지능형 자동차 내부 네트워크에서 생체인증을 이용한 인증기법

이광재, 이근호
백석대학교 정보통신학부

Authentication Scheme using Biometrics in Intelligent Vehicle Network

Kwang-Jae Lee, Keun-Ho Lee
Dept. of Information and Communication, Baekseok University

요약 현재 IT기술과 자동차기술을 융합한 지능형 자동차에 대한 연구가 활발히 진행중에 있으며 많은 새로운 서비스 모델들이 개발중에 있다. 지능형자동차에 대한 개발이 활발하게 이루어지면서 무선 네트워크를 이용한 다양한 서비스가 제공이 되고 있다. 이러한 지능형 자동차가 무선 네트워크를 이용한 서비스가 제공되면서 다양한 보안 위협 요소가 도출되고 있다. 본 논문에서는 지능형 자동차의 외부에서 네트워크에 침입하여 지능형자동차의 보안 위협 요소를 분석하고 지능형 자동차의 보안 솔루션의 인증 모델에 대한 기법을 제공하고자 한다. 인증 모델의 경우 신체의 고유성을 식별할 수 있는 생체인식을 이용한 인증기법을 제안한다.

• **주제어** : 지능형 자동차, 인증기법, 생체인식, 씨앤유, 정보기술

Abstract Studies on the intelligent vehicles that are fused with IT and intelligent vehicle technologies are currently under active discussion. And many new service models for them are being developed. As intelligent vehicles are being actively developed, a variety of wireless services are support. As such intelligent vehicles use wireless network, they are exposed to the diverse sources of security risk. This paper aims to examine the factors to threaten intelligent vehicle, which are usually intruded through network system and propose the security solution using biometric authentication technique. The proposed security system employs biometric authentication technique model that can distinguish the physical characteristics of user.

• **Key Words** : Intelligent Vehicle, Authentication Scheme, Biometric, CAN, Information Technology

1. 서론

자동차의 전자 제어 장치인 ECU(Electronic Control Unit)는 자동차의 엔진, 변속기(자동), 조향 장치, 제동 장치, 현가 장치 등을 제어하는 장치를 말한다. 이러한 ECU는 기존 엔진 실린더에 연료분사량 조절, 공회전 등의 엔진 핵심 기능을 제어하는 목적으로 설계되었지만

자동차가 점점 발전하고 그 기능이 많아져 오늘날에 소형컴퓨터 수준에 이르고 있다. ECU는 사람으로 비유하면 뇌와 같은 역할을 하는 것이 때문에 이의 중요성이 점차 늘어나고 있다.

또한 향후 지능형자동차에 대한 인터페이스 개발 경쟁이 본격화 되면서 자동차 산업의 보안문제가 제기될

*교신저자 : 이근호(root1004@bu.ac.kr)

접수일 2013년 08월 13일 수정일 2013년 08월 29일 게재확정일 2013년 09월 02일

것이다. 현재 차량에서 스마트폰과 ECU를 연동한 모바일 네트워크 및 블루투스(근거리 무선 통신망)에 접속할 수 있는 기술들이 개발되고 차량관련 어플리케이션(응용 프로그램)을 내려 받아 차량과 직접 연결하여 사용자 차량의 정보를 열람할 수 있는 현재에 간단한 사용자인증은 컴퓨터 바이러스나 해킹 공격에 취약할 수밖에 없다.

ECU 해킹공격으로 인한 자동차시스템의 오류는 운전자의 생명을 위협하고 개인정보 노출과 전화 도청 및 위치파악에 따른 사생활의 침해 문제로 이어지기 때문에 이를 막기 위한 강력한 보안솔루션이 필요하다. 자동차의 정보나 조작 및 개인의 사생활정보유출을 막고 사용자 생체인증 기법으로 사용자 차량을 분별하고 외부의 접근을 제한 할 수 있도록 하는 것을 목표로 한다.

차량을 보호하는 우선적인 방법으로 외부에서의 접근을 제어하는 시스템 구축이 있다. 접근제어란 외부에서 자동차시스템에 접근하여 차량정보를 열람하거나 기능 제어 및 조작을 막고 사용자의 특정 생체정보아래에서 사용자를 분별하여 ECU에 접속하여 서비스를 제공하는 것을 말한다.

현재 차량시스템과 연동된 서비스는 간단한 비밀번호 인증만으로 접근하는 보안모듈을 사용하고 있다. 쉽게 비밀번호를 해킹당할 수 있으며 이러한 문제점에 대한 보안솔루션으로 사용자 생체인증을 이용한 인증기법을 제안하고자 한다.

