The Journal of the Convergence on Culture Technology (JCCT)
Vol. 6, No. 1, pp.441-448, February 29, 2020. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/2020.6.1.441
JCCT 2020-2-54

스마트 그리드환경에서 전기자동차 양방향 충전기술의 보안과 개인정보 보호에 관한 연구

Security and Privacy Protection of Vehicle-To-Grid Technology for Electric Vehicle in Smart Grid Environment

이성욱

Sunguk Lee*

요 약 Vehicle-to-Grid(V2G) 기술은 전기자동차의 배터리를 분산발전원 및 에너지 저장장치로의 이용하려는 기술로 스마트그리드의 주요한 한 부분을 차지하고 있다. V2G 네트워크는 양방향의 통신망을 사용함으로 피할 수 없는 보안 취약점과 개인정보보호의 문제를 가지고 있다. 본고에서는 V2G 시스템의 구조, 사용되는 개인정보, 보안취약점 및 보안 요구사항에 대해 자세히 알아보고 분석한다. 그리고 V2G 시스템의 특성을 고려하여 효율적인 V2G 시스템의 구조와 운용방안을 제안한다. 제안하는 방식은 대칭키 암호와 해쉬 알고리즘을 이용하여 개인정보의 유출을 방지하고 양방향 인증을 수행하며 개인정보 유출의 위험성을 최소화 한다.

주요어 : V2G,전기자동차, 스마트 그리드, 개인정보 보호 , 보안

Abstract With help of Vehicle-to-Grid(V2G) technology battery in electric vehicle can be used as distributed energy resource and energy storage in a smart grid environment. Several problems of security vulnerability and privacy preservation can be occurred because V2G network supports 2 way communication among all components. This paper explains and makes analysis of architecture , privacy sensitive data, security vulnerability and security requirement of V2G system. Furthermore efficient architecture and operating scheme for V2G system are proposed. This scheme uses symmetric cryptosystem and hash algorithm to support privacy preservation and mutual authentication.

Key words : V2G, Electric Vehicle, Smart Grid, Privacy preservation, Security

Ⅰ. 서 론

스마트 그리드[1,2]는 기존의 전력 인프라와 통신 인프라를 결합하여 수집된 전력 소비자 측의 정보를 바탕으로 효율적으로 전력망을 관리 감독하는 차세대 전력망이다. 스마트그리드는 양방향통신을 지원하며 이 통신망을 통하여 전력망의 모든 시스템을 모니터링 하고 이를 토대로 가장 효율인 방법으로 전력망을 운영을 한다. 또한 스마트 그리드는 양방향의 전력흐름을 지원하여 전력이 모자란 시간대에는 신재생에너지원을 이용한 전력이나 소비자 측의 전력을 전송받아 전력시스템의 효율을 극대화 한다.

*정회원, 한남대학교 멀티미디어공학과, 부교수
접수일: 2019년 12월 27일, 수정완료일: 2020년 01월 11일
게재확정일: 2020년 01월 21일

Received: December 27, 2019 / Revised: January 11, 2020
Accepted: January 21, 2020
*Corresponding Author: sulee0612@hnu.kr
Dept. of Multimedia Engineering, Hannam Univ, Korea

지구온난화의 주요 원인인 온실가스의 가장 큰 발생 원인은 화석연료를 사용하는 전력발전이지만 화석연료를 사용하는 수송 부분 또한 약 24%의 온실가스를 배출하는 것으로 알려져 있다[3]. 이러한 수송부분의 배기가스로 인한 오염을 줄이기 위해 배기가스 규제가 강화되고 있으며 전기모터를 사용하여 구동하는 전기자동차(Electric Vehicle)가 화석연료를 사용하는 내연기관 자동차의 대안으로 각광을 받으면서 환경적인 문제와 각국 정부의 정책적인 지원에 힘입어 그 수가 급격히 증가하고 있다. 미국의 캘리포니아를 포함한 8개주는 330만대의 전기자동차를 2025년까지 보급하는 것을 목표로 하고 있으며 우리나라는 2020년까지 20만대의 전기승용차 보급을 계획하고 있다[4]. 이러한 전 세계적인 흐름에 따라 IEA(International Energy Agency)는 2030년까지 1억대 이상의 전기자동차가 보급될 것으로 예상하고 있다[4].

전기자동차의 보급 확대를 위해서는 무엇보다 전기자동차 충전 기반시설의 구축이 필요하다. 전기자동차의 충전기반시설은 전력망의 효율적인 운용과 관리를 위해 스마트 그리드망의 한 부분으로 연구되고 있다[5]. 또한 급격히 증가하는 전기자동차의 배터리를 스마트 그리드 환경에서 전력부하만으로 생각하지 않고 분산 전력저장장치로도 이용하려는 Vehicle-To-Grid (V2G) 기술이 관심을 끌고 있으며 많은 연구가 이루어지고 있다[6,7]. 아래 그림 1은 스마트그리드 환경에서의 V2G 시스템을 보여주고 있다.

