M2M에서 무선충전 시스템의 보안 위협

이근호
백석대학교 정보통신학부

A Security Threats in Wireless Charger Systems in M2M

Keun-Ho Lee
Division of Information Communication, Baekseok University

요 약 최근 IT기술의 발전에 따라 언제 어디서나 이용할 수 있는 M2M기반의 무선 충전 분야의 기술 개발이 빠르게 진행되고 있다. M2M에서 무선충전기술은 무선 네트워크를 기반으로 하기 때문에 다양한 보안의 위협요소가 발생된다. 본 논문에서는 무선 충전 시 무선 네트워크 공격 기반의 인증 및 지불 공격에 대한 위협을 알아보고, 기존의 인증 및 지불을 위하여 무선충전 서비스 상황에 맞는 대응 기법을 제안한다.

• **주제어** : 무선충전, 사물통신, 보안, 위협, 무선네트워크

Abstract The fast-paced development in the field of wireless charger based on M2M, which is available anytime and anywhere, is being underway in accordance with the development of IT technology. Wireless charger technology in M2M has various security threats because it is based on wireless network. The purpose of this paper is to examine the threats of authentication and payment attacks based on wireless network attacks, and to propose the response technique that fit the situation of the wireless charger service by modifying the existing detecting authentication and payment through wireless charger.

• **Key Words** : Wireless Charger, M2M, Security, Threat, Wireless Network

1. 서론

IT를 기반으로 한 정보통신 산업이 발전하면서 많은 제품마다 배터리에 대한 많은 연구가 진행이 되고 있다. 그중에서도 IT 산업의 중심인 휴대폰, 스마트폰, 테블릿 PC 등 휴대용 IT 기기와 에너지 효율화를 위한 전기자동차 등 많은 분야에서 배터리 충전을 위한 무선 충전에 대한 요구가 높아지고 있다. 특히 배터리의 경우 소형화를 통한 에너지 공급을 위해 기기마다 요구되는 전력의 소비는 더욱 커지고 있는 추세이므로 배터리 교환과 충전에 대한 편리성을 위한 고객만족을 위하여 상용 전원에 연결하여 항시 사용할 수 있는 무선 충전 기술에 대한 요구와 연구가 활발히 진행되고 있다.

현재 진행중에 있는 무선 충전 기술은 여러 회사에서 각 회사의 방식에 맞도록 다양한 무선충전 기술이 개발되었으나, 시장의 빠른 변화와 요구를 반영하기 위하여 표준화가 활발히 진행중에 있다. 특히 WPC(Wireless Power Consortium)에서는 Qi 표준을 통한 규격화를 위해 스마트폰 제조사들이 Qi 표준에 의해 제품을 출시하고 있어 무선 충전 기술의 대중화가 되어 가고 있는 단계이다[1].

무선 충전 분야에서는 스마트폰과 같은 소형 기기와 전기자동차와 같은 대형기기에 대한 무선 충전의 분야로 구분된다. 특히 지능형 자동차에서 전기자동차의 충전 시스템 중 무선을 이용한 무선 충전이 중요한 기술로 자리매김하고 있다. 무선충전기술은 무선으로 기기에 에너

*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2013년 2월 25일 수정일 2013년 3월 22일 게재확정일 2013년 3월 22일

지를 전송하고 전송받은 기기는 수신한 에너지를 충전하는 기술을 의미한다. IT기술의 빠른 변화와 발달로 인해 언제어디서든 사용할 수 있는 다양한 디지털기기를 소유하고 있는 상황에서 쉽게 무선으로 충전하는 기술은 다양한 이점과 다양한 서비스 모델을 창출해 낼 수 있는 기술이다. 스마트폰의 경우 고용량의 데이터 처리와 다양한 응용프로그램을 상시로 사용하다보니 배터리가 급격하게 소모되는 문제가 발생하고 있다. 이러한 대안으로 나온 것이 무선 충전 기술이다. 집에서 사용하는 가전의 경우도 전원 케이블을 통해 미관상 좋지 않은 상황이 발생하여 무선충전 기술의 적용을 적극 검토하고 있는 상황이다.

