자동차 스마트키 보안 취약점 대처 방안과 IoT의 앞으로 나아갈 방향

유승민
고려대학교 컴퓨터정보통신 대학원
소프트웨어 보안 학과
e-mail : ryusm@korea.ac.kr

Security Vulnerability of Automobile Smart Key And Future of IoT Technology

Seung-Min Ryu
Software Security,
Korea University Graduate School of Computer & Information Technology

요 약

1999년 독일에서 처음으로 스마트키가 등장 했다. 기존 자동차 열쇠 키의 대체로 스마트키가 사용되고 있다. 2000년대부터 스마트키 보안 문제가 꾸준히 제기되어 왔지만, 아직까지도 특별한 대체 방법이 있지 않다. 제조부터 실제 제품까지 모든 과정에서 보안에 대한 고려가 필요하다.

따라서 본 논문에서는 보안 문제 중 가장 널리 알려진 주파수 증폭 공격에 대해 설명하고 아데아체(ADAC)의 실험 결과를 통해 심각성을 상기 시킨다. 또한 문제 해결과 동시에 향후 차량 IoT 인프라가 나아갈 방향을 위한 Lora망 도입을 제안한다.

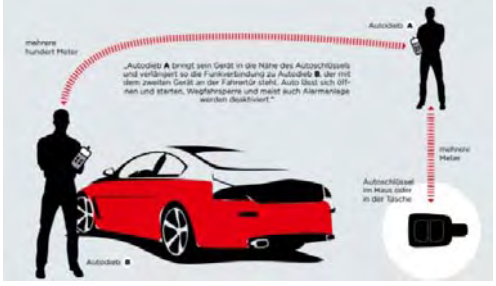
1. 서론

최근 출시되는 차량들의 대부분에는 스마트키를 이용하여 문을 열고 시동을 걸 수 있다. 스마트키는 스마트키에서 자동차에 있는 안테나로 신호를 보내고[1] 상호 신호를 주고받으며 기능이 활성화 되는데, 이 신호를 증폭하여 실사용자가 신호를 보낸 것처럼 보이게 하는 주파수 증폭 공격이 지속적으로 이루어지고 있다.

독일 운전자 클럽 아데아체(ADAC)의 실험 결과에 따르면 실험에 쓰인 자동차 및 오토바이 111대 중 109대가 해킹에 성공하였다는 결과를 볼 수 있다[2].

본 논문에서는 그러한 위험에 대응하기 위해 보안성을 향상시키는 방법으로 IoT 전용 주파수 대역인 LoRa를 제안 하고자 한다. 먼저, 2장에서는 주파수 증폭공격을 설명한다. 3장에서는 LoRa의 대한 소개와 보안성에 대해 설명하고, 4장에서는 향후 기술 적용 방안과 앞으로 나아갈 방향에 대해 논하고자 한다.

2. 주파수 증폭 공격

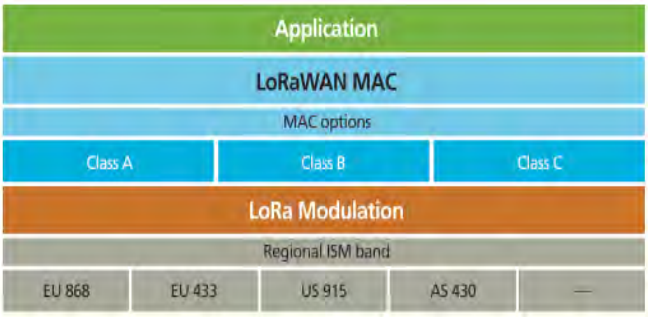


(그림 1) 주파수 증폭 공격의 프로세스

주파수 증폭 공격은, 단말기 동작 원리에서[3] 공격자 1,2로 나누어 공격자1이 스마트키의 신호를 받아서 공격자2에게 전송하여 전달 받은 신호를 공격자2가 자동차로 신호를 보내어 자동차 문을 열 수 있게 된다. 스마트키에 수신 센서가 있는 경우에도 마찬가지로 주파수 탈취의 위험을 가지고 있다.

3. LoRa Solutions

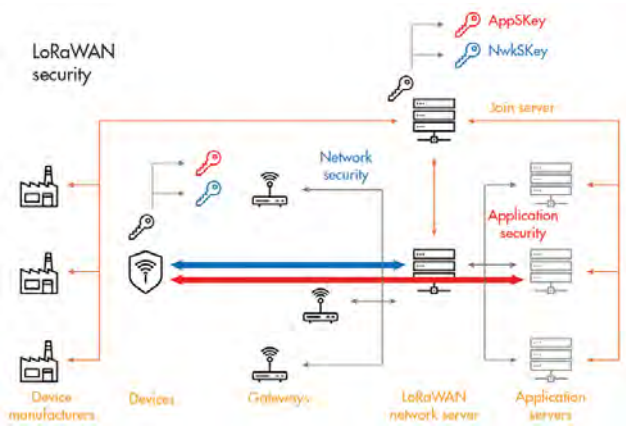
LoRaWAN은 장거리 광역 네트워크의 약자로 저속, 저전력의 특징을 가지고 있다. 중계기와 메쉬 네트워킹을 사용하지 않는 (그림 2)와 같은 단순한 네트워크 아키텍처를 가지고 있다[4].



