은 ECU들에 의해 제어되는 시스템을 갖추고 있으며, 이 추세는 점차 늘어나는 추세이다. 이 시스템의 ECU들은 하나의 자동차 내부 통신망(예, CAN, LIN, FlexRay bus)으로 연결되어 있으며, 이 연결된 통로에 의해서 CAN 메시지들을 주고받는다. 운전자는 실내 온도, 주행시간 등 여러 정보들을 쉽게 얻을 수 있으며, 자동차를 제어하는데 편리성을 제공받는다[1,2].

그러나 이와 같은 시스템에 대한 보안 매커니즘이 미비하게 구성되어 있어, 공격자가 자동차의 외부에서 내부 통신망에 접속하여 많은 ECU들을 제어할 수 있다. 그 결과 ECU의 정상적인 동작을 방해할 수 있다. 특히 자동차의 내부 통신망에 연결된 ECU의 수 및 기능 증가로 자동차 보안의 위험 요소가 점점 증가하고 있으며, 그 예로 현재 악의적인 공격을 시도하여 문 개폐부터 자동차의 가벼운 오동작 및 브레이크나 엔진 등의 오동작을 발생시켜 자동차 안전에 심각한 문제를 일으킬 수 있는 것을 보이고 있다[3-5].

자동차 ECU공격은 경제적인 측면에서 볼 때 자동차에 사용되는 ECU에 외부 위협이 발생 시 자동차 판매에 영향을 심각하게 주어 자동차 산업 전체에 큰 영향을 미칠 수 있으며, 자동차 운행 안전에 영향을 미칠 경우 인적/물적 피해의 정도는 엄청나게 크다. 따라서 사이버 공격으로부터 위협이 발생하게 되면서 국내외적으로 자동차에 대한 악의적인 공격 방법 및 이를 방어하기 위한 방법과 관련한 관심이 증가하고 있다.

따라서 이러한 문제를 해결하기 위하여 자동차의 공격 및 방어에 대한 다양한 형태의 연구가 진행되고 있으나 현재까지 이에 대한 자세한 정보들은 많은 부분이 공개되지 않는 상태이며 공격이나 방어 방법과 관련하여 실제 실험 위주보다는 시나리오 위주의 실험 방식을 택하고 있다[2,3,15]. 하지만 논문[3,6]에서는 실제 자동차의 ECU를 대상으로 한 공격이 성공하였음을 보이고 있다.

해외 사례를 보면 Karl Koscher 등[3]은 CarShark 이라는 도구를 개발한 다음 차량에 대한 다양한 실험 환경을 구성하였으며 그 중에서 802.11 ad hoc 네트워크를 이용한 무선 통신환경에서 자동차에 공격을 시도하여 자동차에 대한 외부 위협이 발생할 수 있음을 보였다. 국내에서는 실제 자동차 ECU를 대상으로 외부 위협 가능성을 시험하여 발표한 자료는 [6]외에는 없다.

본 논문에서는 자동차용 ECU를 사용하여 자동차 외부에서 자동차를 대상으로 외부 위협 가능성을 검증하기 위한 방법을 제안하고 이를 이용하여 실제 자동차 ECU를 대상으로 실험을 실시하고 그 결과를 제시한다. 특히, [6]과는 달리 실험 대상 자동차의 정보가 전혀 없는 상태에서 자동차 ECU의 공격 가능성을 보인다. 또한 제안하는 실험 환경에서는 실제 자동차에서 공격 환경과 유사하게 공격자가 자동차에 접근하지 않고 가까운 거리를 유지하면서 공격을 시도하여 자동차의 안전에 악영향을 줄 수 있는지를 확인하고자 외부에서 무선 통신망으로 자동차의 내부 통신망(CAN)을 접근하는 방식을 이용한다.

마지막으로 본 논문에서 제안하는 방법의 가용성을 검증하기 위하여 실제 자동차에서 분리한 엔진 ECU을 대상으로 실험을 수행하고 실험 결과를 이용하여 실제 자동차에서 실험을 진행하였다. 제안한 방법을 통해 ECU에 대한 외부 위협이 발생하여 자동차의 안전에 영향을 미칠 수 있음을 보인다.

본 논문의 구성은 다음과 같다. 2장에서는 자동차용 ECU에 대한 공격 가능한 유형별로 정리하고, 공격에 사용될 수 있는 도구들에 대해서도 분석하여 기술한다. 3장에서는 자동차용 ECU의 테스트 환경 구축하는 방법을 기술하며, 4장에서는 실험을 통하여 자동차의 외부 위협을 보인다. 마지막으로 5장에서는 결론을 맺는다.

II. 관련 연구

2.1. 공격 유형

자동차 ECU에 대한 공격 방법은 CAN과 같은 자동차 내부 네트워크에 직접적으로 접근하거나 무선 통신을 이용한 공격으로 나눌 수 있다. 두 가지 유형의 공격은 공격이 미치는 영향과 공격 대상 및 세부 기술에서 서로 차이점을 가질 수 있다.

1) 내부 공격

공격에 사용될 장치를 CAN 버스 시스템에 연결하여 CAN 버스에 물리적으로 접근할 수 있는 통로를 생성한 후 이를 이용해 CAN 상의 메시지를 분석하여 공격에 필요한 정보를 획득하거나 악의적인 메시지를 주입하여 자동차의 정상적인 동작을 방해 혹은 오동작을 유발하는 공격 방식이다.

