무선 전력 전송 기술 보안 연구 동향

Analysis of Wireless Charging Technology And Security Solution Trend

안성규, 박기웅[1)]
Ahn Sung-Kyu, Park Ki-Woong

(05006) 서울특별시 광진구 능동로 209, 세종대학교 SysCore Lab, 정보보호학과
yiimfn@gmail.com, woongbak@sejong.ac.kr

요 약

IT 기술의 발달로 IoT, 의료장치, 모바일 장치 및 EV와 같은 다양한 분야의 장치들은 네트워크 통신 기술과 고성능의 컴퓨팅 기능을 보유하게 되면서 이러한 장치들을 일상 속 생활필수품으로 사용하고 있다. 이러한 장치들의 원활한 이용을 위해서는 지속적인 전원 공급이 안정적으로 유지되어야 한다. 하지만 배터리 용량은 기술적 한계로 인해 사용자의 수요를 충족하지 못하는 상황이며, 전력 공급의 한계를 극복하기 위해 지속해서 전원을 공급할 수 있는 무선 전력 전송기술이 적용되고 있다. 본 논문에서는 무선 전력 전송기술에 대해 분석하고, 무선 전력 전송기술에서 발생 가능한 보안 위협과 보안 위협을 해소할 수 있는 솔루션에 대한 동향 분석 내용을 제시한다. 본 연구를 통해 무선 전력 전송기술 분야에서 보안 위협에 대한 대응 전략을 수립할 수 있을 것으로 예상한다.

Abstract

With the development of IT technology, devices in various fields such as IoT, medical devices, mobile devices and EVs have network communication technology and high performance computing function. Due to the development of these technologies, devices such as mobile devices, IoT devices and EVs have been limited to maintain stable power supply for smooth use. However, due to the increase in network traffic and computing power, the power supply of the device could not satisfy the user's demand, and to solve this problem, a wireless power transmission technology that can continuously supply power is being applied. In this paper, we analyze wireless power transmission technology, and present security threats that may occur in wireless power transmission technology and trend analysis for solutions that can solve security threats. It is expected that through this study, it will be possible to establish a response strategy for security threats in the field of wireless power transmission technology.

키워드: 무선충전, 무선 전력 전송, IoT 보안, 임베디드시스템 보안
Keyword: Wireless Charging, Wireless Power Transfer, IoT Security, Embedded System Security

1) 교신저자

논문투고일자 : 2022. 07. 18 심사일자 : 2022. 07. 21 게재확정일자 : 2022. 08. 18 http://doi.org/10.23019/kingpc.18.4.202208.006

1. 서론

IoT, 의료장치, 모바일 장치, EV(Electric Vehicle) 등 정보기술의 발달과 함께 다양한 플랫폼에서 활용되는 장치들은 네트워크 통신 기술의 장착과 고성능의 컴퓨팅 기능을 보유하게 되었다. 특히 스마트폰 및 태블릿과 같은 모바일 장치는 브라우징, 게임과 사진 촬영을 포함한 다양한 비즈니스 및 엔터테인먼트 활동을 위한 일상적인 도구가 되었다. 이러한 장치들은 사용자에게 편리한 경험을 제공하고 있으며, 최근 시장이 급속도로 성장하고 있는 PM(Personal Mobility) 및 EV(Electric Vehicle)도 다양한 서비스를 제공하고 있다. 이러한 장치의 주요 기능들을 활용하기 위해서는 지속적인 전원 공급이 필수적으로 유지되어야 하며, 이는 배터리 기술의 발전 필요성을 확대하는 계기가 되었다.

배터리 장치는 IoT 및 모바일 장치 등에서 필수 요소로써 활용되고 있지만, 장치에 따라 사용자가 필요로 하는 전력 사용 시간을 충족하지 못하는 경우가 많아졌다. 배터리의 용량을 증가시키는 연구가 지속해서 연구되고 있지만, 기술적 한계로 인해 수요를 충족하지 못하고 있다. 이러한 문제를 해소하기 위해, 배터리 충전 방식의 편의성을 제공하기 위한 다양한 무선 전력 전송 방식 기반의 무선충전 제품 및 서비스가 출시되고 있다[1]. 이러한 기술들을 통한 무선충전 제품 및 서비스로는 모바일 장치 무선충전 및 체내형 의료장치 무선충전, EV 무선충전 기술 등이 활용되고 있다. 현재 무선충전 기술에 관한 연구는, 전력 전송에 대한 효율성 및 휴대성 확대에 대한 초점이 맞춰져 있어 무선충전 기술을 대상으로 하는 보안 위협에 대해 대응 적용 가능한 연구 사례가 적다. 일례로, 기존의 유선 충전 환경에서 발생하는 보안 위협 역시 무선충전 기술 환경에서 적용될 수 있으며, 전파 전송 및 비접촉 충전이라는 특징을 가진 무선충전 기술환경에서는 공격자가 사용자의 무선충전 환경 시스템 내부를 관찰하거나 조작할 가능성이 있다.

