스마트그리드 환경에서 전기자동차 충전 중 발생 가능한 보안 위협 대응 기법

황치광 홍충선*
경희대학교 컴퓨터공학과
{chikwang16, cshong*}@khu.ac.kr

Countermeasure against Threat to Steal Energy during Electric Vehicle Charging in Smart Grid Environment

요 약

전기자동차는 환경 문제를 해결하기 위해 반드시 대중화되어야할 기술이며, 스마트그리드는 전력난을 극복하기 위해 현재의 전력망에 필수적으로 적용되어야할 기술이다. 전기자동차가 스마트그리드의 중요한 요소로 자리 잡고 있어 전기자동차에 관련된 보안 위협 또한 스마트그리드와 함께 다루어져야하지만, 스마트그리드 연구에 비해 전기자동차 관련 보안 연구는 매우 제한적으로 이루어지고 있다.

본 논문에서는 스마트그리드 환경에서 전기자동차 충전 시에 발생할 수 있는 전기를 절도하기 위한 목적의 위협들을 분석하고, 이원화된 측정 장치를 이용해 전기자동차 충전 시 발생할 수 있는 전기절도에 대응하는 기법을 제안한다.

1. 서 론

지난 6월 말부터 8월까지 제주도는 국내 최초로 민간을 대상으로 한 전기자동차 보급사업을 진행하였다. 160대로 한정된 지원 사업이었지만 환경부에서 1,500만 원, 제주도에서 800만 원 등 기본적으로 2,300만 원이라는 상당한 금액의 보조금을 지급하기로 하여 많은 관심을 받았다. 우리나라뿐만 아니라 세계 각국에서도 민간에 대한 전기자동차 보급 정책이 진행되고 있다. 미국은 7,500달러의 보조금과 더불어 보험료 감면, 세금 공제 등의 혜택을 지원하고 있으며, 일본은 139만 엔의 보조금과 세금 감면 혜택을, 중국 또한 6만 위안의 보조금과 세금 감면 혜택을 지원하고 있다[1].

이처럼 세계 각국이 전기자동차의 보급을 장려하는 직접적인 이유는 전기자동차가 온실가스의 배출량을 줄이는 효과적인 방법 중의 하나이기 때문이다. 2005년 발효된 교토의정서(Kyoto protocol)에 따라 나라별로 지정된 감축 비율만큼 의무적으로 온실가스 배출량을 줄여야 한다. 그 결과로 전기자동차 보급과 같은 온실가스 저감 정책의 시행은 각국의 피할 수 없는 숙제가 되었다.

그러나 계획 없이 전기자동차를 보급하는 것은 위험한 결과를 초래할 수 있다. 전력사용량 증가로 인해 우리나라는 여름과 겨울, 전력예비율 부족으로 전력 사용을 적극적으로 제한하고 있다. 이런 상황에서 전력 피크 시간대에 전기자동차의 충전으로 많은 전력이 소모된다면 대규모 정전사태(black out)가 발생할 수 있다.

이러한 위험을 예방하기 위해 우리나라를 포함한 전 세계 여러 나라들은 스마트그리드(Smart Grid)의 도입을 추진 중이다. 전력 계통에 정보 기술과 통신 기술을 융합하여 지능화 및 고도화된 전력망인 스마트그리드는 에너지 효율성이 기존의 전력망 보다 좋을 뿐만 아니라, 분산 전원의 활성화를 통해 신재생에너지 활용성을 높여 전력 부족 문제를 효과적으로 해결할 수 있는 대안으로 떠오르고 있다[2]. 따라서 전기자동차의 대중화가 스마트그리드의 도입과 동시에 이루어지면 전기자동차로 인한 전력 부족 문제는 쉽게 발생하지 않을 것이다.

하지만 정보통신 기술을 활용하는 스마트그리드의 특성 때문에 각각의 요소를 연결하는 네트워크 구축이나 관련 서비스 개발, 그리고 전체 시스템을 운영하는 데에 다양한 보안위협이 발생할 수 있다. 이러한 이유로 이와 관련된 다양한 보안 연구들이 선행되었으며 현재도 많은 연구들이 진행 중이다.