가) 메시지 감청 및 재전송 공격(Sniffing Replay Attack) : 네트워크를 감청하여 유효한 메시지에 대한 정보를 획득한 후 이를 재전송하여 정당한 사용자로 가장하는 공격이다. Hoppe 등은 CAN 버스 상에 특정 메시지를 전송할 수 있는 기능을 수행하는 모듈을 부착하고 이를 이용하여 CAN 상에서 메시지의 감청 및 재전송을 수행하여 방향 표시등과 에어백 등의 오작동을 유발하는 실험을 하였고 공격 대상이 동작 불능 상태가 되거나 비정상적 동작을 보이는 것을 확인하였다[7,8].

나) 간접 물리적 공격 : OBD(On-Board Diagnostics)-II를 이용하여 자동차의 CAN 버스에 직접 접근이 가능하면서 자동차 시스템 전체에 걸쳐 손상을 야기할 수 있는 접근이 허용된다. Stephen 등은 실제 자동차에 탑재된 OBD-II와 오디오 시스템을 통해 공격 가능한 루트를 찾아 해당 시스템을 경유한 공격 방법을 제안하고 실험을 수행하여 성공시켰다[9].

다) 복합 공격 : 복합 공격은 자동차 내부 네트워크는 다양한 컴포넌트가 서로 상호작용하는 복합적인 환경이므로 저속/고속 CAN 네트워크에 동시에 연결되어 있는 장비 중 텔레매틱스 장비를 이용한다. 공격은 우선 저속 네트워크에 연결되어 있는 장치를 이용해 텔레매틱스 장비를 재 프로그램 하는 것부터 시작한다. 재 프로그램이 완료되면 텔레매틱스 장비는 두 네트워크 사이의 브리지 역할을 수행할 수 있게 되어 저속 CAN 네트워크 메시지를 고속 네트워크로 전달하는 것이 가능해진다. 즉 이와 같이 공격자에 의한 장비의 의도되지 않은 브리징은 BCM 게이트웨이를 거치지 않은 메시지 흐름을 유발시켜 고속 CAN 네트워크 상의 중요 부품들을 공격할 수 있다.

2) 외부 공격

자동차에 탑재된 장치 가운데 RFID(Radio Frequency IDentification)나 블루투스 혹은 네트워크 등을 사용하는 장치의 인터페이스에 대한 접근을 통해 자동차 절도, 공격에 필요한 정보 획득, 자동차의 정상 동작 방해 등을 수행하는 공격 방식이다.

가) RFID를 이용한 공격 : 역공학을 이용해 특정 자동차의 RFID 시그널을 탐지하고 이를 공격에 이용하는 시나리오를 가정 할 수 있다. Rouf 등은 실험을 통해 자동차의 수가 2억 5천 6백만 대가 넘지 않으면 센서 ID만을 이용하여 자동차의 식별이 가능하며 설령 자동차의 수가 이 수를 넘어선다고 해도 자동차에 탑재된 네 개의 타이어 내 센서 ID 조합을 이용하면 자동차의 식별이 가능함을 보였다. 이와 같이 자동차 내 타이어에 탑재된 RFID를 이용한 자동차 식별을 이용하면 자동차의 위치 추적, 스푸핑/RFID 키 분석 공격이 가능해진다고 주장하였다[10,11].

나) 무선 신호를 이용한 공격 : 최근의 자동차 업계에서는 운전자의 편이성 증진을 위한 목적으로 무선을 통해 인증한 사용자 정보를 가지고 자동차 문의 개폐를 지원하는 형태가 증가하고 있다. 무선으로 사용자를 인증하는 절차는 무선 신호를 통해 데이터 교환이 이루어지므로 여러 가지 형태의 공격이 가능해지는 불리함을 가진다. 메시지 전달 공격, 사전 공격/두 도둑 공격/세 도둑 공격/키 복제 공격이 가능해진다[12].

다) VANET(Vehicular Ad hoc NETwork)를 이용한 공격 : 최근 자동차의 안전한 주행을 지원하기 위한 다양한 방법들이 고려되면서 자동차 간, 혹은 차와 네트워크 간 통신이 주요한 이슈로 떠오르고 있다. 그와 관련하여 VANET가 발달하게 되었으나 공격자가 네트워크

상에 메시지를 추가하거나 메시지의 변경 혹은 삭제하여 해당 네트워크를 사용하는 사용자에게 문제를 일으킬 수 있다. Irshad 등은 VANET에서 발생될 수 있는 공격 모델을 크게 감시, 소셜, 시간차, 응용 프로그램 및 네트워크(DoS/분산 DoS/시빌/노드 위장 공격) 등의 다섯 가지로 구분하고 각각에 대한 공격 방법을 설명하였다[13].

2.2. 공격 도구

자동차에 장착되어 있는 전차장치인 ECU은 현재 자동차 한 대 당 많게는 100개 이상 탑재 되어 있으며 ECU마다 약 9~20개 정도의 CAN ID들을 사용하고 평문 상태의 메시지를 그대로 이용하고 있다[6]. 따라서 공격자가 어떠한 제약도 받지 않는 상태에서 내부 통신망의 메시지를 도청이나 조작할 수 있어 ECU의 외부 위협이 발생할 수 있다.