(그림 2) Architecture of LoRa[4]

LoRa 기술을 제안한 이유는 3G, LTE, WIFI 와 같이 기존 인프라에서 크게 벗어나지 않는 다는 점이다. LoRa

아키텍처는 (그림 3)과 같이 게이트웨이가 최종 장치와 백엔드의 중앙 서버 사이의 메시지를 중계하는 브릿지 배치된다. 게이트웨이는 표준 IP 연결을 통해 네트워크 서버에 연결되며 최종 장치는 하나 이상의 게이트웨이에 단일 홉 무선 통신을 사용한다. 모든 종단 간 통신은 일반적으로 양방향 통신이지만 대기 통신 시간을 줄이기 위해 대기 또는 배포 메시지를 통해 소프트웨어를 업그레이드 할 수 있는 멀티 캐스트와 같은 작업도 지원한다.[4]



(그림 3) LoRa Network Session and Application Session[5]

LoRa는 128 비트 AES 암호화를 사용하는 802.15.4의 보안 메커니즘을 사용한다[5]. LoRa는 네트워크 세션 키와 응용 프로그램 세션 키를 사용한다(그림 3). 네트워크 세션 키는 연결을 관리하기 위해 LoRa 네트워크 내부의 통신에 사용된다. 응용 프로그램 세션 키는 실행중인 프로그램과 클라우드에서 실행중인 서버 프로그램 간 통신에 사용된다. 즉, 데이터를 해당 내용을 통신 사업자에게 공개하지 않고 LoRa 네트워크를 통해 전송할 수 있다.

4-1. LoRa 네트워크를 적용한 스마트키 해킹 방어 방안과 활용 가능성

스마트키에서 가장 큰 문제는 주파수가 탈취 당할 수 있다는 점이다. 이 점에서 LoRa 는 다음과 같은 보안성을 가지고 있어서 공격에 대응이 가능하다.

기본적으로 AES 128 암호화를 사용하고 있어서 기존의 방식처럼 패킷을 탈취 한다고 하여도, 서버에서 송신, 수신된 메시지에 대한 카운터를 관리하고 있고, 또한 장비의 MAC address를 통한 무결성 코드 검사를 통해 탈취에 대응이 가능하다.[6]

노드가 LoRa 네트워크에 참여할 수있는 첫 번째 방법은 OTAA(Over-The-Air-Activation)를 사용하는 것이다. 여기서 각 노드는 노드가 조인 요청 메시지를 보낼 때 사용되는 고유 한 128 비트 앱 키 (AppKey)와 함께 배포된다. 메시지는 암호화되지 않지만, AppKey를 통하여 보장된다. 노드는 고유 한 AppEUI 및 DevEUI 값과 랜덤하게 생성된 DevNonce를 포함하는 조인 요청 메시지를 보낸다. AppEUI는 장치 소유자에게 고유해야하고, DevEUI는 장치에 대한 전역적 고유 식별자여야 한다. 이 세 값은 다음 계산을 사용하여 생성 된 4 바이트 MIC로 서명된다.[7]

mac=aes128_cmac(AppKey, MHDR | AppEUI | DevEUI | DevNonce)
MIC = mac[0..3]

위에 언급한 내용들을 정리 해보자면 스마트키 보안 문제에서 생기는 주파수 공격을 차단 가능하고 향후 스마트카와 연동될 IoT 장비들 간의 연동에도 보안적인 측면에서 고려할 만한 네트워크라 판단된다.

4-2. LoRa 네트워크를 사용 불가능한 상황에서의 대안

LoRa 망이 사용 불가능한 경우의 문제에 대해서는 다음과 같은 경우를 예상해 볼 수 있다.

통신망 지원 거리를 벗어나는 경우와 사용자 인증에 따른 지연시간의 발생 가능성 등 예상 되는 문제점들이 존재한다.

이를 해결하기 위해서 Car Beacon 장치를 추가 한다든지 추가적인 장치 도입을 제외한다면 LoRa망이 사용 불가능할 경우 Bluetooth 기술을 사용한다면 네트워크가 사용 불가능한 상황에서도 근거리 통신을 이용하여 이를 극복할 수 있을 것이라 예상한다.

5. 결론

앞으로도 스마트카에 사용될 기술로 거론 되는 것들은 다음과 같다. 스마트 컨트롤을 통한 원격제어, 주차위치 확인, 목적지 전송, 차량관리와 도난 추적 등 자동차 1대에서만 통신해야할 장비들의 수가 적지 않다.

위에 언급한 기술은 LoRa 네트워크를 통해서 1차로 문제 재기 했던 자동차 스마트키의 보안 문제를 해결함과 동시에 미래 스마트카에 사용될 IoT 인프라를 위한 해결책을 마련할 수 있을 것으로 예상한다.

향후, 이에 따른 스마트카에 적용될 IoT 장비들 간의 LoRa를 이용한 통신에 대해 연구하고자 한다.

참고문헌

[1]RADIO ATTACK LETS HACKERS STEAL 24 DIFFERENT CAR MODELS :

https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/
[2]Autos und Motorräder mit Keyless-Schließsystem, die der ADAC illegal öffnen und wegfahren konnte : https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/keyless/default.aspx?ComponentId=257251&SourcePageId=8749&quer=keyless
[3]당신의 '자동차 스마트키'는 안전합니까? : http://www.kbench.com/?q=node/161504
[4]LoRa Alliance : https://www.lora-alliance.org/technology
[5]What is LoRa? : http://www.semtech.com/wireless-rf/internet-of-things/what-is-lora/
[6]LoRa Rolls Into Philly : http://www.electronicdesign.com/embedded-revolution/lora-rolls-philly
[7]LoRa Security, Robert Miller : https://labs.mwrinfosecurity.com/assets/BlogFiles/mwri-LoRa-security-guide-1.2-2016-03-22.pdf