한편, 전기자동차가 스마트그리드의 중요한 요소로 자리 잡고 있어 전기자동차에 관련된 보안 위협 또한 스마트그리드와 함께 다루어져야하지만, 이러한 연구는 매우 제한적으로 이루어지고 있다. 따라서 본 논문에서는 전기자동차가 스마트그리드에 직접적인 영향을 주고받는 충전인프라(charging infrastructure)에서의 보안 위협을 분석하고 이를 해결하기 위한 방법을 제시한다.

본 논문의 구성은 2장에서 전기자동차 충전 중에 발생할 수 있는 보안 위협을 분석하고, 3장에서 이를 해결하기 위한 방법을 제안한다. 4장에서 제안 사항에 대한 자체 평가를 한 후, 5장에서 결론을 맺는다.

2. 잠재적 위협

전기자동차 충전 인프라의 보안 위협에 대한 몇몇 연구가 진행되어 도청(eavesdropping), 부인(repudiation), 중

본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 IT연구센터 육성지원 사업의 연구결과로 수행되었음. (NIPA-2013-(H0301-13-4006)) *Dr. CS Hong is corresponding author.

간자 공격(man-in-the-middle attack), 탬퍼링(tampering) 등의 잠재적인 위협이 충분히 발생할 수 있다는 사실이 알려졌다. 본 연구에서는 중간자 공격 등을 이용해 소비자에게 금전적인 손해를 입히는 위협에 대해 자세히 살펴보려 한다. 그림 1과 같이 악의적으로 조작된 충전기를 이용하여 전기절도가 가능하다. 공격의 대상이 된 소비자는 공격자가 설치한 조작된 충전기를 통해 전기를 충전한다. 조작된 충전기는 정상 충전기와 연결된 전력선을 통해 전기의 일부를 가로채 공격자에게 공급한다. 그러나 조작된 충전기는 정상적인 충전기와 연결되어 있어 소비자의 전기자동차와 정상 충전기 사이의 통신을 훼손 없이 제공한다. 소비자와 정상 충전기 사이의 통신은 정상적으로 이루어지므로 소비자는 자신이 충전한 전기와 공격자가 공급 받은 전기 모두에 대해 결제하게 된다[3].

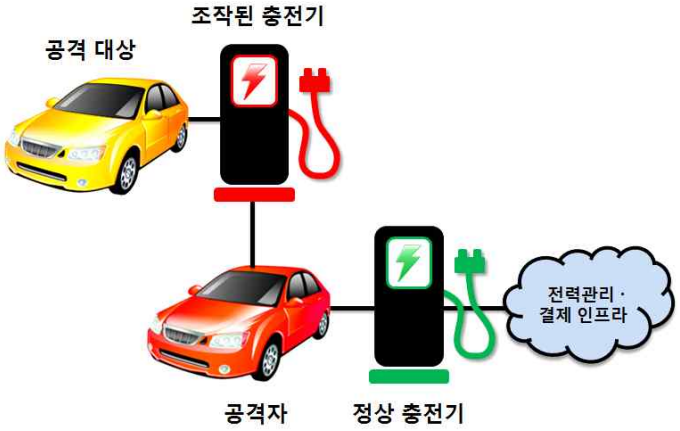

그림 1. 전기절도 목적의 중간자공격

그림 2는 조작된 충전기를 이용한 또 다른 공격 방법을 보여준다. 충전기는 전기자동차를 충전함과 동시에 미리 연결해둔 배터리도 함께 충전한다. 멀티 탭을 이용해 동시에 여러 전기제품을 사용하는 것과 같은 구조이다. 그림1의 방법과 마찬가지로 이 방법 또한 소비자와 충전기 사이의 통신을 훼손 없이 제공한다. 결과적으로 소비자는 자신이 충전한 전기와 공격자의 배터리에 공급한 전기 모두에 대해 결제하게 된다.