2) CAN 통신 도청 및 조작을 통한 차량 ECU의 외부 위협 가능성 분석

연구에서는 두 대의 자동차를 이용하여 실험 환경을 구성하되 유선으로 CAN 네트워크를 접근하는 방식을 선택하였다[6]. 실험 결과 공격을 성공시켜 자동차의 ECU에 대한 외부 위협이 가능하다는 것을 보였다.

가) 실험 내용

- 메시지 감청 : OBD-II 커넥터를 통해 평문 상태의 메시지 그대로 읽어 들였다.
- 메시지 재생 : 감청을 통해 수집된 메시지들을 가지고 그대로 실차에서 재현 시켰다.
- 메시지 인젝션(Injection) : 공격용 CAN 메시지만을 찾아 차량의 메시지 전송 시간 간격(7~10ms)보다 빠르게 메시지를 인젝션 시켰다.
- 메시지 퍼징 : 감청을 통하여 얻어낸 CAN 메시지에 대한 패턴을 분석하여 메시지를 퍼징 할 수 있는 ECU 공격자 도구를 직접 개발하여 공격하였다.

나) 실험 분석

공격을 시도하는 실험 결과 문 잠금부터 엔진 RPM/속도 상승, 에어백/경고 등 조작 및 기어 조작이 가능하였으나 바퀴 조향은 각각의 모델들이 피드백 메시지만을 출력하며 브레이크는 기계적 방식인 유압식으로 메시지를 출력하여 조작할 수 없음을 나타내었다.

3) Carshark을 통한 ECU의 외부 위협 가능성 분석

Karl Koscher 등[3]은 CarShark 이라는 도구를 개발한 다음 차량에 대한 다양한 실험 환경을 구성하되 차량에 직접 접근하지 않고, 무선 통신으로 CAN 네트워크를 접근하는 방식을 선택하였다. 실험 결과 공격을 성공시켜 차량의 외부에서 차량에 직접 접근 하지 않아도 공격자로부터 자동차 ECU에 대한 공격을 받을 수 있음을 보였다.

가) 실험 방법

- 실험실에서 환경 구축 : 자동차 내에서 전자 브레이크 제어 모듈을 추출하여 실험 환경을 구성 하였으며 CAN-to-USB 변환기를 이용하여 CAN 메시지를 획득하였다.
- 자동차 고정시킨 상태에서 환경 구축 : 차가 어떠한 이상 동작을 할지 모르기 때문에 자동차를 움직이지 못하게 앞 바퀴을 빼 놓은 상태로 실험을 진행. 그리고 차 내부에서는 노트북과 OBD-II 포트를 연결하고 자동차의 고속 네트워크를 사용하기 위하여 CAN-to-USB 인터페이스를 사용하였다.
- 도로에서 환경 구축 : 자동차 3대를 이용하여 실제 실험을 진행하였다. 하나의 자동차는 달리는 자동차이며 두 번째 자동차는 메시지를 읽어 들이는 자동차이며 마지막 세 번째 자동차는 802.11 ad hoc 네트워크를 통해 CAN으로 메시지를 보내는 자동차를 이용하여 실험을 수행하였다.

나) CarShark을 이용한 공격

CarShark은 CAN 인터페이스 따라 무작위 테스트를 할 수 있는 개발한 도구이며 CarShark을 이용하여 CAN 메시지를 감청하고 감정한 메시지에 대하여 분석한 다음 분석한 메시지를 무작위로 조작하여 공격을 시도하였다.

다) 실험 결과

다양한 ECU들에 대해 정리하고 공격 방법론을 적용하여 실험한 결과 공격이 가능함을 보였다. 라디오, 바디 컨트롤러 및 IPC(Instrument Panel Cluster)의 제어가 가능하였으며 자동차의 전원을 차단시키거나 엔진에 센서 오류를 주기적으로 삽입하여 엔진에서 패킷을 전송되는 타이밍을 방해시키는 것도 보였다.

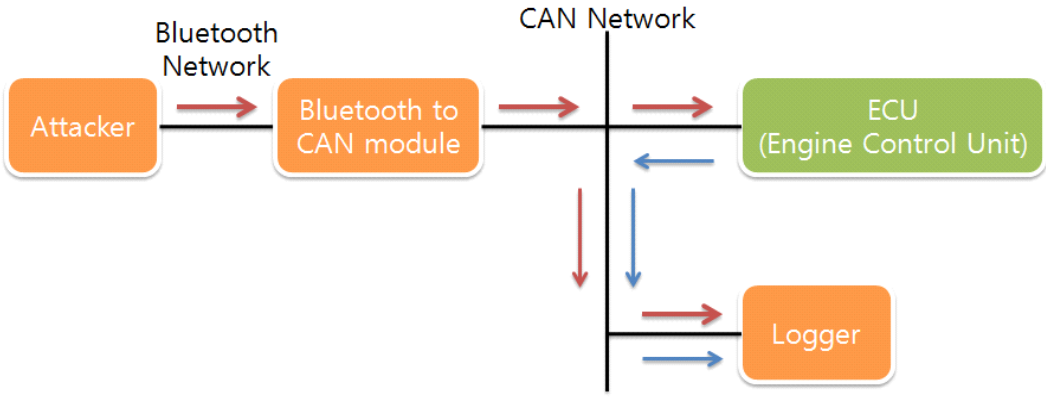

그림 1. CAN 정보 획득을 위한 테스트 환경
Fig. 1. CAN test environment for obtaining information

III. ECU 테스트 환경 구축

3.1. CAN 정보 획득을 위한 환경

기존 많은 연구에서는 실제 자동차에서 CAN 메시지들을 감청하고 획득한 메시지들을 분석하여 자동차에 재전송하였으며 자동차에 전송하는 방법은 실제 케이블에 물려서 전송하거나 무선 네트워크를 통하여 전송하는 방법을 택하였다. 그 결과 자동차가 오동작 하는 것을 확인하여 공격에 굉장히 취약하다는 점을 보였다.