이와 관련된 연구로써, 본 논문 이전에 관련 연구를 진행하였으며[2], 본 논문에서는 이전 연구에 이어 무선충전 환경에서 발생 가능한 보안 위협 문제점을 해소하기 위해 여러 무선 전력 전송기술에서 발생 가능한 보안 위협들에 대해 분석하고, 발생 가능한 보안 위협에 대응할 수 있는 보안 솔루션 연구를 분석하고 제시한다.

본 논문의 2장에서는 무선 전력 전송기술을 분석하고 해당 문선 전력 전송기술의 동향에 대해 분석 및 제시한다. 3장에서는 2장에서 기술한 무선 전력 전송기술을 대상으로 발생 가능한 공격 사례와 취약점 분석 연구 등을 기반으로 무선 전력 전송기술 보안 위협을 제시한다. 4장에서는 3장에서 제시한 무선 전력 전송기술 위협을 해소할 수 있는 기존의 솔루션 기술을 분석하고 제시한다. 5장에서는 본 논문의 결론을 제시한다.

2. 무선 전력 전송기술 분석 및 기술 동향

본 장에서는 무선 전력 전송기술에 대해 분석하고 기술별 분류 및 활용 사례에 관해 기술한다. 대표적인 무선 전력 전송 기술로는 <표 1>과 같이 자기 유도 방식, 자기 공진 방식, 전자파 및 광학 기반

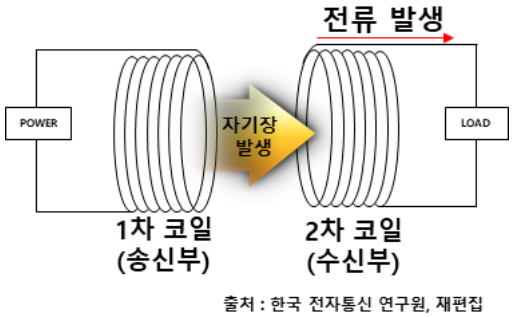
〈표 1〉 무선 전력 전송기술 종류

방식	자기 유도	자기 공진	전파 및 광학
동작 원리	코일 간 전자기 유도 현상	공진주파수가 같은 코일 간 자기 공진 현상	안테나의원역장 방사 현상 광전 효과 기반
장점	수 cm 이내 전송에 유리 코일 소형화에 유리	수 m 이내 전력 전송에 유리 코일 간 정렬 자유도가 높음	장거리 이상의 원거리 에너지 전송이 가능
단점	전송 거리가 짧음 코일 간 정렬에 민감	코일 설계 난이도가 높음 전자파 환경 극복 필요	전송효율이 낮고 환경문제 고려 필요
사용 분야	모바일 기기, EV	모바일 기기, 주행 중 전기자동차, 공공서비스 등	우주 태양광 발전, 무선 전력 전송 등

의 무선충전 방식이 있다[3] [4]. 현재 가장 많이 상용화되어 있는 기술은 자기 유도 방식이며, 자기 공진 방식 역시 상용화 단계에 진입하고 있다. 전자파 및 광학 방식은 실험단계에 들어서 있다.