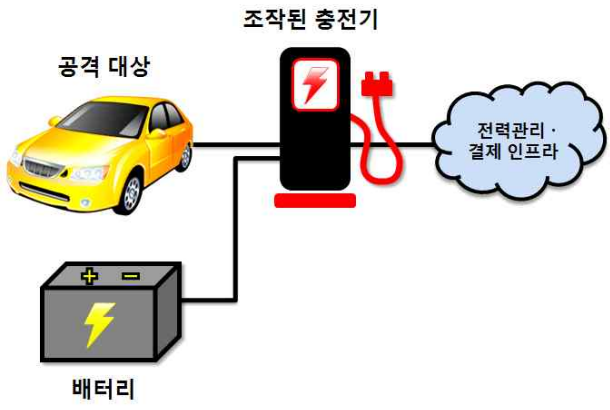

그림 2. 조작된 충전기를 이용한 전기절도

앞서 분석한 전기절도 목적의 위협들은 충전기와 충전기를 연결하는 전력선을 조작해야하므로 발생할 가능성이 낮다고 여겨질 수 있다. 그러나 가짜 휘발유 사건이나, 주유기 조작 사건 등이 실제로 일어난 것으로 미루어 볼 때, 다가오는 전기자동차 시대에 충분이 발생할 수 있는 위협이다.

3. 제안 사항

현재 스마트그리드 환경 조성의 초기 단계이기 때문에 아직 전기자동차 충전 시스템의 구조가 하나로 확립되지 않았다. 하지만 논의되고 있는 전기자동차 충전 표준에 기반을 두어 기존의 충전 시스템들은 대부분 같은 충전 절차를 따른다. 충전 절차는 간단히, 연결 - 인증 - 충전 - 결제 단계로 진행된다고 볼 수 있는데 기존 충전 시스템들은 인증된 요소를 완전히 신뢰한다는 문제가 있다. 이런 이유로 충전기가 측정하여 전기자동차로 전달한 정보에 따라 그대로 결제가 이루어진다. 하지만 앞서 살펴본 전기절도 목적의 공격들은 측정된 사용전력량과 실제로 소비된 전력량이 다르다는 특징이 있다. 따라서 인증이 완료된 경우라도 추가적인 기능 및 절차를 통해 충전 단계에서 이를 탐지하고, 소비자의 금전적인 손해를 최소화해야한다. 이를 위한 알고리즘은 다음과 같다.

알고리즘1. 전기절도 탐지 (전기자동차)

```
//연결 단계, 인증 단계 진행 후
//충전 단계 진입
B = battery remains
n = 0
flag = true
ID_EVSE = null
WHILE flag is true //충전 루프
  n = n+1
  M_EV = 0
  reqCharging()
  startMetering()
  charging(T_n)
  endMetering()
  M_EV = metered electric energy
  M_C = reqMeter()
  B = battery remains
  IF M_EV not equals M_C THEN
    flag = false
    ID_EVSE = ID of electric vehicle supply equipment
  ENDIF
  IF B is 100 THEN //완전 충전의 경우
    flag = false
  ENDIF
END WHILE
//충전 단계 종료 후 결제 단계 진입
payment()
//결제 단계 종료
```

B: 배터리의 잔량 (%)
T_n: 충전 스케줄에 따른 충전시간 (s)
flag: 충전 루프 진입 여부 확인
M_{EV}: 전기자동차가 측정한 사용전력량
M_C: 충전기가 측정한 T_n 동안 사용한 전력량
ID_{EVSE}: 충전기의 ID
reqCharging(): 충전기에 충전 요청
reqMeter(): 충전기에 사용전력량 요청
startMetering(): 사용전력량 측정 시작
endMetering(): 사용전력량 측정 종료
charging(): 충전 진행
payment(): 결제 진행