그러나 이러한 테스트 환경은 실제 자동차의 CAN등의 네트워크에서 메시지들을 감청하여 메시지가 어느 ECU에서 사용되는 메시지인지 이를 분석하여야 한다.

따라서 본 논문에서는 실제 CAN 통신을 하는 자동차 ECU에 대한 아무런 정보를 알지 못한다는 가정 하에서 무선으로 접속하여 ECU 공격을 시도하는 환경을 구성하기 위하여 2가지 고려사항을 검토 한 후 하나의 ECU로부터 CAN 메시지를 감청하는 방법을 제안하여 기존 연구들과의 차이점을 가지도록 한다.

- CAN 네트워크에 연결된 ECU들은 브로드캐스트(broadcast) 방식으로 메시지를 주고받는데 ECU는 입력 메시지에 대하여 출력 메시지만을 내보낼 뿐 입력 메시지에 대하여 어떠한 새로운 조작을 하여 메시지를 출력시키지 않으며 잘못된 메시지가 입력으로 들어올 경우 그 메시지에 대하여 응답하지 않고 무시하는 점을 이용한다.
- 블루투스 환경은 핸드폰 및 네비게이션과 같은 시스템이 자동차와 통신할 수 있는 환경을 갖추고 있어 자동차의 주요 외부 위협 요소가 되어 서브시스템 전체에 악영향을 미칠 수 있다는 점을 이용한다.

그림 1과 같이 공격용 컴퓨터를 두고 ECU에게 메시지를 보낼 수 있는 환경과 동일하게 구성하기 위하여 무선 네트워크 중 차량에서 흔히 사용되는 블루투스 모듈을 사용한다. 공격자는 블루투스 환경에서 메시지를 보내고 CAN 네트워크에서는 블루투스로부터 받은 메시지를 ECU에게 전송시켜 준다. 이 메시지를 받은 ECU는 자기의 메시지 일 경우 받은 메시지에 대하여 적절한 동작을 수행한다. 또한 네트워크 상의 모든 메시지는 로거에 남기고 후에 로거 데이터를 분석하여 공격 결과를 알아낸다.

이렇게 구성한 테스트 환경은 공격자가 자동차 외부에서 자동차에 어떠한 물리적인 연결을 하지 않는 상태로 자동차에 공격을 가하여 오동작을 일으킬 수 있는 환경을 제공할 수 있다.

테스트 환경의 구성 요소는 총 6가지이다. 공격자, 블루투스와 CAN 연결 모듈(Bluetooth to CAN module), ECU, 로거, 블루투스 네트워크, CAN 네트워크로 구성된다.

1) 공격자 : ECU에 공격을 수행하는 PC이다. 다양한 CAN 메시지를 ECU에 전송할 수 있도록 블루투스 네트워크로 보낸다. 공격자는 우선 무선 환경인 블루투스 네트워크를 통하여 CAN 메시지를 전송한다. 블루투스 모듈로 CAN 메시지를 전달하기 위해 Firmtech 사의 블루투스 USB 모듈인 FB200AS 모델을 사용하였다. 또한 공격자 컴퓨터에서 CAN 메시지를 블루투스에서 CAN으로 데이터를 전송할 수 있도록 간단한

프로그램을 이용한다.

2) Bluetooth to CAN module : 공격자로부터 전송 받은 CAN 메시지를 CAN 프로토콜에 맞게 변환하여 CAN 네트워크상으로 전송하는 모듈이다. 본 논문에서는 CAN 네트워크에 연결하기 위해서 마을소프트웨어사의 CAN to RS232 Converter를 이용하였다. 이는 CAN 통신 프로토콜을 RS232 통신 프로토콜로 변환하는 장치이다. 그리고 공격자와 블루투스를 통해서 통신을 하기 위해서 Firmtech사의 블루투스 임베디드 모듈인 FB155BC 모델을 사용하여 블루투스 네트워크를 구성하였다. 블루투스는 RS232 통신 프로토콜을 사용하는 무선 통신이므로 RS232 통신과 블루투스 간의 프로토콜 변환이 필요 없다. 블루투스 모듈과 RS232간을 직접 연결하면 된다.
3) ECU(Engine Control Unit) : 공격을 받는 대상으로 자동차 엔진의 제어를 담당하는 모듈을 이용하였다. 본 논문에서는 중형 승용차의 ECU를 사용한다.
4) 로거 : CAN 네트워크 상의 모든 CAN 메시지들을 수집하여 로그 파일로 작성해서 저장하는 일을 수행하는 PC로 공격에 있어서 어떠한 일도 수행하지 않는다.
5) 블루투스 네트워크 : 블루투스 프로토콜에 맞게 메시지들을 주고받는 무선 네트워크이다.
6) CAN 네트워크 : CAN 네트워크는 CAN 프로토콜에 맞게 통신을 주고받는 네트워크이다.

