한국정보보호학회
Korea Institute of Information Security & Cryptology

Proceedings

2021년 한국정보보호학회 하계학술대회

CISC-S'21

Conference on Information Security and Cryptography Summer 2021

2021년 6월 24일(목)

온라인 컨퍼런스

(개회식 촬영: 한국과학기술회관 12F 아나이스홀)

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology

주관 KAIST 한국과학기술원

후원 과학기술정보통신부 국가정보원 National Intelligence Service Korea 행정안전부

NSR 국가보안기술연구소 National Security Research Institute KISA 한국인터넷진흥원 ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute

쌍용정보통신주식회사 SsangYong Information & Communications Corp.

자기공진 및 전자기파 무선전력전송 기술에 대한 보안위협 분석

노형준* 박기웅†

세종대학교 시스템보안연구실* 세종대학교 정보보호학과†

Security Threats for Magnetic Resonance and Radio Frequency-Based Wireless Power Transfer

Hyeong Jun Noh* Ki-Woong Park†

*SysCore Lab., Sejong University

† Department of Computer and Information Security, Sejong University

요 약

최근 무선전력전송 기술에 대한 연구 및 개발이 활발히 이루어지고 있다. 무선전력전송 기술은 전송방식 및 원리에 따라 자기장, 전자기파, 초음파 방식 등으로 세분화할 수 있다. 본 논문에서는 다양한 무선전력전송 방식 중 기술적 성숙도가 높아 비교적 상용화에 근접한 자기공진 방식과 전자기파 방식의 보안위협을 분석한다. 자기공진방식과 전자기파방식의 무선전력전송 기술은 기기가 충전기와 접촉하지 않고 비접촉식 충전이 가능함에 따라 그 과정에서 발생할 수 있는 다양한 보안위협이 존재해 사용자의 피해가 발생할 수 있기 때문이다. 따라서 본 논문에서는 자기공진방식과 전자기파방식의 무선전력전송에 관하여 설명하고 두 방식을 활용한 무선전력전송 기술이 상용화 되었을 시 발생할 수 있는 보안위협에 대해 연구한다.

I. 서론

전 세계 무선충전시장 규모는 2021년에 45억 달러로 예상되고 있으며 2026년에는 134억 달러까지 성장할 것으로 예상된다. 더불어 2021년부터 2026년까지 연평균 증가율은 24.6%에 이를 것으로 예상된다[1]. 이는 무선전력전송 기술이 주목받고 있음을 나타내는 수치라고 할 수 있다.

무선전력전송 기술은 전기 에너지를 무선으로 전달하는 기술이다. 특히, 전기에너지를 전달 받는 매체가 배터리인 경우 '무선충전 기술'이라 부른다[2]. 현재 무선전력전송 기술은 전송방식에 따라 자기장, 전자기파, 초음파 방식으로 구분할 수 있다. 자기장 방식은 자기유도와 자기공진방식으로 세분화할 수 있으며 전자기파방식은 Radio Frequency(RF), 적외선으로 구분 할 수 있다[3].

무선전력전송 기술에는 위와 같은 다양한 방식이 있지만 본 논문은 기술적 성숙도가 높아 비교적 상용화에 근접해 모바일 디바이스에 적용 가능한 자기공진과 전자기파방식을 분석하고, 무선전력전송 기술 인터페이스에 기인하여 보안위협 분석 결과를 나타낸다.

자기공진, 전자기파방식 무선충전은 충전기와 접촉하지 않고 이동간에 기기를 충전시킬 수 있다는 점에서 공간 제약이 없다는 것이 큰 특징이다. 위 방식을 이용한 무선전력전송 기술이 상용화가 이루어진다면, 외부에서 정당한 비용

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No.2019-0-00426, 50%) 및 한국연구재단 (No.NRF-2020R1A2C4002737, 50%)의 지원을 받아 수행된 연구임.

을 지불하고 이동 간에 충전할 수 있는 서비스 또한 등장할 수 있음을 예상할 수 있다.

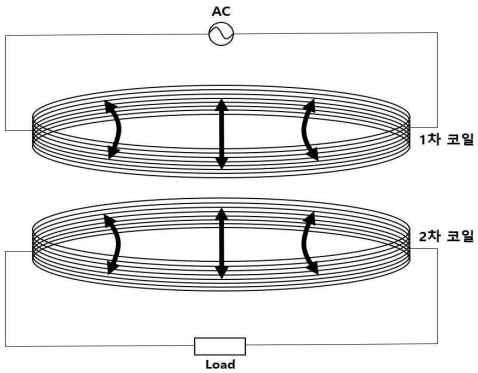
하지만 위 무선충전 기술은 전력 전송 과정에서 발생하는 보안위협과 전력 송·수신기간 통신 과정에서 보안위협이 발생할 수 있다. 따라서 본 논문에서는 자기공진, 전자기파 방식 무선충전시스템의 구동구조를 분석하고, 두 방식 모두 통신 제어 채널이 존재한다는 점에 초점을 맞추어 이와 관련하여 발생할 수 있는 보안위협에 대해 분석한다.

