무선충전에서 보안요구사항에 관한 연구

이근호
백석대학교 정보통신학부

A Study of Security Requirement in Wireless Charging

Keun-Ho Lee
Division of Information & Communication, Baekseok University

요 약 최근에 스마트폰과 디바이스의 무선충전에 대한 관심이 높아지고 있으며, 많은 기업들이 무선충전을 개발하고 있다. 무선충전은 앞으로 모바일기기뿐만 아니라 노트북·청소기 등 거의 모든 전자제품으로 적용 범위가 확대될 것이다. 무선충전 전기자동차도 올해 본격적으로 선을 보일 예정이다. 이렇듯 무선충전은 연관시장이 무궁무진하다. 세계 10대 유망기술에 포함되어 있는 무선충전은 매년 100% 이상 급성장할 전망이라고 한다. 하지만 그에 따라 존재하는 기술적 한계점과 인체 유해성에 대한 보안위협을 분석해 안전한 환경에서 사용할 수 있도록 해야 하고 각종 제도적 보안도 마련해야 한다. 무선충전에 대한 표준화와 보안대책요구사항은 체계적이지 않다. 본 논문은 모바일기기에서 자기공진방식의 무선충전의 보안 위협과 보안요구사항을 정의해 분석하고자 한다.

• **주제어** : 무선충전, 전기자동차, 인증, 클러스터, 보안

Abstract In recent times, there is an increasing interest in wireless charge of smartphones and devices, and many companies are developing wireless charges. The range of application of wireless charge would be expanded to almost all electronics, including not only mobile devices, but also notebook computers and vacuum cleaners. On-line electric vehicles are to be launched in the market this year in a massive scale. As such wireless charge-related markets are inexhaustible. Wireless charge is included in the world's top 10 promising technologies, and its rapid growth is expected to have annual growth by more than 100%. However, there's a need to establish a safe environment, by analyzing security threats to technical limitations and harmfulness to human body, and arrange institutional compliments. The development of communication method for a variety of wireless charging are delivering comfortable and safe information. This paper aims to examine the factors to threaten electric vehicle, which are usually intruded through network system and analyzes security threats to and security requirements for magnetic resonance mode-based wireless charge in mobile devices, and suggests security requirements.

• **Key Words** : Wireless Charging, Electric Vehicle, Authentication, Cluster, Security

1. 서론

다양한 이동 디바이스와 스마트폰을 이용한 게임 및 각종 어플리케이션의 구동으로 전력소비가 증가해 충전의 수요가 급증함에 따라 소비자들은 기존 유선 케이블 제거로 편리성을 제공받을 수 있는 무선충전에 대해 높은 관심을 가지고 있다. 현재 무선충전은 자기유도와 자기공진의 두 가지 방식이 주류를 이루고 있다. 자기유도

*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 : 2014년 7월 12일, 수정일 2014년 9월 21일, 게재확정일 : 2014년 9월 26일

방식은 전력 송신부 코일에서 자기장을 발생시키면 그 자기장의 영향으로 수신부 코일에서 전기가 유도되는 전기 유도 원리를 이용한다. 자기공진 방식은 송신부 코일에서 공진 주파수로 진동하는 자기장을 생성, 동일한 공진 주파수로 설계된 수신부 코일에만 에너지가 집중적으로 전달되도록 한 기술이다[1].

최근까지 출시하고 있는 무선충전은 WPC의 Qi 표준을 이용한 자기유도 방식의 무선충전이다. 하지만 단말기를 충전기에 직접 접촉시켜야만 높은 충전 효율을 얻을 수 있기 때문에 근거리에서만 충전이 가능하다는 한계점을 가지고 있다. 그러므로 요즘은 단말기를 충전기에 접촉시키지 않아도 충전이 되는 A4WP의 자기공진방식의 기술을 개발하는데 초점을 맞추고 있다[2,7,9].

본 논문에서는 향후 전개될 다양한 무선충전의 사용이 높아질 예정인 모바일기기에서의 자기공진방식의 무선충전의 보안 위협을 알아보고 보안요구사항에 대해 분석하여, 다양한 모바일 환경에서의 안전성을 위한 무선충전의 대응방법을 제안한다.

2. 관련 연구

2.1 자기유도방식과 자기공진방식

무선충전기술은 전송거리를 기준으로 분류해 자기유도방식, 근거리전송방식, 자기공명방식, 전자파방식으로 나눌 수 있다. 현재 무선충전에서 사용하는 기술은 자기유도방식과 자기공진 방식이다. 최근 무선충전에는 높은 충전 효율을 얻기 위해 단말기를 충전기에 접촉시켜야 했다면, 요즘은 단말기를 충전기에 직접 접촉하지 않아도 충전이 되는 자기공진방식을 이용한 무선충전이 개발되고 있다.