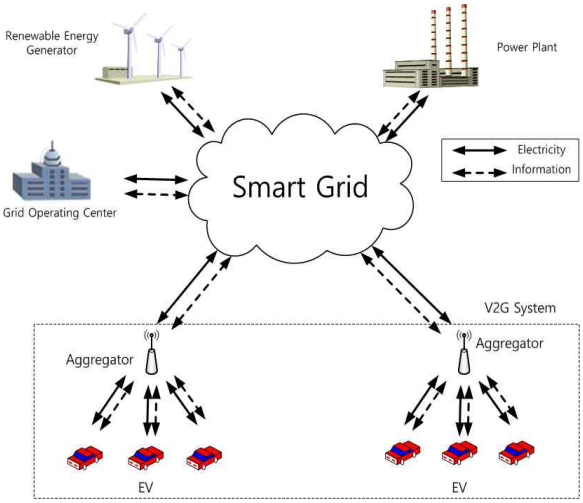

그림 1. 스마트그리드 환경에서의 V2G 시스템
Figure 1. V2G system in Smart Grid Environment

전기자동차 사용자는 전기자동차 충전기를 통하여 스마트 그리드망으로 연결된다. 일반적인 전기자동차는 전력망을 통해서 배터리를 충전하고 이 전력을 이용하여 전기모터를 구동하여 주행 하는 방식이다. V2G 기술을 이용하면 충전된 전기자동차의 배터리를 주행용도 뿐 아니라 전력저장장치 (Energy Storage System) 등의 용도로 사용하거나 전력요금이 저렴한 시간대에 배터리를 충전하고 전려요금이 비싼 시간대에 전력을 역전송하여 경제적 이익을 얻을 수도 있다. 또한 전기자동차의 배터리 전력을 이용하여 전력망운영자는 부하 평준화 (load Leveling)와 첨두부하저감 (Peak Load Shaving)과 같은 장점을 얻을 수 있다 [6].

스마트그리드와 V2G 시스템의 모든 요소는 양방향 통신망을 이용하여 연결되어 있다. 따라서 일반적인 통신 시스템에서 발생 할 수 있는 모든 형태의 보안 위험에 노출되어 있으며 통신망의 공격을 통해 개인정보 유출의 위험성 또한 언제나 존재한다. V2G 시스템의 경우 전기자동차는 이동성을 가지기 때문에 이동하지 않는 다른 스마트그리드 시스템에 비해서 보안 공격의 위험성에 더 많이 노출된다. 또한 AMI의 전력사용량 정보와 같은 다른 스마트그리드 요소들의 정보에 비해 전기자동차는 충방전을 위해 V2G 시스템과 여러 정보를 주고받아야 하며 이정보를 토대로 매우 민감한 개인정보 즉 운전자의 이동경로 , 시간대별 운전 패턴, 결제정보 등이 유출 될 수 있다. 따라서 V2G 시스템은 통신망의 보안 뿐 아니라 민감한 개인 정보 유출을 방지하기 위한 방안이 강구 되어야 한다.

본고에서는 V2G 시스템의 통신망의 구조와 특성에 대해 알아보고 V2G 통신망의 보안 위협과 개인정보 보호에 대해 분석하고 개인정보 보호를 위한 V2G 시스템의 운용 방안을 설명하고 제안한다. 2장에서는 V2G 시스템의 구조와 충방전 시나리오에 대해 알아본다. 3장에서는V2G 시스템에서 전송되는 개인정보와 보안 위험성 그리고 V2G 시스템의 보안 요구사항에 대해 설명한다. 4장에서는 V2G 시스템의 특성과 보안 분석을 바탕으로 효율적인 V2G 시스템 및 운용방안을 제안하고 마지막 5장 결론에서 끝을 맺는다.

II. V2G 시스템

1. V2G Network의 구조

V2G 시스템의 중요한 구성요소는 아래와 같이 전기자동차(EV), 중개자 (Aggregator, AG), 중앙 관리자 (Control Center, CC)가 있으며 전기자동차의 인증을 위한 인증센터 (Authentication Center, AC) 와 요금 결제를 위한 과금 센터 (Billing Center, BC)가 필요하다[8,9].

- 전기자동차 (EV): 개인이 소유한 전기자동차로 충전소를 이용하여 배터리를 충전하여 주행한다. 충방전기를 통하여 V2G 망에 접속하며 V2G 망에서는 전기자동차의 배터리가 전력 부하 뿐 아니라 에너지 저장장치와 분산 발전원의 역할로 이용 된다.
- 중개자 (Aggregator) : 많은 수의 전기자동차 배터리는 개별적으로 중앙의 제어를 받지 않고 지역이나 그룹별로 중개자 (Aggregator)를 통하여 V2G 시스템에 연결된다. 중개자는 전기자동차를 대신하여 전력 인프라와 통신망으로 연결하고 배터리의 충방전을 관리한다.
- 중앙관리자 (Control Center) : 전력망의 상태를 실시간 모니터링 하여 전기자동차의 충전 방전을 관리한다. 필요한 전력량에 따라 전기자동차의 충전 및 역전송 전력가격을 조정 하고 충전 및 방전(전력판매) 요청을 승인하거나 거부 할 수 있다.
- 인증 센터 (Authentication Center) : 전기자동차가 올바른 서비스 가입자 인지 접속 시 인증 절차를 수행하며 중앙관리센터에서 인증 서버를 설치하여 인증 절차를 수행 할 수도 있다.
- 과금 센터 (Billing Center) : 전력망에 접속한 전기자동차의 충전 전력량에 따라 비용을 부과한다. 기존 전력망의 과금 시스템과 달리 역전송된 전력량만큼의 금액을 서비스 가입자에게 지불하므로 양방향의 과금 시스템이 구축되어야한다.

