The Journal of the Convergence on Culture Technology (JCCT)
Vol. 7, No. 1, pp.551-557, February 28, 2021. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2021.7.1.551
JCCT 2021-2-68

정보보호를 고려한 전기자동차 충방전 시스템의 인증과 운영에 관한 연구

Secured Authentication Scheme and Charging & Discharging System Operation for Electric Vehicles

이성욱

Sunguk Lee*

요 약 전기자동차의 증가에 따라 공공장소의 전기자동차 충방전 기반시설 또한 급격히 늘어나고 있다. 전기자동차의 충방전을 위해서는 보안상의 취약점을 최소화하기 위해 전기자동차와 서비스 제공자가 서로의 신원을 확인하는 상호 인증과정 후에 충방전 서비스를 시작하여야 한다. 본고에서는 해쉬함수와 메시지 인증코드를 사용하여 전기자동차와 충방전 서비스 제공자간의 양방향 인증 방법을 제안한다. 그리고 효율적인 충방전 시스템의 운영에 대해 기술한다. 제안된 시스템은 외부로 부터의 공격에 강한 내성을 가지며 충방전 서비스 이용자의 개인정보를 효과적으로 보호할 수 있다.

주요어 : 전기자동차, 충전, 방전 , 개인정보 보호 , 인증, 보안

Abstract With increase of electric vehicle in the road, the number of charging/discharging infrastructure for electric vehicle in public space is also increased rapidly. To charge or discharge the electric vehicle the user of electric vehicle and service provider should verify the each other's identity to minimize security vulnerability. This paper proposes mutual authentication scheme between electric vehicle and charging/discharging service provider with help of hash function and Message Authentication Code(MAC). Also efficient operating scheme for charging/discharging service system is proposed. The analysis shows that the system has robustness against security vulnerability. Also this system can keep the sensitive personal information of service user safely.

Key words : Electric Vehicle, Charging, Privacy , Authentication. Security

*정회원, 한남학교 멀티미디어공학과

Received: December 8, 2020 / Revised: December 28, 2020
Accepted: January 15, 2021

접수일: 2020년 12월 8일, 수정완료일: 2020년 12월 28일
게재확정일: 2021년 1월 15일

Dept. of Multimedia Engineering , Hannam Univ, Korea

Ⅰ. 서 론

이산화탄소 배출을 줄이기 위한 전 세계적인 노력의 하나로 전통적인 내연기관 자동차를 대신할 전기자동차의 보급은 매년 증가하고 있으며 이에 따른 전기자동차의 충전을 위한 기반시설의 설치 또한 빠르게 진행중에 있다[1]. 정책적인 지원으로 많은 아파트나 거주용 주택에서 전기자동차 충전 시설이 설치되고 있으며 고속도로 휴게소등과 같은 공공장소의 충전시설도 빠르게 보급되고 있다. 전기자동차 보급 초기에는 내연기관을 보조하는 하이브리드 전기자동차가 주류를 이루었으나 현재는 배터리의 전력만으로 구동하는 전기자동차가 판매의 대부분을 차지한다. 또한 기술의 발달로 배터리의 용량은 점점 더 커져가고 있다. 이에 늘어가는 전기자동차 배터리의 전력을 스마트 그리드[2] 환경에서 전력저장장치나 분산전원으로 사용하려는 Vehicle to Grid (V2G)[3] 기술이 관심을 끌고 있다. 이를 위해서는 전기자동차가 스마트 그리드망에 연결하여 전력을 전송하거나 배터리를 충전할 수 있어야 하며 또한 스마트그리드 통신망과 충/방전 기반시설과 양방향 통신을 통하여 연결되어야 한다. 그림 1.은 스마트 그리드 환경에서의 V2G 시스템을 보여주고 있다.