- 자기유도방식의무선충전

수 mm내외로 인접한 두 개의 코일에 유도전류를 일으켜 배터리를 충전하는 방식인 자기 유도방식은 충전 위치에 따라 효율이 크게 달라지기도 한다. 전력 전송효율이 90%이상으로 매우 높지만 전송거리가 짧다는 것이 단점이다. 2008년 12월 자기유도방식의 무선충전기술 표준화단체인 WPC(Wireless Power Consortium)가 결성되었고, 2010년에 Qi 1.0 표준을 발표로 가장 활발하게 상용화가 추진되고 있는 기술이다[1,3].

- 자기공진방식의 무선충전

자기공진방식은 두 매체가 같은 주파수로 공진할 경우 전자파가 근거리 자기장을 통해 한 매체에서 다른 매체로 이동하는 감쇄파 결합 현상을 이용하는 기술이다. 거리 측면에서 가장 편리성을 제공하는 자기공명 방식은 최근 휴대폰에 채택이 점차 늘어나고 있다. 현재 스마트폰 제조사 및 여러 충전기 업체에서 가장 신경을 많이 쓰고 있는 기술이며, 이 기술의 장점은 최대 7대의 단말기까지 동시에 충전이 가능하며, 충전기에 단말기를 올려두지 않고 근처에만 있어도 충전이 이루어져 상용화가 되면 시장 파급력이 가장 클 것으로 예상한다. 하지만 원거리까지 자기장을 발생시켜 충전하는 방식으로 인체 및 주변 가전제품의 유해성 부분은 아직 주요한 문제로 남아있다[1].

2.2 WPC와 A4WP

- WPC (Wireless Power Consortium)

무선충전 표준인증 기관으로 국제 표준으로 정한 Qi 표준을 가지고 최근 가장 활발하게 상용화되어있다. WPC의 전 세계의 회원 수는 200개를 초과하고, 퀄컴, 삼성전자, LG, HTC, 소니 등 큰 기업들이 포함되어 있다. 최근 마이크로소프트에서 정식으로 가입하게 되어 마이크로소프트의 WPC에 대한 지지는 큰 힘으로 작용될 것으로 보인다[4].

- A4WP (Alliance for Wireless Power)

A4WP는 자기공진방식의 무선충전 연합이다. 삼성전자, 퀄컴, 인텔, 브로드컴 등이 주도해 6.78MHz 공진방식 무선전력전송 기술을 선도하고 표준화를 추진하는 단체로 2012년 설립되었다. 2013년에는 한국정보통신기술협회가 세계 최초로 A4WP로부터 국제공인시험기관으로 지정되었고, 새 무선충전 시스템 표준인 리젠스(Rezence)를 발표했다. 충전패드와 3cm 떨어져도, 2대 동시에 충전이 가능한 인증 제품을 2014 CES에서 시연했다. 2014년 1월에는 삼성전자가 A4WP로부터 세계 최초로 국제인증을 받은 자기공진 방식의 무선충전기를 선보이기도 했다. 삼성전자는 두 협회에 모두 참여해 업계에서는 삼성전자가 무선충전 협회에서 주요 위치를 차지함에 따라, 후에 시장이 형성될 경우 사업화가 빠르게 이루어질 것으로 예상하고 있다[5].

2.3 무선충전 시스템

무선충전 시스템의 구성요소에는 사용자 장치, 무선충전 관리센터, 무선충전 장치로 이루어져있다. 모바일 기기에 부착된 사용자 장치가 무선충전 관리센터로 무선충전을 요청하면 무선충전 관리센터는 무선충전 장치에게 충전지시를 내려 무선충전장치가 다시 사용자 장치에 전력을 전송하는 구조이다. 이러한 구조에서는 사용자에 대한 인증의 모델과 사용량에 따른 지불에 대한 안전성을 확보하는 것이 필요하다. 각 무선충전 시스템에서 각 장치별 역할에 대한 연구가 진행이 되고 있으며, 본 연구에서는 각 장치별 역할에 대한 세부적인 모델에 대한 내용을 고려하지 않고, 발생 가능한 보안 위협 요소를 분석하고 그에 따른 보안 요구사항을 제안하여, 향후 전개될 무선충전에서의 안전성을 확보할 수 있는 대응방법을 제안하고자 한다.