그림 2에는 V2G 시스템의 구조가 나타나 있다. V2G 시스템은 중앙에서 전기자동차의 충방전을 관리하는 방식과 중앙의 관리 없이 운전자가 충방전을 결정하는 방식으로 나뉜다. 중앙의 관리 없이 운전자가 충전만을 할 경우는 운전자가 직접 배터리의 충전 상태를 확인하고 전력충전소의 전력 요금을 확인한 후 신용카드를 사용하여 원하는 만큼의 전력을 충전하면 된다. 이럴 경우는 전기자동차나 운전자의 신원을 확인하는 절차가 필요하지 않고 배터리의 충전상태 (SOC) 정보나 충전 요금 정보만 있어도 가능하다. 그러나 전기자동차 배터리의 충방전을 중앙에서 관리하거나 중앙에서의 충방전 관리가 없더라도 운전자가 전기자동차 배터리의 전력을 전력망으로 판매(역전송)할 경우에는 전기자동차나 운전자의 신원을 확인하는 절차가 필요하다.

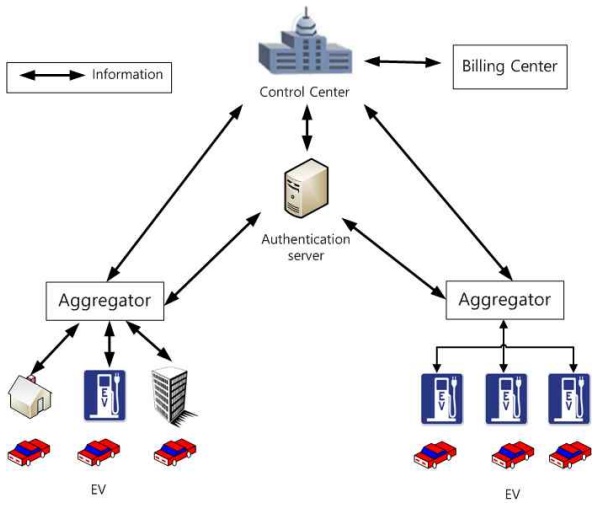

그림 2. V2G 시스템의 구성
Figure 2. Configuration of V2G System

2. 전기자동차 충방전 시나리오

현재 대부분의 전기자동차 운전자는 전력공급자와 계약을 통해 집에서 전력요금이 저렴한 야간 시간대를 이용하여 전기자동차를 충전하여 사용하고 있다. 공공 충전기반 시설 또한 전기자동차의 급속한 증가에 따라 빠르게 늘어나고 있으며 전기자동차와 충전기반시설 그리고 스마트 그리드 사이의 통신을 위한 표준화 작업도 ISO/IEC를 중심으로 진행 중이다. V2G 시스템은 아직 시험단계로 V2G 시스템의 운영을 위한 많은 연구가 이루어지고 있다[8,9]. 전기자동차와 충전기반시설 사이의 통신 표준인 ISO/IEC 15118 [10]은 충전을 위한 사용자 식별 방법을 아래와 같이 2가지 방식으로 분류한다.

- 외부 수단을 이용한 사용자 증명(External Identification Means) : 전기자동차 운전자가 충전을 위해 직접 인증작업 (Authentication)을 수행하는 방식으로 NFC, 전력공급자와 계약된 스마

트카드 그리고 스마트폰 등을 이용하여 사용자 인증을 할 수 있다. 이 방식을 사용할 경우 기존의 구축된 시스템을 사용할 수 있는 장점이 있으나 운전자가 충전기에 가서 직접 인증 및 지불을 해야 한다.

- 플러그 앤 차지 (Plug and Charge) : 전기자동차의 충전을 위해 충전기와 연결만 하면 통신망을 통해 모든 인증 절차, 과금정보, 제어정보 송수신이 이루어지는 방식.