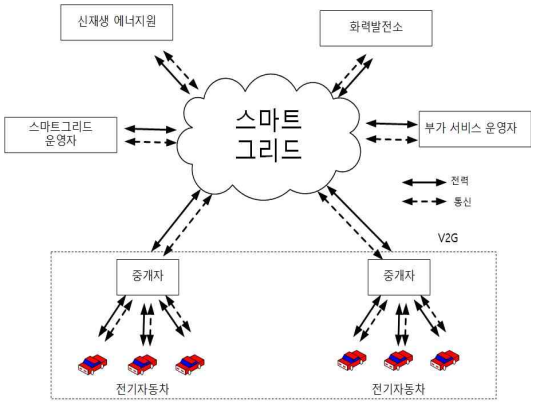

그림 1. 스마트그리드 환경에서의 V2G 시스템
Figure 1. V2G system in Smart Grid Environment

전기자동차는 한곳에서만 충전 혹은 방전을 하지 않고 계속 이동하여 충/방전 위치가 계속 변한다. 또한 아주 짧은 시간만 충방전을 위해 전력망과 통신망에 접속을 하고 오랜 시간동안에 통신망에 접속을 하지 않을 수도 있다. 따라서 전기 자동차는 여러 통신망을 옮겨다니며 새로운 통신망에 접속 하기 때문에 신분을 위장한 공격자로부터 공격당할 가능성도 높아진다. 충방전 서비스 제공자 입장에서는 전기자동차가 통신망에 오랜 시간 동안 접속을 하지 않기 때문에 공격자가 신분을 위조하여 정상적인 사용자인 것처럼 망에 접속하여도 알아내기가 쉽지 않다.[4] 또한 전기자동차의 충방전을 위해서는 전기자동차의 사용자 ID, 위치정보, 배터리 정보 그리고 결제정보와 같은 민감한 개인정보들이 서비스 제공자에게 제공 되어야 한다. 이러한 보안 위험성과 개인정보의 보호를 위해서 전기자동차와 충방전 서비스망 사이에는 지속적인 인증과 통신채널의 암호화 그리고 메시지의 무결성 확인이 요구된다 [5]. ISO/IEC 15118 표준은 공개키 기반구조 (Public Key Infrastructure, PKI)[6]를 사용한 V2G 네트워크를 제안하였고 많은 연구자들이 전기자동차의 충방전 서비스를 위한 인증(authentication), 보안과 개인정보보호를 위한 연구를 수행하고 있다[5,6,7,8]. 본고에서는 전기자동차의 충방전 서비스를 위한 인증 프로토콜과 충방전 시스템의 운영방안을 제안한다. 공개키 기반 구조나 암호 알고리즘 대신 계산량이 많지 않고 빨리 처리 되는 해쉬 함수[9]와 메시지의 무결성을 확인할수 있는 메시지 인증 코드 (Message Authentication Code)[9]를 이용한 상호 인증 프로토콜을 제안한다. 또한 제안한 시스템의 보안성과 개인정보보호에 대한 분석도 수행하였다. 2장에서는 충방전 시스템의 설계 및 운영에 대해 알아본다. 3장에서는 제안한 시스템의 보안성과 개인정보보호에 대해 분석하고 마지막 4장 결론에서 끝을 맺는다.

Ⅱ. 충/방전 시스템 설계 및 운영

이 시스템은 도로상에 RSU들이 넓게 배치된 상태가 아닌 충/방전소 부근 일정 반경에서만 전기자동차나 전기자동차 사용자와 충/방전 기반시설이 DSRC (Dedicated Short Range Communication), Bluetooth 나 WIFI를 통해서 통신하는 환경을 기반으로 한다. 전기자동차는 OBU(Onboard Unit)가 탑재 되어 충/방전 기반시설과 통신 하고 인증을 위한 계산을 수행한다. OBU가 없을 경우는 전기자동차 사용자의 스마트폰에 설치한 서비스사용자 어플리케이션을 이용하여 직접 충방전 기반시설과 통신을 수행할 수 있다. 그림 2는

제안하는 충방전 시스템의 통신네트워크 구성을 보여 주고 있다.

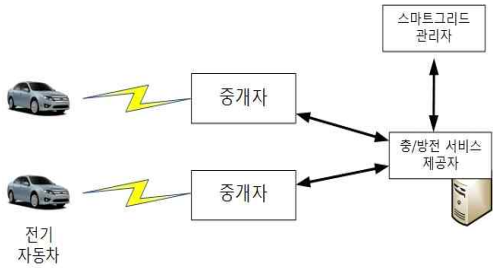

그림 2. 충방전 서비스 시스템의 통신 네트워크
Figure 2. Communication Network for charging/discharging service system

1. 충방전 서비스 환경 및 사용자 가입

전기자동차 사용자는 충전 혹은 전력 판매 전에 서비스 제공자에 자신의 개인 정보와 결제 정보를 제공하고 사용자로 등록한다. 전기자동차 사용자가 충방전 서비스 제공자에게 등록해야 하는 정보는 다음과 같다.