공격 대상 ECU로는 통신용 CAN 인터페이스를 포함하고 있는 2010년도 중형 승용차의 엔진 ECU를 선택하였다. 대상 ECU 모듈에 대한 정보는 인터넷 상에서 구할 수 있는 외부 핀 배치도를 제외한 내부 하드웨어 구성이나 자세한 기능에 대한 정보는 전혀 없다. 아래 표1은 실험 대상 ECU의 핀 배치도에 따른 핀 번호들이다. 여기서 핀 번호는 제품 보안의 이유로 바꾸었다[14].

표 1의 핀들을 연결하고 배터리 전원 핀에 약 12 ~ 14V의 전압을 인가하게 되면 CAN 통신을 통해서 CAN 데이터가 출력됨을 확인할 수 있다. 그림 2는 그림 1 구성도에 따라 실제 구성한 그림이다. 제대로 전압을 인가하였다면 CAN 정보가 주기적으로 출력되는 것을 볼 수 있을 것이다. 이 정보는 로거에 저장된다.

표 1. 실험 대상 ECU의 핀 번호
Table 1. pin numbers of test subject ECU

Pin 번호	Description
1, 3, 5	접지
2, 4, 6, 7	배터리 전원
31	CAN(하이)
32	CAN(로우)

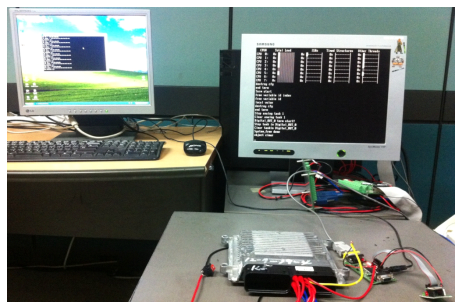

그림 2. 실험 환경
Fig. 2.Experimental environment

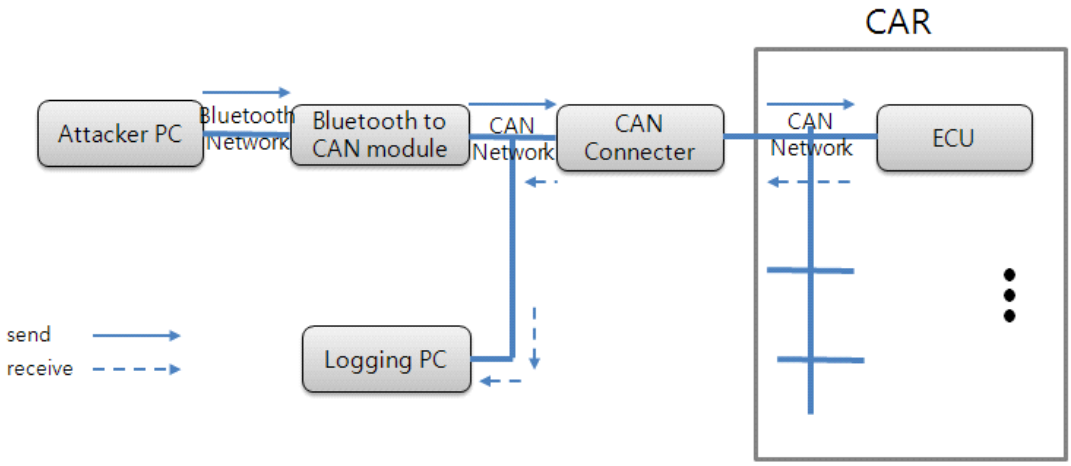

그림 3. 자동차 실험 환경
Fig. 3. Car experimental environment

3.2. 실차 실험 환경 구축

실차 자동차 내부에는 실험 목적으로 안전하게 진행하기 위하여 그림 3과 같이 라디오의 블루투스를 제거하고 엔진 ECU에서 사용하였던 블루투스 모듈을 CAN 커넥터와 연결한 다음 CAN 커넥터와 자동차를 연결시켜 자동차의 블루투스 환경을 구성한다. 다음 그림 3이 실제 자동차 실험 환경 구축한 내용을 나타낸 것이다.

CAN 메시지 값의 변화를 추적하기 위해 노트북을 로거로 사용하고자 자동차에 비치한 상태에서 출력 CAN 메시지를 저장시켰다. 그림 4는 실제 차량에 장착하여 공격 실험을 하고 있는 그림이다.

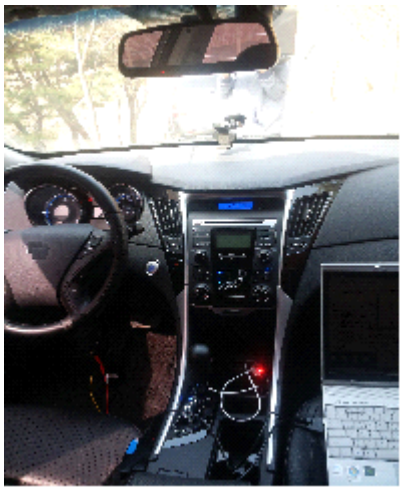

그림 4. 자동차 외부에서 공격하는 모습
Fig. 4. attack from the Car's outside

IV. 실험

앞 절에서 제시한 방법과 같이 테스트 준비 과정을 걸쳐 차량의 엔진ECU에서 CAN 메시지를 뽑아낸 다음 실제 자동차에서 실험하였다.