2.1 자기 유도 방식의 무선 전력 전송

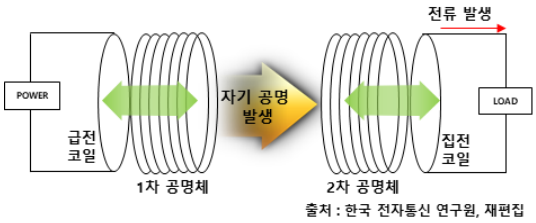
자기 유도 방식의 무선 전력 전송기술은 (그림 1)과 같이 전력 전송을 위해 전자기 유도 기술을 활용한다[5]. 자기 유도 충전은 2개의 유도 코일을 기반으로 하여 하나의 코일에서 교류 전자기장을 생성하고 다른 코일에서 전자기장에서 전력을 수신하여 전류로 변환시켜 장치에 공급하는 역할을 수행한다. 일반적으로 상용화되는 무선 자기 유도 충전기의 유효 거리는 수 cm 미만으로 제한된다. 이러한 자기 유도 충전 기술은 충전 패드 및 모바일 장치에 코일이 이식되어, 수신되는 장치에 장착된 코일에 전력을 공급할 수 있다. 자기 유도 기반 충전 방식은 90% 이상의 효율로 전력을 전송한다는 장점이 있지만[6], 두 개의 코일이 정렬되지 않을 경우 효율이 급격하게 낮아진다는 단점이 있다. 이러한 단점을 해소하기 위해 다중 코일을 활용한 자기 유도 방식을 충전 기술이 연구되었으며, 이러한 기술은 사용자에게 코일의 정확한 정렬을 강요하지 않는다. 이와 같은 자기 유도 방식을 활용한 충전 기술은 WPC(Wireless Power Consortium) 연합의 Qi 표준을 기반으로 제작된다[7].



(그림 1) 자기 유도 방식 무선 전력 기술 원리[7]

2.2 자기공명 방식의 무선 전력 전송

자기공명 방식은 (그림 2)와 같이 2개의 코일이 같은 주파수로 공진하였을 때 전자파가 근거리 자기장을 통해 한 코일에서 다른 코일로 전달되는 특성을 활용한 무선 전력 전송기술이다. 코일 간의 유도전류가 발생하는 것은 자기 유도 방식과 유사하다는 특징이 있으나 각 코일 간의 주파수가 동일하게 공진함으로써 1차 코일에서 2차 코일로 에너지가 이동할 수 있어 자기 유도 방식보다 장거리로 전력을 전달 가능하다는 장점이 있다. 이와 같은 자기 공진 방식을 활용한 충전 기술은 A4WP(Alliance for Wireless Power) 연합의 표준화를 기반으로 제작된다[5].



(그림 2) 자기 공진 방식 무선 전력 전송 원리 [7]

2.2 전파 및 광학 방식의 무선 전력 전송

전파 방식의 무선 전력 전송기술 중 하나로, 마이크로파(Microwave)를 이용한 무선 전력 전송기술이 있다. 마이크로파는 1~10cm의 파장 특성과 직진성이 강하다는 특성이 있다. 이를 통해 수백 Km 이상의 무선 전력 전송이 가능하다.

광학 방식의 무선 전력 전송기술 중 하나로써, 레이저를 기반으로 전력을 전송하는 LPT(Laser Power Transfer) 기술은 1965년에 제안된 광전효과의 원리를 기반을 연구되었다. 이러한 레이저 기반 전력 전송은 수백m 이상의 초장거리 전력 전송을 목표로 연구되고 있다. 하지만 이러한 LPT의 단점으로 에너지 전달 효율이 최대 20~30%로 다른 전력 전송기술에 비해 낮다는 특징이 있다[3].

2.4 무선 전력 전송기술 활용 사례

2.4.1 모바일 장치 분야

스마트폰, 무선 이어폰 등과 같이 모바일 기기는 무선 전력 전송기술이 활발하게 적용되고 있는 분야이다. 최근 출시되는 스마트 기기의 대부분에서 무선충전 전력 전송기술을 탑재하고 있으며, 모바일 장치 분야에서는 (그림 3)과 같이 자기 유도 방식의 무선 전력 전송기술을 통한 무선충전 방식이 가장 활발하게 사용되고 있다. 기존 충전 방식이었던 유선 충전 방식의 단점을 해소하기엔 자기 유도 방식의 무선충전 기술의 장점이 충분하지 않다.

출처: 삼성전자 출처: Apple

(그림 3) 무선충전 기능이 포함된 모바일 기기[8][9]

자기 유도 방식의 무선충전 기술은 기존 유선 충전 방식보다 충전량을 많이 공급할 수 없는 특징과 충전 중 이동 제한이 있다. 따라서 이러한 제한점으로 해소하기 위해 다양한 제조사 또는 연구 분야에서 자기 공진 또는 전파를 활용한 수 미터 거리의 중거리 무선충전 방식 기술을 개발 중이며, 최근 샤오미 社에서는 전파 방식의 충전 서비스를 출시하기도 하였다[9].