2. 지능형 자동차 네트워크

차량 사시제어에 쓰이는 LIN (Local Interconnect Network), CAN (Control Area Network) 등은 단순 제어 명령을 전달하기 때문에 데이터양이 많지 않다. 하지만 지능형자동차 개발에는 레이더 센서, 영상감지 센서, 멀티미디어 기기 등 많은 센서 및 장치들이 장착되는 추세여서 많은 양의 데이터 전송을 요구하게 된다.

따라서 기존의 네트워크에서 처리가 불가능한 부분들을 새로운 제어 네트워크로 대체할 필요성이 발생하게 된다. 하지만 기존의 차량 제어 네트워크를 대체할 수는 없다. 따라서 LIN, CAN 등의 네트워크와 FlexRay, MOST 등 차세대 차량 네트워크를 서로 연동할 수 있는 게이트웨이가 필요하게 된다.

2.1 LIN(Local Interconnect Network)

LIN은 CAN을 토대로 개발된 프로토콜로서, 차량내 바디 네트워크의 CAN 통신 말단 시스템의 분산을 위해 사용된다. LIN의 특징은 하나의 선으로 통신하기 때문에 차량 배선의 문제를 크게 개선할 수 있고 저가의 실용성 있는 네트워크 구성이 가능하다는 점이다. 하지만 하나의 선(Single Wire)이라는 특성상 외부 전자기에 의한 영향이 크며, 이로 인해 20Kbps의 제한된 통신 속도를 갖는다.

2.2 CAN(Control Area Network)

여러 개의 ECU를 병렬로 연결해서 데이터 통신을 하는 CAN 통신은 표준 통신 프로토콜로 ECU들 사이에서 다량의 정보 공유가 가능하고 시장성이 높아 가장 많이 사용되고 있는 통신 방법이다. CAN통신의 특징은 다음과 같다.

- multi Master와 multi Slave가 버스를 공유
- 메시지들은 우선순위를 가짐
- 대기시간(latency time) 보장
- 시간 동기화에 따른 멀티캐스트 수신
- 두 가닥 꼬임선을 사용, 전기적 노이즈에 강함
- 통신 속도는 1Mbps며, 원거리 통신이 가능
- 실시간 분산 통신이 가능
- CAN 하드웨어 내에서 여러 처리
- 표준 인터페이스작업이 쉽고 시장성이 높음

CAN 통신은 단일 버스에 연결된 여러 개의 ECU간의 데이터를 전송해야 하기 때문에CSMA/CR(Carrier Sensing Multiple Access/Collision Resolution)을 사용한다. 메시지를 전송하기 위해서는 버스 사용권을 획득해야만 하는데, CAN 통신에서는 버스 마스터가 존재하지 않으며 지연 없이 우선순위가 가장 높은 메시지가 버스 사용권을 획득한다. 메시지 전송 시에는 각 ECU가 모두 동기화를 이루어 데이터를 주고받을 수 있도록 한다. CAN은 각 ECU가 우선순위를 가지고 CSMA방식을 이용하기 때문에 버스 상에서의 충돌은 없으나 데이터가 전송되는 시간은 예측할 수 없는 단점이 있다.

2.3 MOST

MOST는 차량용 멀티미디어 장비들 간의 통신을 위해 개발된 컴퓨터 네트워크 규격으로 오디오, 비디오 등

의 대용량 멀티미디어 데이터들의 실시간전송 및 제어를 위해 최적화 된 구조를 제공한다. MOST는 스트리밍 데이터와 패킷 기반의 데이터 전송방식을 정의하고 있으며, 특징은 다음과 같다.

- 최대 64개 노드(하나의 마스터를 포함)
- 스트리밍 데이터 전송(동기/비동기 모드)과 패킷 데이터 전송이 가능
- 높은 데이터 전송 속도
- 설정이 가능한 60개의 채널

동기 모드 데이터 전송은 오디오나 비디오 혹은 센서 값등의 실시간 데이터 전송을 위해서 사용하며 데이터 접근 방식을 TDM (Time Division Multiplexing)을 이용한다. 비동기 데이터를 전송할 경우는 바운더리 디스크립터를 설정하여 비동기 데이터의 시작을 나타낸다.

MOST통신에서 마스터는 오직 하나만 존재하며, 이 마스터는 시스템의 상태를 제어하고 중앙 레지스트리를 관리한다. 또한 이벤트를 모니터링하고 슬레이브로부터 들어오는 정보를 관리하여 필요한 내용에 대해서는 슬레이브들에게 알리는 한편 중앙 레지스트리의 정보를 업데이트한다. 마스터를 제외한 모든 노드는 슬레이브로 현재 구성 상태에 대해서 마스터로부터 통지 받는다.