4.1. 엔진 ECU의 CAN 정보 획득

CAN 신호에서 비 주기적인 신호는 일반적으로 특별한 일이 발생되었을 때 발생된다. 따라서 본 논문에서는 사용한 ECU에 대한 정보가 전혀 없는 상태에서 비 주기적인 사건을 만들 수 없다. 이에 비해 정기적인 신호는 ECU가 타 CAN 노드와 주고 받는 메시지로 ECU가 정상적으로 동작하는 상태에서는 나름대로의 주기에 출력되어 ECU 외부에서 획득이 가능하다.

따라서 ECU를 정상적으로 동작시킨 상태에서 로거PC가 CAN 메시지들을 읽어 들인다. 본 논문에서 사용한 ECU에서는 총 14개의 CAN 메시지들을 출력시키는 것을 확인하였으며 다음 표 2는 엔진 ECU에서는 출력 CAN 메시지 일부분을 나타낸 것이다.

4.2. 실차 실험

실차 실험은 두 가지 방법으로 진행하였다. 앞 절과 같이 획득한 CAN 메시지를 이용하여 다음과 같은 2가지 방법으로 나누어 실험을 진행하였다.

우선 첫 번째는 14개의 CAN 메시지를 각각 하나씩 보냈다. 보낼 때에는 CAN 메시지의 데이터 일 부분을 랜덤으로 바꾸어 보냈다. 예를 들어 설명하면 CAN 메시지 0x316 같은 경우 데이터 일 부분 중 1,6번째 바이트에 값이 존재하는 것을 확인하고 1,6번 바이트에 대해서만 랜덤 값을 생성하여 CAN 메시지를 자동차에 보냈다. 그 결과 자동차에서는 아무런 반응을 하지 않았다.

두 번째 방법은 14개의 CAN 메시지 중에서 일부 CAN 메시지를 자동차에 동시에 보냈다. 즉 CAN 메시지 5~7개 정도 엔진 ECU에서 출력된 초기 값을 그대로 보내면서 1개의 CAN 메시지에 대하여 데이터 일 부분을 랜덤으로 바꾸어 보냈다. 그 결과 실제 자동차에서 반응을 일으켰다. 실험 결과 사진들은 실제 자동차에서 반응하는 모습을 촬영한 것이다.

실험 결과 0x43F의 데이터 8바이트 중에서 1,2번째 값

표 2. 엔진 ECU에서 찾아낸 CAN 메시지 내용
Table 2. CAN message found in the engine ECU

CAN ID	1 byte	2 byte	3 byte	4 byte	5 byte	6 byte	7 byte	8 byte
0x43F	11	4F	60	FF	0	0	0	0
0xA0	0	0	0	0	0	FF	1	0
0xA1	80	80	0	0	9	0	0	0
0x316	5	0	0	0	0	2C	0	80
0x545	DE	0	0	85	0	0	0	0

11, 4F에서 15, 47로 값을 바꾸어 자동차에 CAN 메시지를 보내면 자동차에 운전자가 없는 상태에서 기어가 움직이지 않는 상태로 그림 5와 같이 P->R 로 시그널이 바뀌면서 후방카메라 모드가 떴다.

그림 5. 실험 결과 P->R로 변환
Fig. 5. Results P-> R conversion

마찬가지로, 0x43F의 데이터 8바이트 중에서 1,2번째 값 11, 4F에서 8, 46로 값을 바꾸어 자동차에 CAN 메시지를 보내면 자동차에 운전자가 없는 상태에서 기어가 움직이지 않는 상태로 그림 6과 같이 P->N 로 시그널이 바뀌면서 변속되는 소리가 났다.

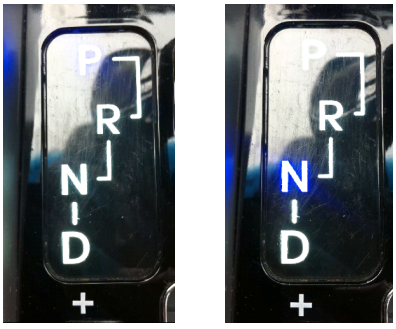

그림 6. 실험 결과 P->N로 변환
Fig. 6. Results P-> N conversion

마지막으로, 0x316의 데이터 8바이트 중에서 1,6번째 값 5, 2C에서 85, 4E로 값을 바꾸어 자동차에 CAN 메시지를 보내면 자동차에 운전자가 없는 상태에서 그림 7과 같이 RPM값이 0으로 떨어지는 것이 계기판에 표시되었고 EPS가 뜨면서 자동차가 문제 있다라고 화면에 오토케어 모드를 띄운다

그림 7. 실험 결과 EPS 발생 및 오토케어 발생
Fig. 7. results occur EPS and Auto Care

4.3. 실험 분석

실험 결과 ECU의 출력 CAN 메시지를 자동차에 주기적으로 보내어 자동차가 어떤 동작을 수행하기 전에 자동차에서 CAN 메시지를 덮어쓰는 현상이 발생하여 운전자로 하여금 운전 할 때 운전을 방해하는 일을 발생시켜 교통사고를 유발할 수 있게 된다. 또한 관련 연구에서 공격 유형별 기준으로 볼 때 외부 공격에 따르는 무선 시그널에 의한 메시지 전달 공격이 가능함을 확인할 수 있다.