출처: Xiaomi

(그림 4) Xiaomi 社 'Mi Air Charge'[9]

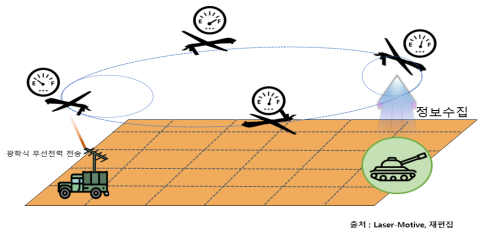
2.4.2 이식형 의료장치 분야

현재 무선 전력 전송을 통한 무선충전 시스템은 광범위한 범위에 적용되고 있다. 무선 전력 전송기술이 활용되고 있는 분야 중 이식형 의료 장치(IMD, Implantable Medical Device)의 경우, 무선충전 기술의 적용 사례는 많은 이점을 가져왔다. IMD는 사용자의 신체 내부에 이식되어 지속해서 사용자의 건강상태를 모니터링 하는 역할을 수행한다. 그러나 이러한 장치의 핵심 성능 중 하나는 사용자의 몸속에 이식된 후, 얼마나 오랜 시간을 정상적으로 작동할 수 있는지에 대한 조건이 있다. IMD는 사용자의 인체 내부에서 자체적으로 보유한 배터리를 기반으로 동작하는데, 해당 배터리가 완전히 소모된 경우, 사용자는 외과적 처치를 통해 IMD를 교체해야 한다. 또한, 환자의 인체 내부에 있는 배터리 내부 화학물질의 유출 문제가 발생할 경우, 사용자의 극심한 위험을 초래할 수 있다. 이러한 문제점을 해소하기 위해 인체 내부에 있는 IMD에서 유선 와이어를 연결하여 피부에 배치하여, 외과적 처치 없이 전력을 공급할 수 있는 방식이 제안되었으나, 피부에 있는 와이어로 인해 상처가 발생하거나 심각한 흉터 및 감염이 발생할 수 있어 의학적으로 적용하기 어렵다는 단점이 있다[11]. IMD 성능 측면에서는 IMD 자체 특성으로 인해 소형화를 유지함으로써, 동시에 장착되는 배터리의 크기 역시 소형화가 필수적으로 요구된다. 이러한 배터리의 소형화는 컴퓨팅 연산 능력을 감소시킬 수 있다. 이러한 문제점을 해소하기 위해 IMD를 위한 다양한 무선 전력 전송 방식이 적용되었다. IMD를 위한 무선충전 기술은 배터리의 수명을 증가시키고, 이를 통해 IMD의 제한적이었던 컴퓨팅 자원을 연산량을 증가시킬 수 있어 사용자에게 더 고도화된 의료 서비스를 제공할 수 있다. 현재 의료분야에서 활용되고 있는 의료장치 무선충전 기술의 경우 주로 자기 유도 방식을 활용한 무선충전 방식을 사용한다. IMD를 피부 하단에 위치하도록 이식한 후, 전원이 필요할 때 해당 이식 위치에 충전 패드를 접촉함으로써 자기 유도 방식을 통해 IMD 내부 배터리를 충전할 수 있다.

(그림 5) IMD 무선충전 개요도

2.4.3 UAV(Unmanned Aerial Vehicle) 분야

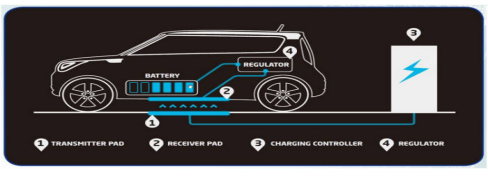
UAV의 운영과정에서의 핵심적인 필요사항은 UAV의 운용 시간이다. 일반적으로 UAV 임무 중 하나는 물리적인 특정 위치의 지속적인 모니터링을 해야 한다[12]. 따라서, 운용 시간이 길어질수록 UAV는 해당 위치에 대한 정확하고 실시간적인 정보를 확보할 수 있다. 이러한 운용 요구사항을 충족하기 위해 배터리 전력량의 증가가 필요하지만, 배터리가 증가하는 경우 UAV 기체 무게가 대폭 상승하게 되어, 해당 UAV의 다른 구성품을 제거하거나 UAV 자체를 더욱 크고 강하게 제작해야 하는 단점이 있다. 이러한 문제를 해소하기 위해 UAV가 비행하는 도중 지속적인 전원 공급을 가능하게 하는 솔루션이 연구되고 있다. 이러한 과정은 유선 또는 무선으로 적용할 수 있다[13]. 유선 충전의 경우 UAV가 비행 도중 전원 공급장치에 접근하여 유선 연결을 수행하고 충전을 하는 동안 비행 상태를 유지하는 방식을 사용한다. 이러한 방법은 무선충전의 방식에 비해 빠른 충전이 가능하지만, UAV의 갑작스러운 돌발상황에 의해 전원 공급장치와 UAV가 동시에 위험에 빠질 수 있다는 단점이 있다. 또 다른 전원 공급 방식으로써, 전원 공급장치에서 무선 전력 전송 방식을 사용하여 주변에서 비행하고 있는 UAV들을 대상으로 전원을 공급해주는 방식이 있다. 이러한 방식은 여러 UAV를 동시에 충전 가능한 장점뿐만 아니라, 돌발상황에서도 유연하게 대처할 수 있어, 자산 손실을 방지할 수 있다는 장점이 있다.