차량용 DVD나 네비게이션, 내부 PC까지 자동차 내부의 디지털 기기가 증가함에 따라 MOST는 멀티미디어 네트워크에 최적화 되어있다는 점에서 이와 같은 요구에 적합하지만, 복잡한 인터페이스를 가지고 있고, 다른 통신시스템에 비해 비용이 비싸다.

2.4 FlexRay

FlexRay는 차세대 차량 네트워크 프로토콜의 일종으로 FlexRay 컨소시엄에서 Core member 회사인 BMW, 보쉬, 다임러클라이슬러, 프리스케일, GM, 포스마겐, NXP Semiconductors 등이 공동연구를 통해 개발하였다. FlexRay는 동기 프로토콜과 비동기 프로토콜의 장점만을 통합하여 확장 가능한 정적/동적 메시지 전송방식을 결합시킴으로써 유연성과 결정론을 제공한다. FlexRay의 특징은 다음과 같다.

- time triggered 방식의 통신
- fault tolerant 기능 지원
- 최대 10Mbit/sec의 고속 통신
- 다중 네트워크 토폴로지 지원

- 2채널

FlexRay는 기본적으로 TDMA(Time Division Multiple Access)방식을 사용한다. 각 노드는 고정된 타임 슬롯을 가지고 있으며 확정적으로 버스에 접근할 수 있다. 타임 슬롯은 같은 패턴으로 반복되기 때문에 모든 노드는 글로벌 타임을 가지고 동기화 되어야 한다.

그러나 각 노드가 가지고 있는 타임 슬롯에 전송할 데이터가 없다면 그 시간은 비효율적으로 흘러가 버린다. 또한 데이터양이 커서 타임 슬롯 안에 전송을 하지 못하게 되면 다시 자신이 접근할 수 있는 시각이 올 때까지 대기해야만 한다. 이러한 문제점을 해결하고자 통신 사이클을 정적인 부분과 동적인 부분으로 분할하여 사용한다. 미니 슬롯의 시간에 버스에 접근하면 미니 슬롯을 필요한 만큼 확장할 수 있도록 함으로써 대역폭을 효율적으로 활용할 수 있다[1].

3. 지능형 자동차 보안 위협요소

기존 자동차보안 솔루션인 간단한 비밀번호를 통한 사용자인증으로 차량시동과 위치추적이 가능하게 하고 차량의 ECU와 스마트폰이 자동적으로 M2M(Machine To Machine) 통신을 수행한다. 간단한 비밀번호인증만으로 차량시동제어 및 위치추적이 가능하게 되어 차량도난사고를 줄일 수 있게 되었다[2,6].

[Fig. 1] Vehicle information collection module interlock system

하지만 비밀번호인증은 보안솔루션으로서 한계가 있어 비밀번호를 도난당하거나 노출되었을 때 사용자차량 정보가 누출될 우려가 있고 그에 따른 보안위협이 발생

하여 사용자에게 완벽한 신뢰를 줄 수 없다[3]. 그러므로 차량 ECU와 연동해서 이루어지는 컴퓨팅자동차서비스 환경에서 다양한 개발과 상용화를 위해선 앞에서 언급하였던 기존 차량보안시스템의 문제점을 해결할 효율적인 방안이 필요하다.

3.1 ECU 펌웨어의 표준구조

ECU는 단일 마더보드로 구성되어 있고 그 안에는 이전만 하더라도 롬이 장착되어 있었다. 하지만 요즘은 FlashROM이 장착되어 있어 간단히 펌웨어 Writing이 가능하다. 이러한 이유로 ECU에 특정 비정상 시그널이 전해지게 되면 Flash ROM 내부의 펌웨어 데이터가 깨져 ECU가 제대로 동작하지 않는다. 언제든 지우고 쓸 수 있는 FlashROM을 장착함으로써 자동차의 기능을 좀 더 효율적으로 관리 할 수 있지만 그에 따른 위험도 같이 동반되기 때문이다. Interaction Layer, Network Management, Transport Protocol는 OSEK에서 정의하였으며, Diagnostic Layer 와 Transport Protocol 는 ISO에서 정의하였다.

