지능형 자동차에서의 RF 통신 보안 위협에 관한 연구

이광재, 이근호
백석대학교 정보통신학부
kwang291@naver.com, root1004@bu.ac.kr

A Study of RF Communications Security Threats of Intelligent Vehicle

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

요 약

차량 내부 네트워크는 LIN, CAN, FlexRay와 같은 제어 네트워크와 MOST와 같은 멀티미디어 네트워크가 있으며 이 내부 네트워크와 연결해 서비스를 사용하는 RF 통신으로는 대표적으로 블루투스, GSM, NFC가 있다. 그러나 능동 안전 시스템과 같은 지능형 기술의 지속적인 도입과 기계, 유압식 기기의 전자화에 따른 네트워크상의 통신량이 급격히 증가하면서 네트워크의 규모 및 통신 복잡도 등이 증가하고 있다. 따라서 차량 내/외부 네트워크의 최적화, 최소화 문제가 반드시 해결되어야하는 문제로 떠오르고 있다. 또한 이러한 통신환경이 갖추어진 이후에도 무선통신 기술의 성능향상 및 통신기술과 응용 서비스 분야와의 연계, 그리고 통신서비스를 위한 사업 모델 개발이 요구되는 등 앞으로 해결해야하는 문제는 여전히 많이 남아 있다고 할 수 있다. 본 논문에서는 지능형 자동차의 RF 통신서비스에서 발생할 수 있는 지능형자동차의 보안위협 요소를 분석하고자 한다.

1. 서론

NFC, 블루투스와 같은 라디오 주파수를 이용한 기술이 등장한 초기에는 인프라 구축에 대한 통신사, 제조사, VAN사 등의 이해관계 부족으로 널리 보급되고 적용되기 어려웠으나 스마트폰의 등장과 국내외 스마트폰 단말기 제조사들의 NFC, 블루투스 기능 탑재로 인하여 라디오 주파수 기술과 관련한 여러 분야에 대한 연구 및 보급이 이루어지고 있다. 스마트폰에 탑재로 인하여 여러 서비스 분야에 대한 애플리케이션의 등장과 정부와 기업체의 적극적이고 활발한 보급과 활용 분야 증대에 힘쓰고 있다. 국내에 경우에는 정부단체와 기업체의 협력으로 NFC 기술을 활용한 다양한 서비스에 대하여 인프라를 구축하고 보급에 힘쓰고 있다. 여러 분야에 적용될 것으로 기대되며 그 중 RF통신을 이용한 스마트 라이프 관련 서비스들이 제공되어 지고 있다. 그 중에서 자동차와 접목된 RF 통신 서비스와 보안위협요소를 분석 하고자 한다.

2. 라디오 주파수 통신

자동차에서 많은 내부 응용은 디지털 통신과 자동차의 다른 네트워크(CAN, LIN 등) 또는 다른 산업 시스템과의 연결을 위해 라디오 주파수를 사용한다.

2.1 라디오

가장 일반적인 라디오 주파수 수신기, 즉 AM/FM/디지털 라디오는 자동차 앞 유리나 뒷유리 열선 시스템에 안테나를 통합했을 수도 있고, 그렇지 않을 수도 있다.

2.2 이모빌라이저나 엔진 시작 방지

이모빌라이저 기능은 RF 트랜스폰더. 보통 125kHz에서 낮은 주파수LF 반송파로 운영되는 것을 말하며 이것을 이용해 자동차 엔진의 시작을 방지하는 것이다.
이모빌라이저의 목적은 접촉 키의 앞부분에 위치한 비접촉식 모드(트랜스폰더)에서 운영하는 요소가 고정된 베이스 교점과 함께 초당 수 킬로비트로 암호화된 모드에서 통신할 수 있게 하는 것이다. 고정된 교점은 자동차 내에 위치한다. 이 통신의 목적은 엔진의 시작을 허용하면서 암호 해독 시스템이 위치한 자동차 점화/주입 부분의 운영을 가능하게 하는 것이다.

2.3 GSM

잘 알려진 단순한 핸드폰 링크와 함께 라디오 주파수 링크를 사용하면 다음과 같은 내부/외부 서비스에 접근할 수 있다.

- 긴급 전화 응용
- 패닉 버튼을 제어하는 통신
- 호텔 예약, 고장 서비스, GPS 위치 확인과 운영을 포함하는 서비스 전화
- 모든 종류의 전화 링크
- 내비게이션 시스템을 위한 역동적 데이터 업데이트

2.4 블루투스

블루투스 시스템은 현재 잘 알려져 있으며 GSM과 함께 또는 국부적인 액세서리로 가장 많이 사용된다.
운전자가 주행을 하면서 이어폰을 통해 핸드폰을 사용하는 것이다. 이때 운전자는 합법적으로 두 손으로 핸들을 잡고 있는 상태다. 또한 주어진 공간 즉 운전자를 제외한 공간에서 차상 IT 기기나 사무용 기술(이메일 프린터 등)을 상호 연결하기 위해 아주 작은 로컬 네트워크 또는 피코 네트워크(Pico-network)를 만들 수도 있다. 이것이 블루투스 응용의 '내부적' 측면을 형성한다[1].