3. 무선충전 보안 위협

자기공진방식 무선충전을 이용하면 단말기를 직접 충전기에 접촉시키지 않아도 충전을 할 수 있기 때문에 효율적이고, 보다 편하게 충전을 할 수 있지만 여러 가지 보안 위협이 존재한다. 자기공진방식의 무선충전에서 예상되는 보안 위협에 대해서 분석한다. <Table 1>는 보안 위협이 발생하는 구간에 대한 내용이다.

[Table 1] Security Threats

보안 위협	발생 구간
프라이버시 침해	사용자 장치
과다하게 부가된 비용	
인체 유해성 악용	무선충전 관리센터
시스템 위협	

자기공진방식의 무선충전은 무선충전기 근처에만 있어도 충전이 이루어지는 방식으로 공공장소나 차량 내에서 움직임이 있어도 충전이 될 것이다. 이 경우 이동 환경에서 단말 사용자에 관한 위치나 움직임 등의 비정형 데이터가 발생하면서 무선충전 관리센터로 전송될 것이다. 무선충전 관리센터나 기지국 등이 해킹이 된다면 이를 악용해 사용자의 위치정보를 추적하는 불법 행위를 할 수 있을 것이다.

3.1 위조된 인증으로 인한 과금

충전하고자하는 환경이 가정인 경우에는 정당한 인증이 이루어질 수 있지만, 외부 장소와 같은 노출된 공간인 경우에는 충전에 대한 인증이 위조될 수 도 있다. 허가받지 않은 사용자가 인가되지 않은 권한을 획득하게 되어 정당한 사용자의 계정을 위조하거나 도용할 경우, 도용한 계정을 통해 사용한 서비스 이용료가 과다하게 부가되어, 정당한 사용자가 사용하지 않은 무선충전 과금 내역까지 지불하게 될 수도 있다.

3.2 인체 유해성을 악용

전자파는 전기 및 자기의 흐름에서 발생하는 일종의 전자기 에너지로 원래 명칭은 전기자기파로서 이것을 줄여서 전자파라고 부른다. 자기공진방식은 무선충전기와 단말기에 내장된 코일간의 공진을 통해 발생한 전자파를 가지고 전력을 송출하는 방식으로 충전효율을 높일수록 전자파 발생량이 많아져 특정 주파수에서 공진현상이 증폭되는 경우도 있다. 이는 인체에 전자레인지와 비슷한 영향을 미칠 수 있다. 이를 악용해 무선충전의 강도를 해커가 임의로 조절해 많은 전자파를 보내 인체에 해가 되도록 악용될 수 있다.

3.3 무선충전 관리센터 시스템 위협

무선충전 시스템에서 무선충전 관리센터는 무선충전을 제어하는 역할을 하므로 악의적인 용도로 사용될 위험이 높다. 공격자가 사용자가 원하는 서비스를 방해할 목적으로 서비스가 제공되는 무선충전 관리센터의 CPU를 장악해 DDoS의 위험이 있거나 무선충전서비스를 요청하는 정보가 전송되지 않도록 요청하는 데이터를 가로챌 수도 있다.

4. 무선충전의 보안요구사항

모바일 기기에서의 자기공진방식 무선충전 환경에서는 다양한 보안 위협이 존재하고 있다. 하지만 이러한 보안 위협은 막을 수 없는 위협이 아니고, 사용자와 관리자가 관리하고 통제한다면, 위와 같은 위협들로부터 안전

한 무선충전 환경을 사용할 수 있다. 자기공진방식의 무선충전을 안전하게 사용하기 위해 필요한 보안요구사항에 대해서 분석한다. 기밀성(Confidentiality)이란 정당한 사용자에게만 접근을 허용함으로써 정보의 안전을 보장하는 것이고, 무결성(Integrity)은 정보의 내용이 변경되거나 파괴되지 않도록 보장하는 것, 가용성(Availability)은 정당한 사용자에게 언제든지 정보와 서비스를 제공하는 것을 보장하는 것이다.

<Table 2>은 보안 위협에 따른 보안요구사항을 정리한 것이다.

[Table 2] Requirement of Security Threats

보안위협	보안요구사항			
	기밀성	무결성	가용성	인증/허가
인체 유해성 악용	O	O		
프라이버시 침해	O			
과다하게 부가된 비용				O
시스템 위협	O	O	O	

4.1 기밀성 및 데이터 암호화

무선충전 시스템에서 사용자 장치에서 무선충전 관리센터로 무선충전을 요청할 때 전송되는 정보가 정당한 사용자에게만 접근을 허용하도록 전송되는 정보(데이터)를 암호화해야 한다.