기존 연구에서는 먼저 CAN 메시지를 읽어올 때 자동차에서 입력/출력 CAN 메시지를 찾아 분석하기 위해서 자동차를 구입하여 고정시킨 상태에서 역공학을 수행하였다. 이 실험을 진행하기 위해서 금전적, 공간적, 시간적 비용이 발생하지만 본 논문에서 엔진 ECU의 CAN 메시지를 이용하여 공격을 시도하여 기존 실험과 동일한 결과를 얻었다. 또한 새로운 사실은 엔진 ECU로부터 얻은 CAN 메시지가 자동차에 더 큰 영향을 줄 수 있을 것으로 판단할 수 있다.

예를 들어 설명하면 자동차의 기어 같은 경우 P->R로 바꾸는 것을 수행할 경우, 자동차에서 CAN 메시지를 찾아 43F 데이터 값 {0x15, 0x47, 0x60, 0xFF, 0x76, 0x00, 0x00, 0x00}을 보내면 P->R로 시그날만 바뀌었다. 그러나 엔진 ECU에서 찾아낸 43F 데이터 값 {0x15, 0x47, 0x60, 0xFF, 0x00, 0x00, 0x00, 0x00}과 함께 CAN 메시지 여러 개를 값이 보면 후방 카메라까지 켜지면서 자동차에 실제 기어가 들어간 것으로 확인되어 엔진 ECU로부터 CAN 메시지를 추출하여 공격할 시 더 위험할 것으로 판단된다.

방면에 공격에 사용될 수 있는 CAN 메시지가 부족하여 다양한 실험을 진행하지 못하였다. 테스트 케이스 생성 관련

연구가 좀 더 추가가 된다면 CAN 메시지에 대한 공격을 시도 할 수 있으므로 짧은 시간에 공간적, 금전적 비용을 줄이면서 다양한 종류의 공격을 시도할 것으로 본다.

V. 결 론

현재 자동차는 운전자에게 사용의 편의성을 제공하기 위해 점차적으로 자동차에서 ECU들이 차지하는 부분이 커짐으로써 급격한 속도로 ECU 탑재가 증가하고 있다. 따라서 본 논문에서는 여러 참고 문헌들을 조사하여 자동차에 대한 공격 유형별로 정리 하였고, 공격에 사용될 수 있는 도구들을 분석하였다.

이와 같은 분석을 바탕으로 본 논문에서는 자동차용 ECU로부터 CAN 정보를 획득한 다음 자동차 외부에서 자동차를 대상으로 공격하여 자동차의 외부 위협 가능성을 검증하기 방법을 제안하였다. 실제 차량에서 사용되는 ECU를 대상으로 공격을 하되, 자동차의 외부에서 무선 통신환경에서 자동차 내부 통신망에 접근하는 방식을 이용하였다. 이 테스트 환경은 여러 종류의 ECU들에 대해 동일한 테스트가 가능하다.

외부 위협 가능성을 검증하기 위하여 실제 차량의 엔진 ECU을 구입하여 CAN 정보를 획득한 다음, 실제 차량에서 공격을 시도하였다. 그 결과 ECU의 CAN 메시지를 이용하여 자동차의 외부 위협을 보였으며 기존 연구에서 자동차의 CAN 메시지를 분석하는데 발생하는 공간적/금전적/시간적 비용을 줄일 수 있었다. 이는 자동차의 외부 위협의 가능성을 보임으로써 ECU에 대한 보안 테스트를 할 수 있는 중요 기반 기술을 획득하는데 있어서 기여할 수 있을 것으로 기대된다.

향후 이 결과 바탕으로 실제 무선통신 환경에서 외부 위협 가능성 검증 연구가 필요하다. 본 논문에서는 실험을 통하여 공격용 CAN ID을 찾아냈다. 실험을 진행하기 위하여 블루투스 모듈을 자동차에 탑재시켜 실험하였으나 실제 자동차에서 블루투스 모듈을 가지는 칩에 직접적으로 접근하여 CAN 메시지를 보내어 자동차의 외부 위협이 가능한 것을 보여야 할 것이다.

참고문헌

[1] D. K. Nilsson, U. E. Larson, and E. Jonsson, "Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes," in Proceedings of the 68th IEEE Vehicular Technology Conference 2008(VTC 2008-Fall), pp. 1-5, Sep. 2008.

[2] Marko Wolf, Andr´e Weimerskirch, Christof Paar, "security in automotive bus systems," In Proceedings of the Workshop on Embedded Security in Cars 2004, pp.1-13, 2004.

[3] Karl Koscher, Alexei Czeskis, Franziska Roesner, "Experimental Security Analysis of a Modern Automobile," IEEE Symposium on Security and Privacy, pp.447 - 462, May. 2010.