II. 무선전력전송 기술 및 인터페이스 분석

본 장에서는 자기공진방식과 전자기파방식의 무선전력전송 기술에 대하여 알아보며 상이한 두 방식의 시스템 구동원리를 분석하고 인터페이스 분석을 통해 보안위협을 도출한다..

2.1 자기공진방식 무선전력전송

자기공진방식은 송·수신 코일이 같은 주파수를 사용하여 에너지를 전송한다. 이는 자기공진 원리에 의해 송신 코일에서 발생하는 전자기를 수신 코일이 받아 전류로 변환하여 전력을 얻어 충전하는 원리다[4]. 자기공진방식을 이용하면 한번에 여러 대의 기기를 동시에 충전할 수 있으며, 충전기와 직접 접촉하지 않고 10m 내외에서 충전할 수 있다는 것이 특징이다.

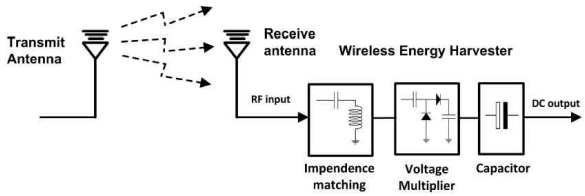


[그림 1] 자기공진방식 전력 전송 개념

현재 자기공진방식 무선충전은 Airfuel Alliance가 주도하여 표준을 제공하며 세계 각국 기업에서 표준에 따라 연구 및 개발 중에 있다. 이 표준에 따르면 Power Transmitting Unit(PTU)과 Power Receiving Unit(PRU)간 Bluetooth Low Energy(BLE)를 이용하여 무선충전 상태를 제어한다[4].

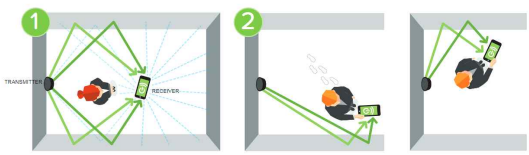
2.2 전자기파방식 무선전력전송

전자기파방식은 무선 주파수를 활용하여 에너지를 전달하는 방법으로 자기공진방식보다 원거리 전송이 가능하며 여러 대의 기기를 동시에 충전할 수 있다. 빔포밍 방식을 사용하여 에너지를 원하는 방향으로 전달할 수 있어 대용량 전력전송이 가능하다[3].



[그림 2] 전자기파방식 전력 전송[4]

전자기파방식 무선전력전송은 중국, 일본 등에서 발표된 표준이 있지만 세계적으로 채택되어 활발히 연구 중인 표준은 없으며 Airfuel Alliance에서도 준비 중에 있다[5]. 하지만 전자기파방식중 RF를 이용한 무선충전을 개발하고 있는 대표적인 Ossia 기업이 있다. Ossia 사가 개발한 Cota 시스템은 수신기의 위치 및 주변환경을 인지할 수 있어 에너지를 원하는 방향에 집중시키고 전자파로 인한 인체 유해성 문제를 감소시켰다[3].



[그림 3] Cota 시스템 동작 개념[6]

2.3 무선전력전송 인터페이스 분석

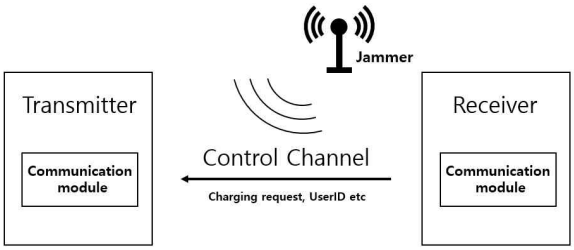
자기공진방식과 전자기파방식은 전력을 전송함에 있어 상이한 구조를 보여준다. 하지만 지정된 기기에 전력을 전송하기 위해서는 송·수신기가 연결되어 있거나 송신기에 수신기의 정보가 등록되어 있어야 한다. 이러한 점을 고려했을 때 전력을 보내는 물리 채널과 통신에 필요한 제어 채널이 따로 존재한다는 것을 알 수 있다. 따라서 두 방식의 공통점은 무선으로 전력을 전송한다는 것과 지정된 기기에 전력을

전송하기 위해 송·수신기간 통신 제어 채널이 필요하다는 것이다.

III. 보안위협 분석

본 장에서는 자기공진방식과 전자기파방식 무선전력전송이 상용화 되었을 때 송·수신기간 통신 제어 채널에서 발생할 수 있는 보안위협에 대해 분석한다.