중앙관리자의 제어를 받는 Plug and Charge 형태가 유력한 V2G 서비스는 아직 표준이 정해지지 않은 상태로 시스템 아키텍쳐, 통신방법, 인증방식, 과금체계 및 정보보호에 관해 많은 제안이 이루어지고 있다 [11,12,13,14]. 스마트 그리드의 중앙관리자(CC)는 전력수요가 실시간 발전 보다 늘어날 것으로 판단할 경우 중개자 (Aggregator)에게 전기자동차의 배터리 전력을 전송할 것을 요구하고 중개자는 이 메시지를 전기자동차에게 전달한다. 이 메시지는 중개자가 일정 범위내의 전기자동차에게 무선통신을 통해 전달하거나 V2I (Vehicle to Infrastructure)의 RSU (Road Side Unit)을 통하여 전기자동차에게 전달 할 수 있다. 이 메시지를 받은 전기 자동차는 전력을 판매할 것인지 혹은 충전을 할 것인지를 판단하고 응답 메시지를 보낸다. 그 후 충/방전을 위해 충방전설비로 이동하여 전력망에 접속한다. 충전기를 전기자동차에 연결하면 전기자동차 통신 콘트롤러 (Communication Controller)가 충전기를 거쳐 중개자(Aggregator)와 통신을 시작하고 중개자는 인증 절차를 통하여 전기자동차를 확인 한 후 세션을 형성한다. 중개자와의 인증절차를 통해 스마트그리망에 접속할 수도 있지만 중개자를 통하여 중앙의 인증센터로 연결하여 인증을 수행할 수도 있다. 인증센터에서는 접속한 전기자동차가 올바른 서비스 가입자임을 확인하고 세션을 형성한다. 또한 인증센터는 중개자와도 인증절차를 지속하여 가짜 중개자가 침입하지 못하도록 막는다. 이후 전기자동차는 충방전요구 정보, 배터리 정보, 접속가능시간등의 정보를 중앙관리자(CC)로 보내고 중앙관리자의 허가 후 충전 혹은 전력판매의 서비스를 시작한다. 중앙관리자(CC)는 서비스에 대한 대가를 과금 센터(Billing Center)를 통하여 징수하거나 지불한다. 이러한 서비스를 제공하기 위해 전기자동차와 중개자, 중앙관리자 사이에는 전기차 식별정보와 위치정보와 같은 많은 민감한 정보들이 오고가게 된다. 따라서 이를 보호하기 위한 보안 대책들이 필요하다.

III. V2G의 개인정보 및 보안 위험성

스마트 그리드와 V2G 시스템은 모든 구성원을 통신망으로 연결하여 모니터링과 관리를 통하여 보다 효율적인 전력망의 운영을 가능하게 한다. 하지만 정보교환을 위한 통신망의 이용은 일반적인 통신망의 보안문제를 그대로 가지된다. 또한 V2G 시스템은 전기자동차의 이동성으로 인해 스마트 그리드보다 더욱더 위험한 보안 문제점을 안고 있다. 스마트 그리드의 경우는 이동성 없이 고정된 전기기기가 계속 접속되어 있기 때문에 새로운 개체의 접속을 쉽게 알 수 있어 공격자가 침입하기가 상대적으로 어렵다. 하지만 전기자동차는 충방전 시간동안만 V2G 네트워크에 접속하고 고정된 망에 접속하는 것이 아니라 여러 네트워크를 돌아다니며 접속을 한다. 따라서 전기자동차가 V2G 망에 접속하지 않을 때 공격자가 신분을 도용하여 접속하여 서비스를 무상으로 이용 할 경우 확인이 쉽지 않다. 또한 전기자동차는 많은 네트워크를 옮겨 다니기 때문에 가짜 중개자(Aggregator)로 위장한 공격자로부터 결제 정보를 포함한 개인 정보가 유출 될 위험이 크다[13].

1. V2G 시스템의 개인정보

전기자동차가 충전 혹은 방전하기 위해 전기충전기와 연결되면 이 둘 사이에 세션 연결을 위한 통신을 시작한다. 전기자동차와 충전기 사이에는 전력선통신 (Power Line Communication)이나 무선통신 기술을 이용 하여 메시지를 송수신한다. 충전기에서 중개자 ,중개자에서 중앙의 관리자로는 기존의 인터넷이나 LTE 망 등을 이용할 수 있다. 표 1 에는 전기자동차와 충전 인프라 사이에 교환되는 정보가 나타나 있다[13,15].

V2G 네트워크에서 송수신 되는 제어명령 및 설정 데이터가 공격자에 의해 위조 혹은 변경 될 경우는 V2G 시스템의 안정성과 신뢰성을 회손 하며 안전에도 문제를 일으킬 수 가있다 [15]. 계량 정보가 위조 혹은 변조 될 시에는 소비자는 사용한 전력보다 많은 돈을 지불 하거나 판매한 전력량보다 적은 금액을 받는 등의 금전적인 손실을 입을 수 있다. 혹은 반대로 전력공급

자가 손실을 입을 수도 있다. 판매 혹은 충전 전력 요금정보가 변조 되었을 경우는 소비자가 정확한 전력요금을 알지 못하고 잘못된 정보를 기반으로 이용할 서비스를 결정하기 때문에 고객의 적절한 서비스 선택(충전 혹은 전력판매)을 어렵게 한다. 전력공급자 또한 잘못된 전력요금을 고객들에게 전달함으로 고객의 신뢰도가 낮아지는 피해를 입게 된다.