(그림 6) 지상형 무선 전력 전송 장치[13]

2.4.4 EV(Electric Vehicle) 분야

최근 EV 시장이 급속도로 성장하면서 다양한 EV가 출현하였다. 이러한 EV와 기존 화석연료 기반 차량의 차이점의 EV의 경우 배터리를 포함하여 전기를 동력으로 주행하기 때문에, 배터리의 상태에 차량 주행 거리 등의 제한점이 생길 수 있다[14]. 특히 EV의 경우, 기존 화석연료 기반 차량과 비교하면 해당 전원을 충전하는 데 오랜 시간이 소요된다는 단점이 있다. 이러한 문제를 해소하기 위해, EV를 위한 다양한 방식의 무선 전력 전송 방식 기술이 적용되었다. 현재 EV 분야에 가장 활성화된 무선충전 방식은 무선 충전 패드를 통한 EV 배터리 충전 방식을 사용한다. 이는 사용자가 EV를 조작해 특정 패드 위에 위치하는 경우 자기 유도 방식의 무선 충전 패드를 사용하여 전원을 공급한다. 주차장 또는 차고와 같은 곳에 전원 패드를 공급하는 경우, 사용자는 전원 공급 인프라를 찾아야 하는 단점을 해소할 수 있다. 또 다른 방식의 경우, EV 차량 주행 중 실시간 충전을 목표로 하는 연구가 진행되고 있다. 이러한 방식은 EV의 주행 간 특정 충전 포인트를 통해 전력을 전달받아 주행과 동시에 충전을 통해 주행 가능 거리를 확보할 수 있다. 하지만 주행 중 충전 방식의 경우 효율성의 문제로 아직 연구 단계에서 진행되고 있다.



(그림 7) EV를 위한 충전 패드 기반 무선충전[15]

(그림 8) (a) 무선 전력 전송 환경 보안 위협 사례 (b) 무선 전력 전송 환경 보안 솔루션 적용 사례[2]

3. 무선 전력 전송기술 보안 위협

본 장에서는 (그림 8)과 같이 무선 전력 전송 기술기반 환경에서 발생 가능한 보안 위협과 관련된 연구 및 공격 사례 등을 서술한다. 본 논문에서는 무선 전력 전송 공격 사례를 무선 전력 충전 시스템에서 발생 가능한 대표적인 공격 사례인 무선 전력 전송 중 전력 부채널 공격, Denial of Service 공격, 인증 우회 공격을 대상으로 분석을 수행하였다.

3.1 자기 유도 방식의 무선 전력 전송 보안 위협

자기 유도 방식의 무선충전 특성상 근거리 접촉이 유지 되어야 한다는 한계점이 있다. 이러한 특성을 사용하여 공격자는 충전 패드를 해킹하거나, 공격자가 별도로 충전 패드를 은닉하여 공격을 수행할 수 있다. 또한, 공격자는 전력 공급 역할을 하는 특성을 활용하여 충전 패드를 조작해 충전 대상 기기의 배터리를 물리적으로 공격할 수 있다[16]. 본 장에서는 물리적인 거리가 가까운 특성을 가진 자기 유도 방식의 무선충전 환경에서 발생 가능한 보안 위협에 대해 분석한다.