알고리즘 1에서 눈여겨 봐야할 과정은 충전에 사용한 전력량을 전기자동차가 직접 측정하고 충전기로부터 전달받은 전력량과 비교하는 부분이다. 전기자동차는 이 두 값을 통해 실제로 사용한 전력량과 결제가 이루어질 사용전력량이 일치하는지 확인한다. 비교 시 두 값의 오차범위를 설정하여 이를 고려한다. 충전기가 측정한 사용전력량은 전기자동차 충전 통신을 위한 표준인 ISO/IEC 15118-2에 메시지로 정의되어 있으므로 전기자동차는 이상 없이 이 값을 전달 받을 수 있다[4]. 그러나 아직까지 관련 업계에 전기자동차에서도 사용전력량을 측정해야할 필요성이 인식되지 못하였기 때문에 충전기와 동시에 자체적으로 사용전력량을 측정하는 기능이 내장된 전기자동차는 출시되지 않았다. 따라서 본 논문은 전기자동차 내부에 미터기를 설치하거나, 충전량을 통해 사용전력량을 계산하는 등 충전 시에 전기자동차 자체에서 정확한 사용전력량을 측정하기 위한 조치가 필요함을 알린다. 이어서 알고리즘 1과 같이 이원화된 측정 장치를 이용하여 충전 단계에서 전기절도를 탐지하고, 탐지 시 추가 충전을 제한하여 소비자의 손해를 최소화하는 기법을 제안한다. 여기에서 결제를 차단하지 않는 이유는 전력 공급자가 의도하지 않은 행위로 인해 공격자로 오인되어 2차 피해자가 되는 사태를 방지하기 위함이다. 또한, 알고리즘 1을 통해 위협의 주체 혹은 위협과 연관된 충전기의 ID를 알 수 있다. 이것은 인증 단계에서 주고받는 메시지에서 얻는다. 그림 2의 방법일 경우 공격의 주체가 되는 충전기를 바로 알 수 있다. 그림 1의 방법일 경우에는 공격의 주체를 파악할 수는 없으나 공격에 참여한 충전기를 파악할 수 있다. 충전 시스템 관리자는 이 정보 이용해 추가 피해를 방지하는데 이용할 수 있다.

4. 평 가

표 1은 제안한 기법을 적용한 충전 방식과 그렇지 않은 기존 방식을 상대적으로 비교하여 정리한 결과이다.

표 1. 제안 사항과 기존 충전 방식의 상대적 비교

항목	제안한 기법	기존 충전 방식
보안성	높음	낮음
소비자 피해	낮음	높음
오버헤드	있음	없음

본 기법은 기존에 연구된 전기자동차 충전 시스템에서 위험성을 고려하지 않아 발생할 수 있는 전기절도를 탐지하고 소비자의 손해를 최소화할 수 있다는 점에서 향후 출시되는 전기자동차에 적용될 가능성이 있다. 그러나 전기자동차 내에 물리적인 사용전력량 측정 장치를 설치할 경우, 전기자동차 제작 시 추가비용이 발생하므로 적용 전 이로 인한 경제적인 측면을 고려해야한다. 또한, 충전량을 이용한 논리적인 방법으로 사용전력량을 측정할 경우 직접 측정하는 것에 비해 정확하지 않을 수 있으므로, 측정값에 대한 신뢰도를 증명하는 연구가 필요하다.

5. 결 론

전기자동차는 환경 문제를 해결하기 위해 반드시 대중화되어야할 기술이며, 스마트그리드는 전력난을 극복하기 위해 현재의 전력망에 필수적으로 적용되어야할 기술이다.

본 논문에서는 스마트그리드 환경에서 전기자동차 충전 시에 발생할 수 있는 전기절도 목적의 위협들을 분석하였고, 이원화된 측정 장치를 이용해 전기자동차 충전 시 발생할 수 있는 전기절도에 대응하는 기법을 제안하였다. 향후에는 V2G(Vehicle to Grid)라 불리는 전기자동차 역송전 기술을 고려하여 본 주제에 대해 발전된 연구를 진행하고자 한다.

참 고 문 헌

[1] 전황수, “주요국의 전기자동차 정책 및 시사점”, 전기통신동향분석, 제27권, 제3호, 186쪽, 2012년 6월
[2] Hassan Farhangi, “The Path of the Smart Grid”, IEEE Power and Energy Magazine, Volume8, Issue1, p18, February 2012
[3] Rainer Falk and Steffen Fries, “Electric Vehicle Charging Infrastructure - Security Considerations and Approaches”, The Fourth International Conference on Evolving Internet (INTERNET 2012), June 2012
[4] ISO/IEC 15118-2: Road vehicles — Vehicle-to-Grid Communication Interface — Part2: Technical protocol description and Open Systems Interconnections (OSI) layer requirements, Work in Progress