전기자동차의 경우 그린 정책에 의해서 많은 연구와 시제품의 개발이 이루어지고 있다. 향후 대중화가 예상되는 전기자동차의 경우 퇴근 후 충전을 위해 선을 연결하는 부분과, 배터리 충전을 위해 수시로 들고 다니는 부분의 불편함을 해결하기 위하여 주차라인에 주차를 하게 되면 자동으로 자동차 인증을 통해 무선으로 충전이 되는 시스템을 연구하고 있다. 이러한 전기 자동차의 경우 무선 충전 시 정확한 사용자 인증과 사용량에 따른 과금에 대한 지불관련 보안 이슈가 예상되므로 해결책의 제시가 중요하다.

본 논문에서는 다양한 기기들의 무선 충전에 대한 기술적 내용을 살펴보고, 발생 가능한 보안 위협 요소를 분석하고 그에 따른 대응 방법을 제안하고자 한다.

2. 관련연구

2.1 무선 충전 기술

기존의 충전 방식은 직접 기기와 전원 공급선을 연결하거나 배터리를 직접 전원에 접촉하는 전도 충전 방식을 사용하고 있다. 전원 공급선 기반의 전원 공급은 IT 기기의 발달로 개인 별로 사용하는 IT 기기가 증가함에 따라 무선 기반의 충전에 대한 요구사항이 대두되기 시작했다. Qualcomm의 조사에 따르면 무선 충전에 대한 선호도가 높다는 조사 결과를 확인해 볼 수 있다. 다양한 IT 기기의 사용자의 무선 충전에 대한 요구가 높아서 세계시장이 매년 80% 이상 성장할 것으로 예상하고 있다. 이러한 무선충전 기술은 표 1과 같이 전자기 유도 방식, 자기 공진 방식, 전자기파 방식으로 구분되어 진다[1,3].

전자기 유도 방식은 1800년대 전기모터나 변압기에 사용하면서부터 시작되었다. 전자기 유도 방식은 무선 충전 기술 중에서 가장 기본적인 기술이다. 수 mm 내외로 인접한 두 개의 코일에 유도전류를 일으켜 충전하는 방식이다. 두 개의 코일 사이의 자기유도는 코일 사이의 거리 및 상대적 위치에 매우 민감한 문제를 야기한다. 두 코일 사이의 거리가 약간만 떨어지거나 틀어져도 전력 전송 효율이 급격히 떨어지기 때문에 근접거리에서만 사용이 가능하다. 이러한 전자기 유도 방식이 적용되는 분야는 전동 칫솔이나 면도기에서 무선 충전에 이용이 되고 있다[1,3].

자기 공진 방식은 두 매체가 같은 주파수로 공진하는

[Table 1] Comparison of the Wireless Chargers

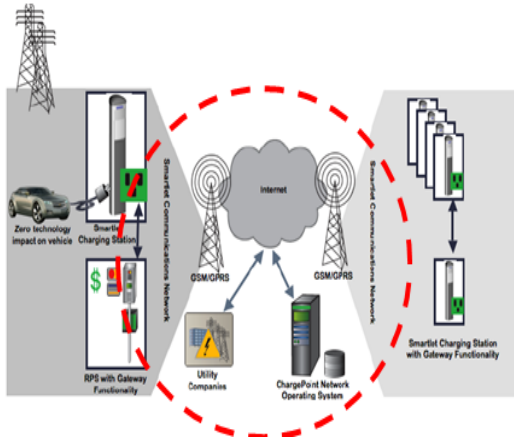
구분	자기유도 방식	자기공진 방식	전자기파
원리	변압기 1~2차 코일간 유도현상 이용	송수신 안테나 간의 공명현상 이용	안테나를 통해 전자파를 직접 송수신
주파수	125kHz, 13.56MHz	수십kHz ~ 수MHz	2.45GHz, 5.8GHz
전송 거리 및 효율	수mm이내-90%이상 효율	1m~90%효율 2m~40%효율	최대 수십km까지 전송 최대 10~50% 효율
인체 유해성	거의 무해	거의 무해	유해
특성	대전력 전송에 유리	대전력 전송 어려움 안테나가 큼	인체 및 장애물 영향
응용	휴대폰, 노트북, 전기자동차 등	가전기기 전원	위성-지구 전력 전송 비행체 전력 등
표준화	WPC 표준 제정	WPC표준이 자기 공진 기술에 대한 표준 부적합	N/A

