https://kiisc.or.kr

2022년 한국정보보호학회 동계학술대회

CISC-W'22

Conference on Information Security and Cryptography-Winter 2022

2022년 11월 26일 (토) | 국민대학교

- 학술대회 등록대: 미래관 자율주행 스튜디오 (4층)
- 개회식/정기총회: 본부관 (1층)

Proceedings

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology

주관 KMU 국민대학교 KOOKMIN UNIVERSITY

후원 국가정보원 NATIONAL INTELLIGENCE SERVICE, 과학기술정보통신부, 행정안전부, KISA 한국인터넷진흥원, ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute, NSR 국가보안기술연구소 National Security Research Institute, KiSTi 한국과학기술정보연구원 Korea Institute of Science and Technology Information www.kisti.re.kr, 지란지교시큐리티, PILAB

한국정보보호학회
Korea Institute of Information Security & Cryptology

자기공진 무선 충전 환경에서 보안위협 분석 및 대응방안 연구

안성규*,박기웅†

* 세종대학교 시스템보안연구실(대학원생)

† 세종대학교 정보보호학과(교수)

A Study on Security Threat Analysis and Countermeasures in Magnetic Resonance Wireless Charging Environment

Sung-Kyu Ahn*, Ki-Woong Park†

* SysCore Lab, Sejong University (Graduate student)

† Department of Computer and Information Security, Sejong University(professor)

요 약

최근 무선 전력 전송기술을 통한 모바일 장치의 무선 충전기술의 발전이 활성화됨에 따라 자기 공진 방식의 무선 전력 전송기술이 대두되고 있다. 자기 공진 기반의 무선 전력 전송 서비스가 상용화가 진행될수록, 이와 관련된 보안 위협도 증가하고 있다. 본 논문에서는 자기 공진 기반 무선 전력 전송 환경에서 발생 가능한 보안 위협에 대해 분석하고 보안 위협을 해소하기 위한 대응 방안에 대해 제시한다. 본 연구를 통해 추후 적용될 수 있는 자기 공진 기술 기반 무선 충전환경에서 보안성을 확보할 수 있을 것으로 기대한다.

I. 서론

최근 모바일 시장이 확장되면서 스마트폰, 태블릿, 스마트 워치 등 사람들이 하나 이상의 모바일 기기를 사용하는 것이 보편화 되었다. 그러나 대부분의 모바일 기기를 지속적으로 사용하기 위해서는 모바일 기기 내부의 배터리를 충전해야 한다[1]. 하지만 배터리의 물리적 한계로 인해 대부분의 모바일 기기들은 장시간 사용하는 것이 어렵다. 보편적인 배터리 충전 방식으로는 전원 공급 장치와 모바일 기기를 케이블로 연결하여 충전하는 방식을 사용한다. 하지만 이러한 방식은 충전 과정 중 모바일 장치의 물리적 이동 거리를 제한한다는 단점이 있어 무선 충전기술을 도입하는 계기가 되었다. 무선 충전기술은 케이블을 사용하는 유선 충전의 한계점을 극복하기 위해, 코일의 유도 전류 현상을 이용하여 전원을 공급하는 장치이다. 무선 전력 전송기술 중 유도 전류를 사용하는 자기 유도 방식과 공진 물체의 에너지 교환 원리를 사용하는 자기 공진 방식으로 구분된다. 자기 공진 방식은 5cm 미만의 전력 전송 거리로 제한되는 자기 유도 방식에 비해 2m 이상의 거리에서도 전력 전송이 가능하다는 장점이 있다. 최근 자기 공진 방식 기반의 무선 전력 전송기술은 지속적인 발전을 통해 최대 15m~30m까지 장거리에서 전력을 전송할 수 있다. 하지만 이러한 자기 유도 무선 전력 전송 방식은 아직 인체에 대한 유해성 검증 등의 안전 검증[2]과 기술 적용에 대한 경제성, 등 추가적인 발전 필

† 교신저자

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업(IITP-2022-2021-0-01816, 20%)및 IITP 정보보호국제공동연구과제의 지원(RS-2022-00165794,60%) 및 2020년도 한국연구재단(NRF) 연구과제의 지원(NRF-2020R1A2C4002737,20%)을 받아 수행된 연구임.