[4] content of Car hacking, http://www.etnews.com/news/international/251094 6_1496.html

[5] McAfee Report on Automotive Systems Finds Prevelant Lack of Security in Today's Vehicles, "Partners with Wind River and ESCRYPT to Provide Analysis of Emerging Risks in Automotive Embedded Systems"

[6] Gang-seok Kim, "Vehicle ECU through CAN communication from eavesdropping and manipulation of the analysis of the possibility of external threats," Korea University, 2011

표 3. 기존 연구들과 비교 분석
Table 3. Comparison with previous studies

	연구1	연구2	제안한 방법
CAN 메시지 추출	자동차에서 직접 추출 (자동차 공간 및 자동차 필요)	ECU 사용	ECU 사용
CAN 메시지 분석	자동차에서 재생하여 확인 (분석 시간 필요)	ECU 사용으로 분석 필요 없음	ECU 사용으로 분석 필요 없음
공격 도구 사용	공격 도구 개발 (개발 시간 필요)	CarShark 도구 개발 (개발 시간 필요)	CAN 출력메시지는 회사에서 제공하는 프로그램으로 확인 CAN 메시지 차량에 삽입 할 수 있는 간단한 C 프로그램 작성
네트워크 환경	유선 네트워크 환경 (외부에서 공격 가능하기 힘듦)	802.11 ad hoc 네트워크 환경에 공격과 공격 받을 노트북 필요	실제 공격이 가능할 블루투스 모듈 사용

〔7〕 T. Hoppe and J. Dittman, "Sniffing/Replay Attacks on CAN buses: A simulated attack on the electric window lift classified using an adapted CERT taxonomy," in Proceedings of the 2nd Workshop on Embedded Systems Security(WESS), pp.1-6, Oct. 2007.

〔8〕 Tobias Hoppe, Stefan Kiltz, Andreas Lang, Jana Dittmann, "Exemplary Automotive Attack Scenarios - Trojan Horses for Electronic Throttle Control System (ETC) and Replay Attacks on the Power Window System, Automotive Security," VDI reports

〔9〕 S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, " Comprehensive experimental analyses of automotive attack surfaces," in Proceeding of SEC'11 Proceedings of the 20th USENIX conference on Security, pp.1-16, 2011.

〔10〕 I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar. "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," In USENIX Security 2010, pp. 323-338, Aug. 2010.

〔11〕 S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device," in Proceeding of SSYM'05 Proceedings of the 14th conference on USENIX Security Symposium, pp. 1-15. 2005

〔12〕 Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, Mohammad T. Manzuri Shalmani, "On the power of power analysis in the real world: a complete break of the KEELOQ code hopping scheme," in Proceeding of the 28th International Cryptology Conference-CRYPTO 2008, pp.203-220, Aug. 2008.

〔13〕 Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan "Classes of attacks in VANET," in Proceedings of Electronics, Communications and Photonics Conference(SIECPC), 2011 Saudi International, pp.1-5, April. 2011.

〔14〕 Search for ECU pin numbers, http://www.globalserviceway.com/

〔15〕 Xiao Ni, Weiren Shi, Victor Foo Siang Fook, "AES Security Protocol Implementation for Automobile Remote Keyless System," in Proceedings of the 65th IEEE Vehicular Technology Conference 2007(VTC2007-Spring). pp.2526-2529, April 2007.

〔16〕 Hye-ryun Lee, Kyoung-jin Kim, Gi-hyun Jung, Kyung-hee Choi, "Research of generate a test case to verify the possibility of external threat of the automotive ECU," The Korea Society of Computer and Information, pp21-31, Sep. 2013.

저 자 소 개

이 혜 련

2006: 조선대학교 인터넷소프트웨어공학과 공학사.
2008: 아주대학교 정보통신전문대학원 공학석사.
현 재: 아주대학교 컴퓨터공학과 박사수료
관심분야: 보안테스팅, 소프트웨어공학
Email : cocom12@ajou.ac.kr

김 경 진

2012: 아주대학교 전자공학과 공학사
현 재: 아주대학교 전자공학과 석사과정
관심분야: 임베디드 시스템, 테스팅, 실시간 시스템 등
Email : klm0012@ajou.ac.kr

최 경 희

1976: 서울대학교 수학교육과 학사.
1979: 프랑스 그랑데꼴 Enseeiht대학 석사.
1982: 프랑스 Paul Sabatier대학 정보공학부 박사
현 재: 아주대학교 컴퓨터공학과 교수
관심분야: 컴퓨터공학, 운영체제, 실시간시스템, 테스팅 등
Email : khchoi@ajou.ac.kr

정 기 현

1984: 서강대학교 전자공학과 학사.
1988: 미국 Ilinois주립대 EECS(석사)
1990: 미국 Purdue대학 전기전자공학부 박사
현 재: 아주대학교 전자공학과 교수
관심분야: 컴퓨터구조, VLSI 설계, 실시간시스템, 테스팅 등
Email : khchung@ajou.ac.kr

박 승 규

1974: 서울대학교 응용수학과 학사
1976: 한국과학원(KAIST) 전산학과 석사
1982: Institut National Polytechn- ique de Grenoble 전산학과 박사
1976 ~ 1992 KIST, KIET, ETRI 선임/책임연구원
1992 ~ 현재 아주대학교 소프트웨어융합학과 교수
관심분야 : 임베디드 테스팅, 자가 컴퓨팅/치료 시스템, 차세대 컴퓨터 구조 등
Email : sparky@ajou.ac.kr

권 도 근

2004: 아주대학교 전자공학과 학사
2006: 아주대학교 전자공학과 석사
현 재: 한국전자통신연구원 부설연구소 연구원
아주대학교 전자공학과 박사과정
관심분야: 임베디드 시스템, 취약점 분석
Email : kwondk@ensec.re.kr