경우 근거리 자기장을 통해 한 매체에서 다른 매체로 이동하는 감쇄파 결합 현상을 이용하고, 주파수가 줄어드는 파동에 의하여 에너지가 전달되는 형상을 이용하는 충전기술이다. 주파수/파장에 비해 짧은 거리에서의 전달로 근접한 곳에서 효율성이 높다. 자기 공진 방식은 수십 cm에서 수 m 의 근거리 무선 전력 전송이 가능하다. 특히, 송수신 코일은 방향성의 자유도가 매우 높고 같은 주파수를 갖는 물질에만 전력을 전송하는 특징이am로 무선 충전기의 위치에 상관없이 무선 충전을 할 수 있다는 장점이 있다. 적용하는 분야는 전기 자동차에서의 주차시 무선 충전 하는 모델에 효율적인 적용이 가능하다[1,3].

전자기파 방식은 원거리에서 수 GHz의 고주파수를 이용해 고출력 에너지를 전송하는 기술이다. 많은 기술적 제약과 인체의 영향 때문에 실용화까지는 많은 연구가 필요하다. 전자기파 방식은 특정 목표 지점으로의 방향성을 가지고 수 km 이상의 장거리에서 사용되는 기술이다. 전자기파 전송을 하기 위해서는 매우 큰 송수신 안테나가 필요하다. 무선으로 충전되는 전력이 대기 중에 흡수되거나 수분에 의한 방해가 있어 비효율적이다[1,3].

2.2 전기자동차 기술

지능형 자동차의 분야는 다양한 첨단 기술을 접목 시켜 안전한 주행과 편리한 서비스를 제공하기 위한 많은 연구가 진행이 되고 있는 분야이다. 특히, 그린 환경 정책의 일환으로 전기를 이용한 전기자동차에 대한 연구 또한 활발하게 진행이 되고 있다. 전기 자동차의 경우 그린 정책을 반영하기 위하여 전기의 에너지를 이용하는 기술로서, 주정차시 전기를 공급할 수 있는 기술의 개발이 진행이 되고 있다. 특히, 주차 시 주차장에서 자동으로 충전을 하기 위한 무선 충전 기술의 적용을 위한 모델이 사업화 모델로 제시되어 다양한 무선 충전 기술에 대한 많은 연구가 진행중이다. 이러한 전기 자동차의 특징은 우선 주행 중에 배기가스가 전혀 나오지 않는다. 그리고 소음이 아주 작다는 장점이 있다. 또한 에너지원이 다양하다. 단점으로는 1회 충전 후 주행거리가 짧다는 것이다. 그 이유는 배터리의 중량이 무겁기 때문이다. 또한 비용에도 문제가 있다. 판매가격은 동격 내연기관 자동차의 3배 이상이다. 게다가 전지의 수명이 짧고 그것의 교환 비용까지 생각한다면 비용적인 부담이 크다. 충전에 걸리는 시간 또한 너무 길어 문제이다. 때문에 실용화되지 못하다가 고유가 문제와 공해문제가 대두되면서 차세대 자동차로 부상하고 있다. 그림 1에서처럼 전기 자동차의 충전 방식은 단자 접촉에 의해 전류를 직접 유입하는 컨덕티브 방식과 전자 유도에 의해 전기 에너지를 전달하는 인덕티브 방식으로 나뉜다. 또한 충전 시간에 따라 보통충전, 급속충전, 중속충전으로도 분류된다. 무선 충전 인프라는 미국 캘리포니아의 Coulomb Technology에서 Charge Point라는 무인 충전소를 설치하고, 충전 인프라 이용자를 대상으로 정보를 제공하고 있다. 제공 서비스로는 웹 기반 시스템을 통해 인터넷이나 휴대전화로 충전 설비 지리 정보, 이용 가능 상황 등을 실시간으로 검색할 수 있다는 것이다.[1,2,3]



[Fig. 1] Infrastructure of the Wireless Charger

3. 무선충전 보안위협

무선충전의 보안 위협요소는 근접 무선 충전, 주차시 무선충전, 차량 이동간 무선충전의 서비스모델에서의 보안 위협요소를 분석하였다.