표 1. V2G 네트워크에서 교환 되는 정보
Table 1. Informations exchanged in V2G network

정보	내용
고객 식별 정보	고객 이름, 차대번호(Vehicle identification Number)등 고객이나 전기자동차의 식별 및 인증 정보
배터리 정보	배터리의 충전 정보 (State of Charge)
위치 정보	사용 충전기 식별 및 위치 정보
계량 정보	일정시간 동안의 충전 혹은 방전한 전력량 정보
제어 명령	요구 수행, 경보 및 서비스 실행을 위한 제어 명령
설정 데이터	시스템의 설정 값, 경보의 임계치값의 시스템 정보
요금 정보	고객에게 제공 되는 실시간의 전력 충전 및 방전 요금 정보
결제 정보	전기자동차가 제공한 서비스의 대가를 지불하거나 혹은 받기 위한 결제정보

외부로의 유출을 막고 내부 망에서도 보호해야할 개인정보들로는 고객 ID, 위치정보, 배터리 정보 그리고 결제 정보가 있다. 고객 식별 정보로 서비스가입자나 전기자동차를 식별하게 되면 충전 위치정보를 기반으로 가입자나 전기자동차의 행동반경이나 특정지역을 방문하는 경향을 유추 할 수 있다. 또한 배터리 정보를 토대로 전기자동차의 주행거리나 운전 패턴을 추측해 볼 수도 있다. 결제 정보가 유출될시 에는 악의를 품은 다른 사용자가 이 정보를 이용하여 서비스를 이용할 수 있으므로 유출시 매우 위험하다.

2. V2G 네트워크 보안 위험성

V2G 네트워크는 유무선의 통신 네트워크를 이용하므로 기존의 통신 네트워크의 보안 문제점을 그대로 가지고 있으며 이동성으로 인해 기존의 스마트 그리드 보다 더 높은 보안 위험성을 가진다. V2G 네트워크에서 대표적인 보안 위협을 아래에 설명하였다[9,12].

- 도청(Sniffing) : 전기자동차와 충전 인프라 사이의 정보 교환을 엿듣는 공격으로 전기자동차와 충전기가 무선통신망을 통해 연결될 경우 공격자는 물리적인 접속 없이 근접거리에서 전송되는 정보를 중간에서 엿들을 수 있다. 이러한 엿듣기는 인터넷 환경에서는 프러미스큐스 모드(Promiscuous Mode)로 네트워크 인터페이스 카드를 설정시 누구나 쉽게 할 수 있는 공격으로 이러한 단순한 공격으로도 고객식별정보 , 위치정보, 및 과금정보등의 민감한 개인정보가 유출 될 수 있다.
- 중간자 공격(Man In The Middle Attack) : 공격자가 전기자동차와 중개자 혹은 중개자와 중앙제어자 사이에 끼어들어 정보를 중개하는 형태의 공격으로 민감한 개인 정보를 유출하거나 전송되는 정보를 위변조하여 아무런 문제가 없는 정보인 것처럼 전송할 수 있다. 공격자가 중간에서 미터 정보를 실제 충전량 보다 많게 변조 한다면 고객은 실제 충전량 보다 훨씬 더 많은 비용을 지불하게 된다.
- 재전송 공격(Replay Attack) : 이미 전송된 명령이나 메시지를 정상적인 새로운 메시지인 것처럼 보내는 공격법으로 정상적인 충전서비스의 결제 정보 메시지를 복사 혹은 저장 하였다가 공격자가 미리 복제한 이 결제정보를 과금 시스템으로 전송하여 대금이 지불되면 공격자는 공짜로 서비스를 이용하고 결제 정보가 유출된 다른 사용자가 이 공격자의 서비스 비용을 지불하는 피해가 발생한다.
- 위장공격 (Impersonation Attack) : 공격자가 정상적인 서비스 이용자나 충전기반시설의 중개자로 위장하는 공격으로 공격자가 전기자동차의 식별정보나 비밀키(Secret Key)와 같은 정보를 알게 되면 공격자가 피해 전기자동차인 것처럼 위장하여 중개자로 접속하고 서비스를 제공받을 수 있다. 또한 공격자가 중개자인 것처럼 위장하여 전기자동차 사용자에게 조작된 메시지를 보낼 수 있다.
- 부인공격(Repudiation Attack) : 전기자동차 사용자가 충전 등의 서비스 사용 후 서비스를 사용하거나 어떤 특정한 행동을 한 적이 없다고 부인하는 공격 형태로 실제 개인정보가 도용되어서

입은 피해인지 부인공격의 형태인지 구별하여야 한다.

- 서비스거부 공격 (Denial of Service Attack) : 전기자동차와 충전기사이가 무선 네트워크로 통신이 이루어질 경우 공격자는 완전한 세션을 형성하지 않고 계속적인 인증요청으로 시스템의 자원을 소모시켜 실제 서비스를 이용하려는 전기자동차 사용자들이 V2G망에 접속할 수 없게 하는 형태의 공격이 가능하다. 전력선통신(PLC)과 같은 유선통신기술을 사용하여 전기자동차가 V2G망에 접속하는 경우는 충전기가 전기자동차와 물리적으로 연결되어야지만 통신 세션이 형성되기 때문에 이러한 형태의 공격 위험성은 낮아진다.