[Fig. 2] OSEK / VXD Standard firmware structure

CAN 이라는 것은 해당 소프트웨어에서의 표준 프로토콜이라 생각하면 된다. CAN Calibration Protocol는 ECU의 FlashROM에 다양한 데이터 접근방식으로 읽기와 쓰기를 담당하는 프로토콜이다. Network Management는 주된 목적은 자동차의 전원 사용 효율성이다. Transport Protocol는 대용량 데이터를 보내기 위한 고안된 프로토콜이다. 데이터 분할 기능과 동기화 기능, 에러감지 기능을 가지고 있다. Diagnostic Layer는 자동차에 내장된 각종 진단 기능에 대해 인터페이스를 제공하는 Layer이다. 또 예외처리를 담당하고 있으며 CAN과 관련한 요구

를 처리한다. Interaction Layer는 소프트웨어 구조 설계 시 정의된 메시지 전송 형태의 핸들링을 처리하는 기능의 Layer이다. 또 데이터 교환에 관한 API를 제공하고 각종 기본 값들을 설정 할 수 있다.

3.2 지능형 차량과 애플리케이션

텔레매틱스 차량의 발전으로 차량의 효율적인 관리가 이루어지고 있다. 최근에 생산되는 차량들은 ECU 시스템이 장착되어 있다. ECU를 통해 엔진과 동력 계통, 에어백, 브레이크, 기타 편의 시설의 상태나 동작된 데이터를 실시간으로 차량상태를 점검할 수 있다. 실시간으로 점검된 차량의 정보를 블루투스로 실시간 업데이트하여 메모리에 저장한다.

3.3 지능형 자동차의 취약점을 이용한 해킹

보안이 취약한 차량 내부 네트워크(CAN)를 통해 악성코드에 감염된 스마트폰으로 자동차와 연결되어 ECU에 접근한다. ECU를 제어 할 수 있게 된 공격자는 상대방차량을 무선으로 제어 할 수 있게 된다[4].

[Fig. 3] Vehicle hacking scenarios

[Fig. 4] Vehicle information acquisition App operation screen

4. 사용자 생체인증기법을 이용한 M2M 서비스

외부에서 차량 ECU와 이루어지는 모든 동작을 사용자 생체정보를 이용한 인증기법으로 접근을 제한한다.

[Fig. 5] New Vehicle information collection module interlock system

차량 내부 네트워크에 접근하기 위해 생체인증을 통해 인증을 받은 후 접근하게 된다. 사용자의 신체정보는 센서가 부착된 단말기에서 부호화를 거친 후 차량내부의 ECU로 이동하기 위한 여러 가지 정보를 삽입해야한다. 이러한 정보는 사물통신으로 전송되기 때문에 트래픽이 가벼워야한다. 그러므로 이런 정보를 데이터 안에 숨김으로 기밀성과 동시에 트래픽의 절약을 얻을 수 있다.

[Fig. 6] Biometric authentication scheme Process

5. 결론

본문에서 기존의 차량보안솔루션보다 높은 보안성을 가지고 있고 지능형 자동차의 구현의 문제점을 해결 될 수 있는 기초기반이 되고자 사용자 생체인증기법으로 새

로운 차량 정보 수집 모듈을 제안해 CAN에서의 보안성을 높여 자동차해킹위험에서 벗어나고자 한다. 제안한 인증기법은 차량 내부 네트워크에 접근하기 위한 기존의 프로세스보다 보안성이 높으며 사용자 신체정보를 기반으로 한 프로세스로 사용자의 신체정보는 고유의 암호가 될 수 있으며 높은 보안성을 가지고 있다. 기술적인 부분에서 실현가능성을 확인할 수 없지만 여러 가지 요구사항들을 분석하고 이를 실현할 기술을 접목시킴으로 지능형자동차에 대한 보안위협요소를 줄여 지능형자동차서비스가 활력을 얻기를 기대한다.

감사의 글

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2013R1A1A1A05012348)

REFERENCES

- [1] Park, Sang Hyun "Intelligent smart sensors for your car Network design framework", Proceedings of 2009 Korea Computer Proceedings Vol. 36, No.1, 2009.
- [2] Jung Ho An, "Android applications for intelligent vehicles Implementation Options", Korea Institute of Information Technology undergraduate paper competition Proceedings of 2011.
- [3] Shin Hyung Back, "Android-based vehicle information system Research", Fall Conference Vol. 37, No. 2, 2010.
- [4] Sung Hyung Back "Android-based vehicle information system study ", Journal of Korea Information Science Society, the Korea Information Science Society, pp. 397-400, 2010.
- [5] Chung Gun Song, "M2M for environment of U-Healthcare Certification system designed by the expression", Korea Institute of Convergence Winter Conference 2012.
- [6] <http://www.ituran.com/en/>

저자소개

이 광 재(Kwang-Jae Lee)

[학생회원]

- 2006년 8월 : 백석대학교 정보통신학부 재학생
- <관심분야> : M2M 보안, 지능형자동차 보안 등

이 근 호(Keun-Ho Lee)

[종신회원]

- 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야> : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호