3.1 근접 무선충전

그림 2처럼 스마트폰이나 디지털 카메라, 전동칫솔 등 근접한 기기에 대한 무선 충전 시 발생할 보안 위험 요소로는 기기 사용자에 대한 위조나 변조의 위험이 존재한다. 충전환경이 가정의 경우는 가정 내 사용에 대한 기기에 대한 정당한 인증이 이뤄지지만, 외부 장소에서 충전 시 발생하는 충전 기기에 대한 인증에 대한 위조가 가능하며, 그에 따른 충전 비용에 대한 악용도 예상된다. 무선

충전 시 무선을 이용한 악성코드의 삽입을 통한 디바이스의 공격이 가능하다. 특히, 무선 충전 시 기기간의 도청, 가로채기, 부인과 관련된 프라이버시 및 변조 위협요소가 법 도용 및 접근을 통한 권한 위배, 물리적 침입, 재사용 공격, 중간자 공격의 위협이 가능하다.

[Fig. 2] Wireless Charger in Devices

3.2 전기자동차에서 주차 시 무선충전

그림 3처럼 전기자동차의 경우 주차 시 무선으로 충전할 수 있는 방법으로 인프라가 구축되어지고 있다. 주차 시 전기 자동차에 대한 무선 충전 시 발생할 위협 요소는 차량에 대한 사용자 인증에 대한 위조나 변조가 가능하다. 사용자 인증이 잘못될 경우 그에 따른 충전 비용이 잘못 부과 될 수 있는 위협이 존재한다. 충전시에도 공공장소에서의 위협을 통해서 무선을 통한 악성코드의 삽입으로 다양한 보안 위협이 예상된다. 전기자동차의 충전 시 차량에 대한 정확한 인증이 안 될 경우 충전에 대한 남용의 공격이 가능하다. 무선에서 발생할 수 있는 다양한 DoS 공격의 유형이 발생 할 수 있다. 특히, 무선 충전 시 불법침투, 서비스 거부를 통한 차량 운행 마비, 바이러스, 웜, 트로이목마, 자원고갈 등의 보안 위협 요소들이 발생 가능하다.

[Fig. 3] Wireless Charger in Parking

3.3 주행 중인 차량들 사이의 무선 충전

그림 4에서는 차량 주행 시 차량간 무선 충전을 위한 방법으로 차량간 충전 시 차량에 대한 상호 인증의 부재를 통한 사용자 위조와 변조가 가능하다. 주행중 차량간 무선 충전 시 무선을 사용한 악성코드의 삽입으로 차량의 큰 사고를 유발 할 수 있다. 또한 무선충전 시 M2M의 지능형 자동차에서 발생 가능했던 다양한 공격 유형이 동일하게 발생할 수 있다. 특히, 거짓 정보를 발생시키는 공격 차량에 의해 일정 네트워크 영역안에 있는 다른 차량들에게 거짓 정보를 보내는 Forgery 위협과 일정 네트워크 영역안에서 다른 차량의 통신에 장애를 가하는 신호를 발생시키는 Jamming공격이 가능하다. 무선 충전 시 차량의 상태 정보를 변경하여 다른 차량으로 하여금 오인하도록 하는 공격하는 Impersonation 공격이 가능하다. 시간, 위치, 차량 ID, 이동 정보 등의 차량과 관련된 개인 프라이버시 정보에 대한 침해하는 Privacy Violation과 차량 내부의 정보인 속도, 위치, 차량 전장 부분의 상태, 각종 센싱 정보 등에 대한 위변조의 공격이 가능한 위협요소이다.

[Fig. 4] Wireless Charger in Vehicle to Vehicle

4. 무선 충전시 공격 대응방법

무선충전 시 보안에서의 가장 큰 위험요소로는 사용기기에 대한 인증과 그에 따른 전기 사용량에 대한 비용에 대한 지불의 문제가 가장 중요한 보안 위협요소이다. 이동간 기기간의 상호 충전 시 발생할 수 있는 위험요소들은 기기에 악성코드 삽입을 통한 기기의 오작동이나 전기 사용의 오남용의 위험이 존재 한다. 이러한 위험에 대응하기 위해서는 무선충전 환경에 적합한 사용자 인증

기법과 지불에 대한 대응 방법이 필요하다.