3. V2G 시스템의 보안요구사항

V2G 시스템은 기존의 통신네트워크에서와 같은 보안 위험성을 가지지만 전기자동차는 고정된 네트워크에 머무르는 것이 아니라 여러 네트워크들을 이동하면서 충전 혹은 전력판매(방전)을 위해 민감한 개인정보를 송수신한다. 그리고 전기자동차의 통신 콘트롤러는 일반 컴퓨터와 같은 고성능의 처리기능을 가지지 못하기 때문에 이러한 특성을 고려하여 보안 체계를 구성하고 V2G 시스템을 운영하여야 한다. V2G 시스템이 가져야할 보안요소를 아래에 설명하였다[8,15].

- 전송데이터의 암호화 : V2G 시스템의 전기충전기, 중개자 그리고 중앙의 관리자 사이의 통신은 기존의 통신 인프라 즉 인터넷망의 TLS 프로토콜과 같은 보안 채널을 이용하여 연결할 수 있다. 그러나 전기자동차와 전기충전기사이의 통신기술인 전력선통신이나 무선통신기술은 그 특성상 데이터 유출에 매우 취약한 기술이다. 따라서 정보의 기밀성(Confidentiality)보장을 위해서 암호화 시스템의 사용이 필요하다. ISO/IEC 15118에서는 비대칭 암호 기술인 공개키 기반기술 (PKI)들 사용하나 이 기술은 매우 높은 연산능력과 시간이 소모 되므로 전기자동차에 사용하기 위해서는 전기자동차의 정보처리기능이 더욱 강화 되어야한다.
- 양방향 및 지속적인 인증 : 정당한 서비스 가입자만 V2G망에 접속할 수 있도록 전기자동차의 신분을 확인하는 인증은 매우 중요한 요소이다. 기존의 통신 시스템이나 ISO/IEC 15118 표준은 중앙의 서버만이 가입자의 신분을 확인한다. 하지만 공격자가 중개자나 다른 V2G망의 요소로 위장할 수 있으므로 서비스 사용자쪽 에서도 올바른 서비스 제공자인지 확인을 하여야 한다. 또한 중앙관리자는 여러 지역에 설치되어 있는 중개자와 주기적으로 인증작업을 통해 공격자의 침투를 막아야 한다.
- 개인정보 보호 : 전기자동차와 V2G망 사이에 교환되는 정보가 누구의 것인지 추측 할 수 없어야 하며 전기자동차의 이동과 행동 패턴의 추측이 불가능해야 한다. 중개자가 전기자동차의 ID나 충전시간, 배터리 상태와 같은 정보를 알수 있다면 특정 서비스가입자의 이동경로, 이동패턴등의 분석이 가능함으로 중개자(Aggregator)는 서비스 사용자의 개인정보에 대해 알 수 없어야 한다.

Ⅳ. 제안하는 V2G 시스템

V2G 시스템의 특성과 위에서 언급한 보안 요소들을 고려하여 효율적이고 비용 부담이 적은 V2G 시스템을 제안한다. 그림3은 제안한 V2G 시스템의 구조를 보여주고 있다.

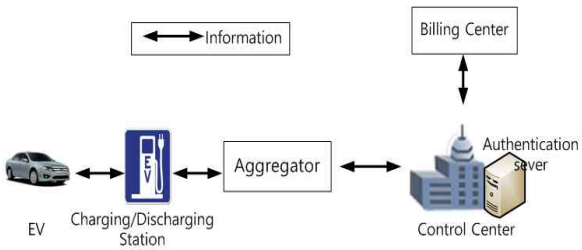

그림 3. 제안하는 V2G 시스템의 구성
Figure 3. Architecture of V2G system

충전 및 방전(전력판매) 서비스를 사용하기 위해 전기자동차 사용자는 미리 서비스에 가입을 하고 가입자는 가입자 ID와 비밀문자열을 설정한다. 가입자의 ID는 가입자나 차량의 종류를 유추 할 수 없게 설정하여야 하고 가입자는 서비스 제공자에게 차량의 고유번호(VIN)와 최소한의 개인정보를 제공하여 개인계정(account)을 만든다. 개인결제정보는 제공하지 않으며 서비스 사용대금은 개인계정에 저장되며 추후 청구되거나 지불된다. 서비스 제공자도 가입자별로 고유의 비밀문자열를 부여한다. 가입자와 서비스 제공자의 비밀문자열은 정해진 정책에 의해서 주기적으로 변경되어

야 하며 정해진 해쉬(HASH) 알고리즘에 의해서 해쉬된 양측의 비밀문자열은 대칭 암호알고리즘의 비밀키로 사용한다. 전기자동차와 서비스 제공자는 서로의 비밀 문자열만 저장하며 암호화 및 복호화 시는 저장된 비밀 문자열의 해쉬값을 계산해 비밀키로 사용하며 키값은 저장하지 않는다. 사용하는 해쉬 알고리즘 또한 주기적으로 변경한다. 전기자동차와 충전기사이의 통신은 유선통신 기술인 전력선통신을 이용하여 충전기나 중개자에 대한 서비스거부공격(DoS)의 가능성을 차단한다. 그리고 중앙의 콘트롤 센터는 각 지역의 중개자와 주기적으로 인증작업을 수행하여 공격자의 침입을 방지한다. 제안하는 시스템은 아래와 같은 방식으로 작동한다.