요 요소가 남아있어, 현재는 OSSIA[3], Energous[4], Powercast[5], Technovator[6], Wi-charger[7]와 같은 무선 충전기술 회사에서 사용하거나 연구실 단위에서 연구가 활발히 진행되고 있다. 본 논문은 이러한 자기 공진 방식의 무선 전력 전송 기술의 발전을 기반으로 자기 공진 방식의 무선 전력 전송기술이 적용될 수 있는 상용 서비스 환경을 분석하고, 이러한 상용 서비스에서 발생할 수 있는 보안 위협[8] 중 서비스거부공격 및 주파수 간섭을 통한 보안 위협을 분석하고 이러한 보안 위협을 분석하고 보안 위협을 해소할 수 있는 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 자기 공진 방식의 무선 전력 전송기술에 관한 관련 연구 및 상용 제품에 관해 기술한다. 3장에서는 현재 상용화되고 있는 자기 공진 방식의 무선 전력 전송기술에서 발생 가능한 인증 관련 보안 위협 및 대응 방안을 서술한다. 4장에서는 본 논문의 결론을 제시한다.

II. 무선 전력 전송기술

본 장에서는 현재 사용되고 있는 무선 전력 전송기술 중 대표적인 기술[9]인 자기 유도 방식의 무선 전력 전송기술과 자기 공진 방식의 무선 전력 전송기술에 관해 기술한다.

2.1 자기 유도 방식의 무선 전력 전송기술

자기 유동 방식은 현재 가장 많이 사용되고 있는 모바일 기기 무선 전력 전송기술이다. DC 전원에서 발생한 전원이 인버터를 통해 고주파를 생성하고 해당 고주파는 송신 코일을 통해 자기장을 생성해 모바일 기기 등에 부착된 수신 코일에서 전류를 유도하는 방식을 사용한다. 이러한 기술은 WPC(Wireless Power Consortium)에서 제정한 Qi 표준이 대표적으로 사용하며, 표준에 따라 'selection', 'ping', 'identification & configuration', 'power transfer' 의 4단계의 통신 프로토콜로 구성된다. 2015년에는 15W급 무선 충전이 가능한 1.2 버전을 출시하였다.

2.2 자기 공진 방식의 무선 전력 전송기술

자기 공진 방식은 같은 주파수로 공진하는 두 매체에서 전자파가 다른 매체로 이동하는 현상을 이용한 무선 전력 전송기술이다. 자기 공진 방식의 무선전력전송은 2007년 MIT의 연구원들에 의해 도입되었다. 2m 이상의 근거리에서도 전력 전송이 가능한 특징을 가진 자기 공진 방식 기술은 자기 공진 방식의 A4WP(Alliance for Wireless Power)에서 제정한 방식이 대표적으로 사용된다. 이 방식의 경우 동시에 다수개의 기기를 충전할 수 있고 근거리에서 충전할 수 있다는 장점을 통해 차세대 무선 충전 방식으로 주목받고 있다[10]. 하지만 자기유도 무선전력 전송방식과 같은 초단거리 무선 충전기술에 비해 인체에 대한 명확한 안전성의 확보가 중요한 과제로 남아있다. 2015년 10~50W급 무선 충전이 가능한 1.3버전을 출시하였다.

III. 무선 전력 전송기술 보안 위협 분석

본 장에서는 자기 공진 방식의 무선 전력 전송기술이 실제 적용될 시 발생할 수 있는 보안 위협에 대해 분석하고 이에 대한 대응 방안을 제시한다.

3.1 서비스 거부 공격

전력 송신 기기와 전력 수신 기기 사이의 전력 전송 정보 교환을 위해 BLE, Zig Bee, 모바일 통신 등 다양한 방법이 사용된다. 무선 충전 서비스를 원활히 제공하기 위해서 서비스 제공사는 각 모바일 장치로부터 전력 전송 데이터를 수신받아 송신 기기에서 전송되는 전력량을 조정한다. 이러한 환경의 경우 전력 전송 데이터 통신에 사용되는 통신 방법을 이용하여 서