- '핸즈프리'출입 시스템을 제공하기 위한 추가 응용
- 릴레이 공격 원칙을 바탕으로 한 절도 방지 시스템 응용
- 자동차에서 에어백을 발사하기 위해 삼각형을 이용한 승객위치

2.5 열리는 부분의 원격 제어

개인 주택, 아파트, 빌딩 또는 자동차 같은 사적인 공간으로의 출입을 관리하는 모든 원격 제어 장치를 포함한다. 광학 적외선 링크가 수년 동안 사용됐음에도 불구하고 전통적인 원격 제어 시스템은 방향성을 줄이고 운영 범위는 길게 함으로써 현재 더 사용자 중심의 운영을 제공하는 것을 목적으로 한다. 주로 ASK나 FSK 모듈화된 UHF 라디오 주파수가 사용되며, 운영 주파수는 유럽에서는 433MHz의 ISM 밴드와 866MHz이고, 미국에서는 915MHz, 미국과 일본에서는 315MHz다.

2.6 일방향 원격 제어

지금까지 이런 원격 제어 시스템의 대다수는 원격 제어 모듈로부터 자동차로 통신을 하는 완전히 일방향 시스템이다. 이런 원격 제어 유닛에 의해 전송된 메시지는 이모빌라이저 기능용 시스템에 사용된 것과 동일한 방식으로 암호화된다. 수신된 메시지는 이모빌라이저로 전달되기 위해 CAN 프레임으로 코드 변환된다.

- 도어(door)
- 트렁크
- 선루프(Sun roof)

선루프의 원격 제어 장치 전송 순서는 라디오 주파수, 그 후에는 LS CAN, HS CAN 최종적으로 LIN을 통해 이루어진다.

2.7 양방향 원격 제어

(그림 1) 양방향 교환 방식

라디오 주파수 링크와 그들과 다른 버스와의 관계에 있어 자동차가 사용자의 원격 제어 장치로 특정 메시지를 보내게 하는 것이다. 이 경우 트랜스시버가 두 개 필요하다. 하나는 원격 제어 장치에 있고 다른 하나는 자동차에 있는 것이다[1].

3. 라디오 주파수 통신의 문제점 및 취약점 분석

원격 제어 장치에 LED 불빛을 나타내는 간단한 명령 정도면 원하는 임무가 제대로 수행됐다는 것을 알려주기에 충분할 것으로 보이나 때때로 더 높은 수준의 보안이나 편의성을 위한 응용을 위해서는 원격 제어 장치에 LCD나 비슷한 기술을 이용해 문자, 숫자 겸용 스크린을 장착할 필요도 있다. 스크린에 자동차의 차상 컴퓨터가 국부적으로 다운로드될 수 있게 하기 위함이다.

예를 들어 아주 춥거나 아주 더운 일부 국가에서는 사용자가 집에 여유롭게 앉아 아침을 먹고 있는 동안 자동차가 외부에는 잠겨있지만 따뜻하게 또는 시원하게 내부 온도를 유지할 수 있다. 원격 제어는 원하는 운영에 관한 정보를 스크린에 완전히 보여줌으로써 모든 절차를 사용자가 확인할 수 있게 해준다. 여기서 모든 절차를 사용자가 확인 할 수 있다는 것은 제3자도 모든 절차를 볼 수 있고 통제 할 수 있다는 문제점이 발생한다.

(그림 2) RF 트랜스폰더를 이용한 공격시나리오

현재 RF통신 서비스 중 NFC통신을 활용한 자동차 서비스에서는 서로 만나서 키를 주고받는 번거러움이 없어

지고 한 사람이 여러 대의 차량을 제어할 수 있게 되었다. 등록이 가능한 차량대수에는 제한이 없고 차량 전부를 NFC통신을 이용한 서비스로 제어할 수 있다. 시동을 걸어놓고 차량을 잠글 수 있어 편리하고 안전하다고 설명하고 있다. NFC 기술 활용은 그러나 편리한 만큼 다양한 보안 문제를 안고 있는 것으로 드러나 주의가 요망되고 있다. 문제는 응용서비스의 특성, 응용프로그램 자체의 취약성, 태그 보안 취약성처럼 NFC 기술 활용과 관련된 분야의 보안 수준이 완벽하지 못하다는 점과 NFC 서비스 이용을 위한 실제 접촉 거리는 5㎝ 미만이지만 전송되는 정보를 도청하는 것은 최대 10m 거리에서도 가능하기 때문이다. 태그 정보가 보호되지 않으면 제3자가 서비스 거부 공격(DoS)을 하거나 피싱을 통해 개인정보를 탈취할 수도 있으며 사용자의 차량을 제어할 수 있게 된다.