1. 전기자동차가 충전기에 연결되면 충전기와 통신 세션을 형성하고 전기자동차의 통신 콘트롤러는 가입자ID 와 해쉬된 차량 정보, 서비스 요청(충전 혹은 방전)을 가입자의 비밀키로 암호화 하여 충전기와 중개자를 거쳐 서비스제공자의 중앙 콘트롤 센터로 보낸다. 충전기와 중개자는 이정보를 저장하지 않고 바로 중앙의 콘트롤 센터로 전송한다.

2. 중앙의 콘트롤 센터는 전기자동차로부터 받은 가입자ID로 저장된 가입자의 비밀번호를 확인한다. 이 비밀번호를 미리 약속된 방식으로 해쉬 하여 가입자의 비밀키를 구한다. 이 비밀키를 이용하여 해쉬된 차량정보를 복호화 한 후 계산한 해쉬값과 비교하여 서비스 사용자의 신원을 확인한다.

3. 서비스 요청자가 정당한 가입자로 확인되면 서비스 제공자는 해쉬된 차량고유번호, 접속승인, 서비스제공 내용 등의 정보를 서비스제공자 자신의 비밀키로 암호화 하여 전기자동차로 전송한다.

4. 전기자동차의 통신 콘트롤러는 저장된 서비스제공자의 비밀문자열을 약속된 방식으로 해쉬하여 비밀키를 구한다. 이를 이용하여 메시지를 복호화 하고 자신의 해쉬된 차량고유번호를 확인하여 서비스제공자의 신원을 확인한다. 이후 서비스에 필요한 모든 정보는 서로의 비밀키로 암호화 하여 통신한다.

5. 서비스 종료 후 발생한 비용이나 얻은 이익은 가입자의 개인계좌에 기록되고 V2G 시스템과는 무관한 기존의 결재 시스템을 사용하여 결재서비스를 이용한다. 가입자는 인터넷을 이용하여 자신의 서비스이용 내역, 결재정보를 확인할 수 있다.

제안한 방식은 공개키 암호알고리즘보다 처리속도가 빠르고 계산량이 적은 대칭키 암호알고리즘과 해쉬 알고리즘을 사용하여 효율을 높이고 전기자동차의 부담을 줄였다. 민감한 정보인 차량고유번호(VIN), 암호 비밀키는 전기자동차나 서비스 제공자에 저장되지 않고 차량고유번호와 비밀문자열의 해쉬값을 식별정보와 암호 비밀키로 이용하여 혹시 모를 전기자동차의 해킹 시에도 암호키와 식별정보가 직접적으로 유출 되지 않도록 하였다. 그리고 유출시 위험도가 큰 결재정보는 시스템에 저장되지 않고 가입자가 자신의 계좌 정보를 확인 후 직접 처리하도록 설계하였다. 처음 전기자동차가 중앙의 콘트롤 센터에 보내는 메시지의 가입자 ID정보를 제외하고는 모든 데이터가 대칭키 암호알고리즘으로 암호화 되어 보호된다. 그리고 암호화키 생성에 사용되는 비밀문자열과 해쉬 알고리즘도 일정 횟수 사용 후에는 변경하여 보안을 더욱 강화 하였다. 민감한 개인정보인 가입자ID 는 통신 시작시 한번 암호화 되지 않은 상태로 중앙의 관리자로 전송되지만 전력선 통신을 사용하여 전기자동차가 전기충전기와 연결되기 때문에 전기충전기에서의 도청은 매우 힘들다. 중개자나 그이후의 단계에서 이 정보가 유출되더라도 가입자 ID는 가입자나 전기자동차에 대해 추즉 할 수 있는 아무런 정보가 없기 때문에 도청한 정보가 어느 전기자동차의 것인지 알기는 매우 힘들다. 또한 사용자 ID도 일정 횟수 사용 후 변경하거나 여러 개를 특정한 규칙에 의해 사용해서 보안성을 높일 수 있다.