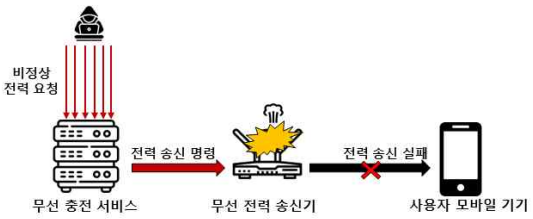

그림 1. DoS 공격을 통한 전력 송신 지연 유발

비스 거부 공격(DoS, Denial of Service) 공격이 발생할 수 있다. [그림1]은 서비스 거부 공격

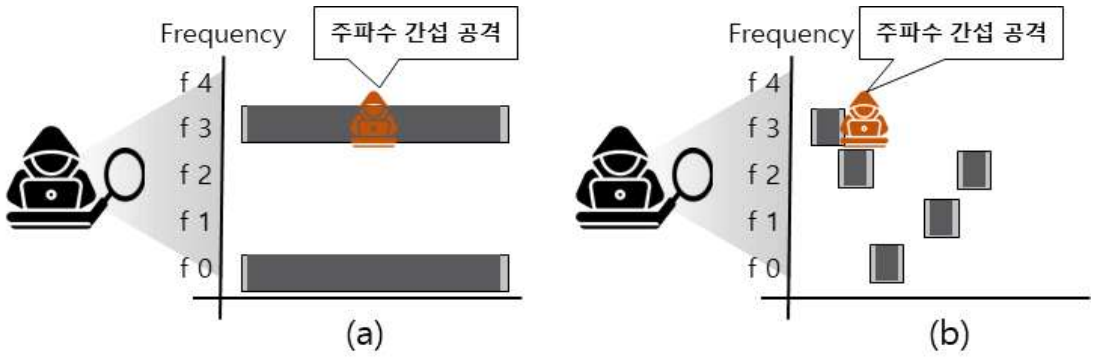

그림 2. 주기적인 주파수 변경을 통한 주파수 간섭 공격 대응 개요

을 통한 무선 전력 송신 지연 유발 개요도이다. 공격자는 통신 모듈을 통해 전력 송신 기기 측에 지속적으로 메시지를 전송하여 통신 모듈의 과부하를 유도함으로써, 송신 모듈에서 제공하고 있는 충전 서비스를 마비시키거나 통신 모듈의 전력 소비량을 증가시켜 전력 전송량을 물리적으로 감소시키는 공격을 수행할 수 있다. 또한, FOD(Foreign Object Detection) 기능을 기반으로 충전 요청 메시지를 지속적으로 전송하여 해당 전력 송신 기기를 통한 전력 전송 서비스를 방해할 수 있다.

3.2 서비스 거부 공격 대응 방안

무선 충전 서비스 거부 공격의 경우, 별도의 네트워크 채널을 생성하는 방법을 통해 위협을 해소한다. 전력 전송과 데이터 통신을 동시에 수행할 수 있는 PPN(Power-Positive Networking) 채널을 생성하는 방법이 대표적이다. 이러한 방법을 위한 연구로써, 기존 무선 주파수 신호와 달리 무선 충전 신호를 사용하여 통신 채널을 구축하여 통신과 전력 전송이 동시에 분리될 수 없도록 하고 채널을 사용하여 PPN을 구축하는 방식의 연구가 제시되었다.

3.3 주파수 간섭 공격

자기 공진 방식 무선 전력 전송기술을 특정 주파수 대역 내에서 전력 전송이 이뤄지는 특징이 있다. 공격자는 이러한 특징을 활용하여 서비스가 제공되는 주파수 대역을 지속적으로 모니터링하여 전력 전송 서비스가 제공되고 있는 주파수 대역을 찾을 수 있다. [그림 2]는 주파수 대역 변경을 통한 주파수 간섭공격의 개요이다. 이러한 방식을 사용하여 인증 여부와 관계없이 주파수 스캐닝을 통해 기존 사용자에게 제공되고 있는 전력 전송을 방해하여 무단으로 전력 전송을 받을 수 있고, 기존의 사용자는 공격자로 인해 정상적인 전력 전송을 받을 수 없다.