4.2 데이터 무결성

무선충전 시 전자파가 발생하는 것을 악용해 지정되어 있는 주파수보다 과다한 전자파를 보낸다는 내용에 대한 정보의 무결성을 보장해야 한다. 전자파에 대한 등급기준을 적용하고 무선충전의 전력 전송을 하는 부분에도 기준 등의 가이드라인을 세워 해커가 악용해 임의로 전력을 전송해 과다한 전자파를 보낼 수 없도록 해야 한다.

4.3 데이터 가용성 및 정보 백업 시스템

무선충전 시스템에서 정당한 사용자가 무선충전 요청을 요구할 때, 언제든지 서비스를 제공하도록 해야 한다. 사고가 생겨 의심 위협요소와 공격으로부터 보호하기 위해서는 무선충전 시스템의 서비스 지속성을 확보하고, 사고에 대비한 백업 시스템을 가동하고 복구해야한다.

4.4 인증과 허가

무선충전 관리센터에 요금을 지불하고 무선충전을 사용할 경우 합법한 사용자인지 확인하고 어떤 서비스를 받을 수 있는 사용자인지 확인할 수 있는 인증과 지불 메커니즘이 필요하다.

5. 무선충전시 공격 대응방법

무선충전시 보안에서의 가장 큰 위험요소로는 사용기기에 대한 정당한 사용자와 기기에 대한 인증과 그에 따른 사용량에 따른 과금에 대한 처리 부분에 대한 정당한 절차를 무시한 보안의 위협이 상당히 존재하고 있다. 이동간 기기간의 상호 충전시 발생할 수 있는 위험요소들은 기기에 악성코드 삽입을 통한 기기의 오작동이나 전기 사용의 오남용의 위험이 존재 한다.

사용자 인증에 대한 부분은 각 기기에 대한 사용자의 고유 식별을 위한 생체정보를 이용한 사용자 인증과 디바이스 고유의 식별을 통한 기기 인증을 위한 대응을 위한 인증서버와 고유의 킷값을 갖는 프로토콜과 기법의 제안을 통해서 안전성을 확보할 수 있다.

충전기기간에 기기에 대한 클러스트 단위로 구성을 통한 공동의 킷값을 통한 관리와 키관리 기법을 이용한 서명기반의 인증으로 클러스터 단위의 인증을 통해 처리의 효율성을 확보할 수 있다.

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 상호 인증을 받아야 한다. 상호인증을 위해서는 차량의 고유의 정보와 사용자의 생체정보 등을 이용한 인증을 통해서 차량의 정당한 사용자임을 안전하게 확인해 주어야 한다.

6. 결론

무선충전은 앞으로 모바일기기뿐만 아니라 노트북·청

소기 등 거의 모든 전자제품으로 적용 범위가 확대될 것이다. 무선충전 전기자동차도 올해 본격적으로 선을 보일 예정이다. 이렇듯 무선충전은 연관시장이 무궁무진하다. 세계 10대 유망기술에 포함되어 있는 무선충전은 매년 100% 이상 급성장할 전망이라고 한다. 하지만 그에 따라 존재하는 기술적 한계점과 인체 유해성에 대한 보안위협을 분석해 안전한 환경에서 사용할 수 있도록 해야 하고 각종 제도적 보안도 마련해야 한다. 본 논문에서는 무선충전에서 발생할 위협요소를 분석해보았으며, 필요한 보안 요구사항을 정의 하였다.

참고문헌

[1] Hyun-Joo Jung, Keun-Ho Lee “Wireless Charging Technology Trend and Security threats” 2013 Korea Convergence Society Conference, Nov. 2013.

[2] J. Kim.H. -C. Son. K. -H. Kim, and Y. -J. Park, “Efficiency analysis of magnetic resonance wireless power transfer with intermediate resonant coil”, IEEE Antennas and Wireless Propagation Letters. Vol. 10. pp. 389-392, 2011.

[3] “Wireless charging industry-blooming“, Eugene Investment & Securities.

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

[5] http://www.a4wp.org/

[6] Kim Baro, (A)study on enhanced wireless connectivity authentication and a security threat prevention in a wireless LAN environment, 2012

[7] Ken-Ho Lee, “A Security Threats in Wireless Charger System in M2M”, 2013 Korea Convergence Society Conference, Vol. 4, No. 1, pp. 27-31, 2013

[8] 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.

[9] 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.

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