V. 결론

본고에서는 V2G 네트워크의 구조와 개인정보, 보안 취약점과 보안요구사항에 대해 알아보고 효율적인 V2G 시스템을 제안하였다. V2G 시스템은 기존의 통신 기술을 이용하기 때문에 기존의 통신네트워크 및 스마트 그리드와 같은 보안 위험성을 가지고 있다. 하지만 V2G 시스템은 전기자동차의 이동성과 같은 시스템의 특성상 기존의 통신망 보다 더욱 보안에 취약한 점이 존재하며 민감한 개인정보가 교환되기 때문에 개인정보 유출에 대한 대비가 필요하다. 시스템을 설계할 때 전기자동차의 제한된 연산능력 또한 고려되어야 한다. 전기자동차는 특정 네트워크에 머물러있는 것이 아니

라 여러 네트워크를 이동하며 충전이나 방전 서비스 시에만 V2G망에 접속한다. 따라서 공격자가 피해 전기자동차의 신분을 위조하여 망에 접속하여도 중앙의 관리자는 이를 식별하기가 쉽지 않다. 그리고 전기자동차도 새로운 망으로 이동시 정당한 서비스 제공자인지 확인 후 망에 접속하여야 한다. 제안하는 시스템은 전기자동차와 서비스 제공자와의 양방향 인증을 수행하고 연산의 부담이 적은 대칭키 암호와 해쉬 알고리즘을 이용하여 정보 유출에 대비하였다. 그리고 전기자동차를 식별할 수 있는 정보의 교환을 최소화 하고 민감한 결재 정보는 중앙에서 처리하도록 설계하였다. 현재 V2G 시스템은 상용화 되지 않은 단계로 상호인증, 결재시스템, 전기자동차의 이동성 관리 등 V2G 시스템의 보안 및 개인정보 보호를 위한 더 많은 연구가 이루어 져야 할 것이다.

References

[1] Fang, Xi , Misra, Satyajayant , Xue, Guoliang , Yang, Dejun “Smart Grid – The New and Improved Power Grid: A Survey“ IEEE Communications Surveys & Tutorials, Vol.14, Issue. 4 , 2011, pp 944-989
DOI: 10.1109/SURV.2011.101911.00087

[2] Nazmus S.Nafi, Khandakar Ahmed, Mark A Gregory, Manoj Datta “ A survey of smart grid architecture, applications, benefits and standardization” Journal of Network and Computer Applications 76, 2016, pp.23-36

[3] Martion Tran, Justin D.K Bishop, David Banister, Malcom D. McCulloch, “ Realizing the Electric Vehicle Revolution ” Natural Climate Change, 2, pp. 328-333, 2012

[4] IEA, Global EV Outlook 2018

[5] Murat Yilmaz, Philip T.Krein “ Review of the Impact of Vehicle-to-Grid Technologies on Distribution Systems and Utility Interfaces” IEEE Transactions on power electronics“ Vol.28,N0.12,2013,pp.5673-5689
DOI: 10.1109/TPEL.2012.2227500

[6] Salman Hahih, Muhammad Kamran, Umar Rahid “Impact analysis of vehicle-to-grid techology and charging strategies of electri vehicle on distribution networks-A review”, Journal of Power Sources 277 pp.205-214, 2015

[7]Nathaniel S. Pearr, Hajo Ribberink “Review of research on V2X technologies, stragies and options ” Renewable and Sustainable Energy Reviews“ 105, pp.61-70, 2019

[8] Yan Zhang , Stein Gjessing, Hong Liu, Huansheng Ning, Laurence T.Yang, Mohsen Guizani “Securing Vehicle - To - Grid Communications in The Smart Grid”, IEEE Wireless ommunications ,vol.20, Issue 6 ,2013, pp. 66-75
DOI: 10.1109/MWC.2013.6704476

[9] Neetesh Saxena, Santiago Grijalva, Victor Chukwuka, Athansio V.Vasilakos “ Network Security and Privacy Challenges in Smart Vehicle-To-Grid” IEEE Wireless ommunications Vol.24 Issue 4, 2017, pp.88-98
DOI: 10.1109/MWC.2016.1600039WC

[10] ISO 15118 manual, “Mastering the Vehicle-2-Grid(V2G) Communication Interface”, https://www.v2g-clarity.com

[11] Zhenyu Yang, Shucheng Yu, Wenjing Lou, Cong Liu “ P2: Privacy-Preserving Communication and Precise Reward” IEEE Transaction On Smart Grid, Vol.2, No.4 ,2011 pp. 697-706

[12] Aljawharah Alnasser, Hongjian Sun,Jing Jiang “ Cyber security challenges and solutions for V2X communications: A survey” Computer Networks 151, 2019, pp.52-67
DOI: 10.1016/j.comnet.2018.12.018

[13] Wenlin Han, Yang Xiao, “Privacy preservation for V2G networks in smart grid: A survey” Computer Communications, 91-92, pp.17-28,2016
DOI: 10.1016/j.comcom.2016.06.006

[14] Zhiguo Wan, Wen Tao Zhu, Guilin Wang, “PRAC:Efficient privacy protection for vehicle-to-grid communications in the smart grid” Computers & Security 62, 2016, pp.246-256

[15] Rainer Falk and Steffen Fries, “Securely connecting Electric Vehicles to the Smart Grid” International Journal on Advances in Internet Technology, vol6, pp.57-67, 2013

※ 이 논문은 2019년도 한남대학교 학술연구비 지원에 의하여 연구되었음