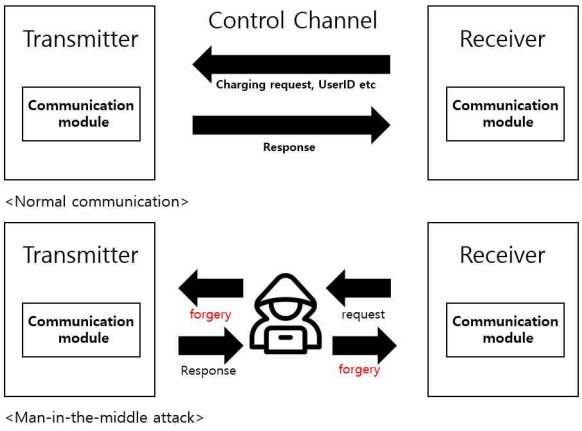
3.1 교란 공격



[그림 4] 교란 공격 개념

교란 공격(Jamming attack)은 송·수신기 간의 통신을 방해하기 위해 의도적으로 간섭을 일으킨다.[7] 따라서 송·수신기는 정상적으로 통신을 하지 못해 최초 연결이 불가능하거나 연결이 끊길 수 있다. 즉, 사용자는 정상적으로 충전 서비스를 이용할 수 없게 된다.

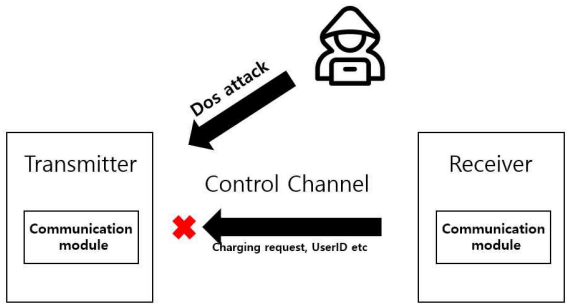
3.2 중간자 공격



[그림 5] 중간자 공격 개념

중간자 공격(Man-in-the-middle attack)을 통해 공격자는 송·수신기간 전송되는 정보를 알아챌 수 있으며 조작까지 할 수 있다. 전송되는 정보에는 사용자 장치 ID, 전력 전송량 및 사용자 주요 정보 등이 있다[7]. 공격자는 알아낸 정보를 자신의 이득을 위해 사용할 수 있으며 충전 중인 사용자에게 피해를 끼칠 수도 있다. 공격자는 사용자 장치 ID를 도용하여 충전 요청을 보내거나 데이터를 조작해 서비스를 이용중인 기기의 충전을 멈출 수 있다.

3.3 서비스 거부 공격



[그림 6] 서비스 거부 공격 개념

서비스 거부 공격(Denial-of-Service attack)은 악의적으로 해당 시스템을 마비시키는 공격이다. 즉, 공격자는 송신기에 의도적으로 많은 요청을 보내 시스템의 자원을 고갈시켜 충전 시스템 자체를 마비시킬 수 있다. 결국 충전 서비스를 이용하지 못하게 만들 뿐 아니라 해당 서비스를 제공하는 기업에게도 큰 피해를 가져다준다.

IV. 결론

본 논문에서는 무선전력전송 기술을 분류하고 비교적 상용화에 근접하다고 여겨지는 자기공진, 전자기파 방식에 대하여 알아보며 기술이 상용화 되었을 시 발생할 수 있는 보안위협에 대하여 분석했다. 전력을 전송하는 과정에서 발생할 수 있는 보안위협보다는 송·수신기간 연결을 통해 네트워크 통신에서 발생할 수 있는 보안위협에 초점을 맞추었다.

무선충전 환경에서 통신 제어 채널이 존재한다는 점은 제시한 보안 위협으로 인하여 사용자뿐만 아니라 서비스를 제공하는 기업에게도 피해가 발생할 수 있다는 것을 내포한다. 보안위협을 해결하기 위한 과정은 한정된 자원의 시스템에 오버헤드를 불러일으켜 서비스 저하로 이어질 수 있지만 서비스를 제공·이용함에 있어 안전한 환경이 우선시 되어야 한다. 따라서 추후 연구로는 오버헤드를 적게 일으키며

보안위협에 효과적으로 대응할 수 있는 방안을 연구할 계획이다.

[참고문헌]

[1] Marketsandmarekts,“Wireless Charging Market with COVID-19 Impact by Implementation“ [Online]: https://www.marketsandmarkets.com/Market-Reports/wireless-charging-market-640.html, Jan, 2021

[2] 문정익, 김성민, 김상원, 조인귀, 손수호, 이호진, ”스마트 무선충전 기술“, ETRI, 전자통신동향분석, 32권 3호, 2017

[3] 양대근, 김당오, 이주용, 조동호, ”차세대 무선전력전송 기술“, ITFIND 주간기술동향, May, 2020

[4] Xiao Lu, Ping Wang, Dusit Niyato, Dong In Kim, Zhu Han, ”Wireless Charging Technologies: Fundamentals, Standards, and Network Applications“, IEEE Communications and tutorials, 2015

[5] Airfuel Alliance. https://airfuel.org

[6] Joel Hruska, “At CES, AA-Sized ‘Forever Batteries’ That Suck Power Out of the air”, [Online]: https://www.extremetech.com/electronics/261944-ces-aa-forever-batteries-suck-power-air, Jan, 2018

[7] Qingzhi Liu, Kasım Sinan Yıldırım, Przemysław Pawełczak, Martijn Warnier, “Safe and Secure Wireless Power Transfer Networks: Challenges and Opportunities in RF-Based Systems”, IEEE Communications Magazine, 2016