3.1.1 부 채널 공격

무선 전력 충전 시스템을 대상으로 하는 전력 부채널 공격(Power Side-Channel Attack)은 전력 송신장치에서 전력 수신 장치로 전송되는 전력량을 분석하여 전력 수신 장치의 행위를 분석하는 공격으로써, 공공 유선 충전 인프라를 사용하는 이용자를 대상으로 전력 부채널 공격 위협 분석 연구에 기반을 둔다. 자기 유도 방식의 무선충전 방식의 경우 충전 중 전력 수신부의 행위에 따라 전력 송신부의 송신 전력량이 변하는 현상이 발생한다. 이러한 현상은 유선 전력 전송 방식과 취약 요소와 흡사하여 유선 전력 전송의 보안 위협을 적용할 수 있는 특징이 있다. 또한, 유선 충전 방식의 경우 사용자가 직접 케이블을 장치에 연결해야 공격할 수 있지만, 자기 유도 방식의 무선충전 방식의 경우 (그림 9)와 같이 사용자가 사용하는 무선충전 서비스 또는 사용자가 충전기기를 자주 배치하는 장소(책상, 거치대 등)에 악성 무선 충전기를 설치하여 공격할 수 있다. 이러한 특징을 이용한 위협 분석 연구 사례로써, 소모 전력 분석을 통해 자기 유도 방식 기반의 무선 전력 충전 기기를 이용하고 있는 모바일 장치의 웹사이트 핑거프린팅(Finger printing) 공격을 통한 정보 유출 연구를 수행한 사례가 존재한다[18].

출처 : 서울시

(그림 9) 공공 무선충전 플랫폼[17]

3.2 자기 공진 방식의 무선 전력 전송 보안 위협

자기 공진 방식의 무선충전 환경은 전력 송신 기기와 전력 수신 기기의 거리가 1m 이상이어도 충전이 가능한 특징이 있다. 공격자는 이러한 특징을 이용하여 전력 송신 기기와 전력 수신 기기 사이에서 데이터를 가로채거나, 데이터 변조 등의 공격을 통해서 전력 송신 기기 및 전력 수신 기기를 대상으로 공격을 수행할 수 있다. 본 장에서는 물리적 거리가 존재하는 특징을 이용한 자기 공진 방식의 무선충전 환경에서 발생 가능한 공격 방식에 대해 분석한다.

3.2.1 Denial of Service 공격

자기 공진 방식의 무선 전력 충전 방식의 경우, 충전 프로세스 진행 및 서비스 인증 등의 절차를 진행하기 위해 전력 송신 기기와 전력 수신 기기 간의 통신과정을 수행한다. 해당 통신을 위해 BLE 또는 ZigBEE 와 같은 별도의 통신 모듈을 사용할 수 있다. 이러한 특징을 가진 자기 공진 방식의 무선 전력 충전 플랫폼을 대상으로 BLE, ZigBEE 와 같은 통신 모듈을 이용하여 통신 과부화를 유도하여 정상적인 서비스를 방해하는 악성 행위를 수행할 수 있다. 동시에 여러 수신 장치에 전력을 공급할 수 있는 자기 공진 방식의 특성상 전력 공급장치에 부착된 통신 모듈에서 전력을 과도하게 소모할 경우, 정상적인 전력 전송 절차를 수행할 수 없다. 이러한 공격 방식은 크게 두 가지의 방식을 사용할 수 있다. 첫 번째로는 통신 모듈의 소비 전력을 과도하게 증가시켜 정상적인 서비스를 방해하는 공격과 무선충전 서비스의 FOD(Foreign Object Detection) 기능을 기반으로 인증 메시지를 조작하여 가짜 수신 장치가 있는 것으로 위장함으로써, 전력 송신장치가 과도한 전력을 소비하도록 유도할 수 있다. 이러한 특징을 이용한 위협 분석 연구 사례로써, DoS 공격 상황을 인식하고 (Power Positive Network)를 이용함으로써, 통신 과부하 시 전력 송수신 피드백만으로 통신이 가능한 솔루션을 제시함으로써, 무선 전력 전송 DoS 공격으로 인한 전력 전송량의 감소를 방지하는 관련 연구를 수행한 사례가 존재한다[19].

3.2.2 인증 우회 공격

일부 무선충전 서비스 및 플랫폼들은 전력 송신기기와 전력 수신기기 사이의 인증절차를 통해서만 전력 전송서비스를 제공한다. 이러한 서비스를 대상으로 인증 과정을 우회하거나 사용자의 인증 정보를 도용하거나 변경하여 허가되지 않은 전력 전송을 수신함으로써 전력 공급 서비스를 대상으로 추가적인 비용을 발생하게 하는 공격을 수행할 수 있다. 자기 공진 방식 및 전파 방식 및 광학 방식의 경우 자기 유도 방식의 무선충전 방식보다 비교적 먼 거리에서 전력 전달이 가능하여 사용자와 충전 플랫폼 사이에서 중간자 공격 등, 무선 통신을 통한 인증 우회 방식의 위협이 존재할 수 있다.