3.4 주파수 간섭 공격 대응 방안

A4WP에서 제정한 자기 공진 방식 무선 전력 전송기술의 경우, 무선 전력 전송 과정에서 자기 유도 방식과 달리 1개의 전력 송신기가 다수개의 전력 수신기에 전력을 전달할 수 있다. 전력 전달 과정에서 송신기 및 수신기 간의 상호 통신이 불가능한 기술로써, 통신 과정 중 인증이나 전력 제어 등의 한계점이 있다. 따라서 이러한 문제점을 해소하기 위해서는, 전력 전송 주파수를 일정 시간마다 변경함으로써 공격자가 전력 전송에 사용되고 있는 주파수를 파악하여 무단으로 전력을 수신하는 행위를 방

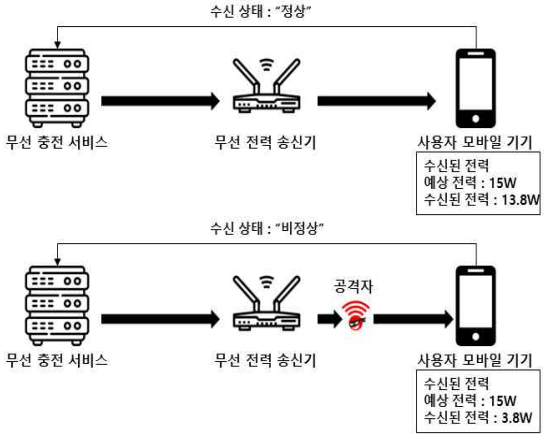

그림 3. 주파수 간섭을 통한 무단 전력

지할 수 있다. [그림2]의 (b)는 주기적으로 전력 전송 주파수를 변경함으로써, 공격자의 무단 사용 행위를 방지하기 위한 전력 전송 주파수 변경 과정의 개요도이다.

따라서 서비스 제공자와 서비스 이용자는 현재 사용되는 주파수 대역에 대한 예상 전력량을 실시간으로 계산해야 한다. 만약, [그림3]과 같이 특정 주파수 대역에서 충전 전력이 급격히 감소하는 경우, 해당 원인을 파악하여 필요한 경우 간섭을 회피하기 위해 충전 주파수를 변경해야 한다.

이러한 방식의 방어 솔루션을 구축하기 위해서는 무선 충전 서비스 제공자는 인증 기반의 액세스를 제공해야 한다. 사용자의 모바일 기기는 송신기와 통신을 통해 인증을 수행하고, 인증과정에서 충전에 사용되는 무선 주파수를 할당받는다. 이후, 사용자가 이동하거나, 해당 주파수에서 전송되는 전력에 이상이 생길 경우, 사용자의 모바일 기기는 즉시 서비스 제공자에게 해당 내용을 전달하여 새로운 무선 전력 주파수를 할당받을 수 있다.

IV.결론

최근 모바일 시장의 성장으로 인해 모바일 기기에 대한 무선 전력 충전의 필요성이 증가하고 있다. 이에 따라 무선 전력 전송기술이 점차 고도화되고 있다. 무선 전력 전송기술은 대표적으로 자기 유도 방식과 자기 공진 방식이 사용되고 있다. 본 논문에서는 자기 공진 방식 무선 충전 서비스 시장이 성장함에 따라, 실제 서비스 제공 현장에서 발생할 수 있는 보안 위협과 보안 위협을 해소할 수 있는 솔루션을 제시한다. 본 연구를 통해 추후 자기 공진 기반의 무선 전력 충전기술이 상용화되는 환경에서 무선 충전 서비스에 대한 보안성을 확보할 수 있을 것으로 기대한다.

[참고문헌]

[1] Jang, Byeong-Jun. "휴대용 IT 기기를 위한 WPC 무선 충전 표준 (Qi) 소개." The Proceeding of the Korean Institute of Electromagnetic Engineering and Science 23.6 (2012): 32-37.

[2] 강준석, et al. "상용 자기유도방식 무선전력 전송 시스템의 인체영향 분석." 한국전자파학회논문지 28.5 (2017): 382-390.

[3] https://www.ossia.com/

[4] https://energous.com/

[5] https://www.powercastco.com/

[6] https://technovator.co/

[7] https://www.wi-charge.com/

[8] 정현주, and 이근호. "모바일 기기에서 자기 공진방식 무선충전의 보안 위협 및 보안요구사항." 한국정보처리학회 학술대회논문집 21.1 (2014): 495-498.

[9] Choe, Hyo-Sang, and In-Seong Jeong. "무선전력전송 (Wireless Power Transfer) 시스템의 기술개발 현황과 동향." 전기의세계 66.2 (2017): 24-28.

[10] Kim, Yong-Hae. "자기공진형 무선 전력전송 기술." The Magazine of the IEIE 38.9 (2011): 17-22.