(그림 3) RF 통신을 이용한 공격 시나리오

4. 지능형자동차 통신의 보안 위협 및 사생활 침해

차량간/차량-인프라간 통신 환경에서는 안전 관련 메시지가 교환되는 만큼 통신 보안관련 문제가 중요한 문제로 인식되고 있다. 차량들이 차량 외부 통신을 통해 안전메시지를 교환하여 얻어진 정보를 바탕으로 차량의 움직임을 조절하는 ITS시스템의 성공적인 구현을 위해서는 안전 메시지의 무결성이 반드시 보장되어야 한다. 만약 이러한 무결성이 보장되지 않아 특정 차량이 잘못된 정보를 수신하게 된다면 심각한 사고가 발생할 수도 있기 때문이다. 또한 악의적 공격자가 허위 안전메시지를 차량 환경에 방송하는 시나리오를 방지하기 위해, 차량탑재 통신장치(OBU)의 인증뿐만 아니라 도로설치 통신장비(RSU)의 인증도 요구하는 쌍방향 인증방식과, 공격자가 통신을 엿듣는 것을 막기 위한 MAC메시지의 암호화가 요구된다. 이러한 기본 보안 문제와 더불어 차량 프라이버시(privacy)문제 역시 중요한 문제로 떠오르고 있다. 차량 외부 통신이 적용되는 차량의 경우, 차량의 위치가 자동차에 할당된 주소나 기지국 추적을 통해 노출될 가능성을 가지고 있다. 그러나 차량의 위치가 노출된다는 것은 운전자의 사생활 침해와 직결되기 때문에 반드시 프라이버시는 그 비밀성이 보장되어야 한다. 이를 위해 차량탑재 통신장치에 할당되는 주소는 랜덤한 형태로 주어지도록 요구되고 있으며, 이러한 요구사항을 충족시키기 위해서는 증가할 주소할당 체계의 복잡도를 효율적으로 관리하기 위한 연구가 선행되어야 할 것으로 예상된다. 그러나 차량 외부 통신은 범인차량 추적, 사고차량 위치추적과 같은 특수한 경우의 차량위치 정보를 파악하기 위한 목적도 가지고 있기 때문에, 이러한 요구사항을 만족시키면서 프라이버시도 보호할 수 있는 기술의 개발역시 필요할 것으로 전망된다. 이외에도 차량 간 통신 환경에서의 그룹 통신을 위한 그룹 키 관리 기술과 안전관련 메시지 전송의 성공 확률 극대화 기술 등이 요구되고 있다. 향후 차량 외부 통신을 이용한 차량 안전 응용서비스의 적용범위가 넓어지게 되면 보안 및 사생활 보호기술의 중요성은 더욱 크게 부각될 것으로 전망된다[2].

5. 결론

현재 RF통신 기술은 국내외 모바일 결제 서비스와 전자 지갑 서비스를 제공하는데 있어서 큰 역할을 하고 있으며 그 외 다양한 스마트 라이프를 제공하는 서비스의 핵심 기술로 적용되고 있다. 이러한 서비스 환경은 단말기 제조사와 통신사 및 정부의 협력으로 더욱 가속화되고 있으며, 인프라 구축 및 보급률의 증가로 RF통신 서비스가 사용되는 서비스 범위는 앞으로 더 넓어질 것으로 예상되고 있다. 하지만 신기술 및 서비스에 따른 새로운 보안 위협 요소와 보안 서비스에 대한 연구도 더 진행되어야 할 것 이며, 현재 보안서비스로 제공되고 있는 SE에 대한 표준화와 TSM에 대한 정의를 명확하게 하여 사용자와 서비스 제공자 간의 편의성과 안전성을 더 가져올 수 있는 방향을 찾아야 할 것이다. 이러한 내용을 바탕으로 앞으로 RF통신 기술을 응용한 새롭게 등장할 수 있는 서비스에 대한 예측과 그에 따른 보안 위협 및 대책에 대한 적극적이고 활발한 연구가 진행되어야 할 것이다.

감사의 글

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2013R1A1A1A05012348). 또한 '산학협동재단'지원으로 수행된 연구임.

참고문헌

[1] 강기호, "CAN, LIN, FlexRay를 활용한 차량용 네트워크", 에이콘 임베디드 시스템 프로그래밍 시리즈 32

[2] 최민음 외 2명, "자동차 통신기술의 현황과 전망", 2010년 5월 전자공학회지 제37권 제5호

[3] Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges, Wireless Network, Online First, 2014.