4. 무선 전력 전송 보안 솔루션 분석

본 장에서는 3장에서 제시한 무선충전 방식에 관한 위협 연구 등을 기반으로 무선 전력 전송기술 보안 위협에 적용 가능한 보안 솔루션에 관한 연구들에 대해 제시한다.

4.1 부 채널 공격 방지 연구

기존의 유선 전력 전송 및 충전 환경에서 수행되었던 부 채널 공격 방지 솔루션은 하드웨어 및 소프트웨어 솔루션으로 구분되어 있다. 하드웨어 솔루션의 경우 유선 충전 케이블을 별도의 전력 안정화 하드웨어에 연결하여 전력 공급을 받는 방법을 사용한다. 소프트웨어 방식의 솔루션의 경우 충전 시 전원에 무작위 버스트를 주입하는 방식을 사용한다. 이에 비해, 무선충전 방식의 경우 충전기와 기기 사이에 적절한 충전 하드웨어를 적용하기 어려우므로 소프트웨어 방식의 솔루션을 적용하여 무선충전 시 공격자가 전력 분석 공격을 수행하기 어렵게 할 수 있다[3].

4.2 인증 우회 방지 연구

자기 유도 방식 무선충전의 경우, Qi 표준을 통해 인증 우회 공격 방지 솔루션이 대표적으로 수행된다. Qi표준 1.3[20]부터 무선충전 환경에서 암호화 인증을 수행하여 인증된 장치에만 충전기에서 제공 가능한 최대 전력을 제공하는 방법을 사용한다. 이를 통해 부 채널 공격 및 인증 우회 등을 목적으로 하는 가짜 장치를 탐지하는 기술을 적용하여 전력 수신 장치의 피해를 최소화하는 기술을 도입하였다. CWD-WPT 충전 시스템[21]은 EV 환경에서 메시지 프라이버시와 무결성, 시스템 요소의 상호 인증, 무선충전 차량의 익명성을 보장하는 CWD-WPT 클라우드 과금 시스템에서 키 관리 및 배포를 위해 서로 다른 암호화 기법을 사용하는 인증 프로토콜을 제시하였다.

4.3 Denial of Service 공격 방지 연구

DoS 공격의 경우, 별도의 네트워크 채널을 생성하는 방법을 통해 위협을 해소한다. 전력 전송과 데이터 통신을 동시에 수행할 수 있는 PPN 채널을 생성하는 방법이 대표적이다. 이러한 방법을 위한 연구로써, 기존 무선 주파수 신호와 달리 무선충전 신호를 사용하여 통신 채널을 구축하여 통신과 전력 전송이 동시에 분리될 수 없도록 하고 채널을 사용하여 PPN(Power-Positive Networking)을 구축하는 방식의 연구가 제시되었다[19]. 이 연구는 에너지 DoS 공격이 기성 임베디드 시스템 플랫폼(Raspberry Pi 및 ESP 8266 SoC 모듈)에 미치는 영향을 연구한다.

5. 결론

정보기술의 발전에 따라 모바일, IoT, EV 등 다양한 분야의 장치에 네트워크 기능이 접목되고 컴퓨팅 능력이 향상되었다. 이러한 장치들의 지속적인 이용을 위해서는 전원 공급의 안정성이 확보되어야 하지만, 물리적, 기능적 한계로 인해 이용자가 만족할 수 있는 전원 공급이 어려운 상황이다. 따라서 이러한 문제를 해결하기 위해 다양한 무선 전력 전송기술이 접목되었다. 본 논문에서는 이러한 무선 전력 전송기술에 대한 동향을 분석하고 무선 전력 전송기술에서 발생 가능한 위협을 분류하고 적용 가능한 보안 솔루션에 대한 동향을 분석 및 제시하였다. 본 연구의 향후 연구로써 무선 전력 전송기술의 특성을 활용한 무선 전력 전송기술 전용 보안 솔루션 연구를 진행할 계획이다.

Acknowledgement

본 연구는 2020년 국방과학연구소에서 주관하는 미래도전국방기술 연구개발사업(UD210029TD)의 지원을 받아 수행되었습니다.

참고문헌

〔1〕 ETRI, "〔표준화 동향〕 무선 전력 전송 표준 기술", 2017.10.12

〔2〕 안성규, 박기웅. "무선충전 기술에 대한 보안 위협 및 보안 솔루션 동향분석." 한국차세대컴퓨팅학회 학술대회 (2022): 216-219.