사용자 인증에 대한 부분은 각 기기에 대한 사용자의 고유 식별을 위한 생체인식(지문, 홍채 등)을 통한 사용자 인증을 통해 정확한 사용자에 대한 식별 방법을 통해서 위험을 방어할 수 있다.

충전 기기간에 클러스터 단위로 구성을 통한 Threshold를 이용한 서명기반의 인증을 통해서 클러스터 서비스시 공개키/개인키 쌍으로 구성하여, 임계치 키 구성 기법을 이용하면 클러스터 내의 기기에 대한 부분 인증이 실패해도 개인키를 이용하여 사용자 인증이 이뤄져 안전성을 보장할 수 있다.

전기 자동차 충전 시에 사용자 인증을 위해서 차량 정보 연결을 요청할 때 사용자는 인증서버로 부터 본인 인증을 받아 차량 정보를 기반으로 안전하게 통신이 되어야 한다. 차량 충전 인증이 진행시 단순 차량 정보와 패스워드 입력을 통한 인증보다는 좀 더 복잡한 인증 과정을 통하는 것이 상호인증에 안전하다. 사용자는 자신의 차량 정보와 생체인식(지문, 홍채 등)을 이용하여 사용자의 차량정보, MAC 주소를 이용하여 만든 비밀 키를 인증 서버에게 보낸다. 인증 서버는 사용자의 생체키를 기반으로 사용자의 마스터 키를 찾아서 사용자 정보를 포함하고 있는 Ticket Key와 세션키를 만든다. 인증서버는 자신의 마스터키를 이용하여 Ticket Key를 암호화 하고 Ticket Key와 세션키를 사용자에게 보낸다. 사용자는 암호화된 Ticket Key 세션키를 가지고 차량정보와 접속한다. 사용자는 TimeStamp를 통해서 암호화와 복호화를 진행하여 세션 키를 이용하여 안전성을 보장한다.

전기자동차간 주행 중 상호 인증하기 위해서는 전기자동차간의 클러스터 단위의 그룹을 통해 그룹 인증을 이용할 수 있다. 충전을 원하는 차량이 클러스터에 진입하려는 경우, 차량은 상호 간 안전한 통신을 통하여 상호인증을 받아야 한다. 상호인증을 위해서는 차량의 고유의 정보와 사용자의 생체키 등을 이용한 인증을 통해서 차량의 정당한 사용자임을 안전하게 확인해 주어야 한다.

4. 결론

무선 충전전송 기술은 산업 분야에 다양하게 적용할 수 있는 파급효과가 매우 큰 첨단기술이다. 하지만 주파수 할당, 인체영향 및 기술적인 한계점 등 해결해야할 부분이 많이 있다. 본 연구에서는 앞으로 전개될 무선 충전 시스템에서의 발생할 경우의 사업 모델을 기반으로 취약점을 분석하고 그에 따른 대응 방법을 제시하였다. 향후 연구로는 이러한 문제를 좀 더 구체화하여 세부적인 대응 기법에 대한 인증과 지불에 대한 연구가 필요하겠다.

REFERENCES

[1] Byung-Jun Jang, “WPC Wireless Charger Standard(Qi) for Mobile IT Devices”, Korean Institute of Electromagnetic Engineering and Science, Vol. 23, No. 26, pp. 32-37, 2012.

[2] http://www.wirelesspowerconsortium.com

[3] Bo-Yeon Choi, Keun-Ho Lee, "Intelligent vehicles technology and security threats of wireless charging', 2012 Korea Convergence Society Winter Conference, Vol. 2, No. 1, pp. 38-40. 2012.

[4] Byung-Jun Jang, S. Lee and H. Yoon, "HF-band wireless power transfer system: concept, issues, and design", Progress in Electromagnetics Research, Vol. 124, pp. 211-231, 2012.

저자소개

이 근 호(Keun-Ho Lee) **[종신회원]**

- 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야> : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호