〔3〕 이동훈, and 김성만. "레이저 무선충전 기술 연구." 한국전자통신학회 논문지 11 (2016): 1219-1224.

〔4〕 이양재,양동민,박기웅, "무선 충전 시스템 사용 권한 검증을 위한 보안 요구사항 도출",한국차세대컴퓨팅학회 춘계학술대회 (2018): 177-180.

〔5〕 Kim, S. M., et al. "The technical trend and future direction of wireless power transmission." Electronics and Telecommunications Trends 29.3 (2014): 98-106.

〔6〕 정현주, and 이근호. "모바일 기기에서 자기공진방식 무선충전의 보안 위협 및 보안요구사항." 한국정보처리학회 학술대회논문집 21.1 (2014): 495-498.
〔7〕 ETRI, https://www.etri.re.kr/webzine/20150313/sub04.html
〔8〕 삼성전자 서비스, https://www.samsungsvc.co.kr/solution/ 25313
〔9〕 Apple support, https://support.apple.com/ko-kr/HT208078
〔10〕 Xiaomi, https://www.mi.com/global/discover/article?id=1653
〔11〕 Taalla, Rajesh V., et al. "A review on miniaturized ultrasonic wireless power transfer to implantable medical devices." IEEE access 7 (2018): 2092-2106.
〔11〕 Lu, Maxim, et al. "Wireless charging techniques for UAVs: A review, reconceptualization, and extension." IEEE Access 6 (2018): 29865-29884.
〔12〕 권영호. "무선 전력환경에서 마이크로 유전자 알고리즘을 적용한 다중드론 배터리 충전 할당 방식." 한국차세대컴퓨팅학회 논문지 18.1 (2022): 29-36.
〔13〕 Nugent, T. J., and J. T. Kare. "LaserMotive White Paper—Power Beaming for UAVs." 2010.
〔14〕 Ahmad, Aqueel, Mohammad Saad Alam, and Rakan Chabaan. "A comprehensive review of wireless charging technologies for electric vehicles." IEEE transactions on transportation electrification 4.1 (2017): 38-63.
〔15〕 김성민, et al. "무선충전 기술동향과 발전방향." 〔ETRI〕 전자통신동향분석 31.3 (2016): 0-0.
〔16〕 Zhang, Jiayu, et al. "Who is charging my phone? Identifying wireless chargers via fingerprinting." IEEE Internet of Things Journal 8.4 (2020): 2992-2999.
〔17〕 서울시, "놀라운 가로등 '스마트폴'로 도시를 더 스마트하게!", https://opengov.seoul.go.kr/mediahub/22504672, 2021.03.17
〔18〕 La Cour, Alexander S., Khurram K. Afridi, and G. Edward Suh. "Wireless Charging Power Side-Channel Attacks." Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021.
〔19〕 Chang, Sang-Yoon, et al. "Power-positive networking: Wireless-charging-based networking to protect energy against battery DoS attacks." ACM Transactions on Sensor Networks (TOSN) 15.3 (2019): 1-25.
〔20〕 Wireless Power Consortium,"COMPLIANCE WITH THE LATEST REVISION OF THE QI SPEC", www.wirelesspowerconsortium.com
〔21〕 Roman, Luis FA, and Paulo RL Gondim. "Authentication protocol in CTNs for a CWD-WPT charging system in a cloud environment." Ad Hoc Networks 97 (2020): 102004.

저자소개

◆ 안성규

- 2011년 ~ 2015년 대전대학교 정보보호학과 학부
- 2015년 ~ 2017년 대전대학교 정보보호학과 석사
- 2017년 ~ 세종대학교 박사과정
- 관심분야: IoT, 임베디드, 스토리지 시스템, 헬스케어 시스템

◆ 박기웅

- 2005년 연세대학교 Computer Science 학사
- 2007년 KAIST Electrical Engineering 석사
- 2012년 KAIST Electrical Engineering 박사
- 2008년 Microsoft Research Asia, Wireless and Networking Group, Research Intern
- 2009년 Microsoft Research, Network Research Group, Graduate Research Fellow
- 2012년 국가보안기술연구소 연구원
- 2012년~2016년 대전대학교 정보보안학과 교수
- 2016년~현재 세종대학교 정보보호학과 교수
- 관심분야: 시스템보안, 모바일-클라우드 컴퓨팅, 보안 프로토콜, 디지털 포렌식