- 사용자 ID : 사용자가 사용할 개인 식별자, 사용자나 자동차의 정보를 유추할수 없는 식별자를 선택 (E-mail, 전화번호 , Vehicle Identification Number 제외)
- 서비스 ID : 서비스 제공자가 사용할 사용자의 식별자.
- 결제 정보 : 신용카드 정보나 은행 계좌 정보

서비스 제공자는 위의 개인 정보를 데이터베이스에 저장하고 서비스 가입자에게 일회용 비밀번호 (OPT)발생기를 발급한다. 서비스 가입자가 충전 혹은 전력판매 서비스 이용을 시작 할 때에 일회용 비밀번호[10]를 이용하여 상호 인증 (Mutual Authentication)과정을 통하여 서비스 제공자와 통신을 시작한다. 웹기반의 OPT 발생기를 전기자동차 사용자의 스마트폰 어플리케이션을 통하여 사용 할 수도 있으며 전기자동차의 OBU에 직접 탑재하여 사용할 수도 있을 것이다. 사용자의 스마트폰은 전기자동차 내부의 버스를 통해 OBU와 통신할 수 있다고 가정한다. 중개자(Aggregator)의 식별자(ID) 또한 충방전 서비스 제공자의 데이터 베이스에 저장되고 관리되며 중개자와 서비스 제공자도 OTP를 이용하여 지속적인 상호 인증을 수행한다. 아래 표 1은 제안된 시스템 설명에 사용되는 기호들을 나타낸다.

표 1. 기호 표기법
Table 1. Notations

심볼	내용
ID_e	전기자동차 사용자의 ID
ID_a	중개자의 ID
SID_e	전기자동차 사용자의 서비스 ID
SID_a	중개자의 서비스 ID
$H(\ )$	해쉬 함수
$HMAC(k,m)$	해쉬된 메시지 인증코드 , k:키, m:메시지
k_e	전기자동차의 비밀값
k_a	중개자의 비밀값
O_e	전기자동차의 일회용 비밀값(OTP)
O_a	중개자의 일회용 비밀값 (OTP)
O_{se}	서비스제공자와 전기자동차의 OTP
O_{sa}	서비스제공자와 중개자의 OTP
$\|$	메시지 연결

2. 충방전 서비스

전기자동차가 충전이나 전력 판매를 위해 전력망과 서비스 제공자와 통신망을 연결하기 위해서는 먼저 전기 자동차 혹은 전기자동차 사용자가 정당한 사용자인지를 확인하는 인증 (Authentication) 과정을 거쳐야만 충방전 서비스망에 접속하여 서비스를 제공받을 수 있다.

1) 인증

인증 과정을 수행하기 위해 전기자동차는 아래와 같은 계산을 수행하여 필요한 값을 구한다 .

- 전기자동차의 비밀값 k_e
- 일회용암호(OTP)를 이용한 전기자동차와 서비스제공자의 비밀값 O_e
- O_e의 해쉬값 : 일회용 비밀값 O_e의 해쉬값 $H(O_e)$
- 사용자 ID와 O_e의 해쉬값 : 서비스 제공자에게 미리 등록한 자신의 식별자 ID_e 와 일회용 비밀값 O_e를 연결한 값의 해쉬값 $H(ID_e \| O_e)$
- ID_e 의 코드값 : 아스키 코드와 값은 코드를 이용한 ID_e 의 코드값 $C(ID_e)$
- 디피-헬만 키교환 프로토콜[9]을 위한 모듈러스 값 q와 p 값 설정

인증 절차를 위해 전기 자동차는 충전기를 통하거나 혹은 직접 중개자(Aggregator)에 아래의 메시지를 보낸다.

$$M_e = C(ID_e)H(O_e) \| H(ID_e \| O_e) \| g^{ke} \bmod q$$
$$S_e = HMAC(\ O_e\ ,\ M_e\ )$$

중개자는 충방전 서비스를 원하는 전기자동차와 서비스제공자에 대한 인증과 전기자동차와의 공유 세션키 값을 얻기 위해 다음의 계산값을 구한다.

- 일회용비밀값(OTP)를 이용한 중개자와 서비스 제공자의 비밀값 O_a
- O_a의 해쉬값 : 중개자의 일회용 비밀값 O_a 의 해쉬값 $H(O_a)$
- 중개자 ID와 O_a 의 해쉬값 : 서비스 제공자에게 미리 등록한 중개자 식별자 ID_a 와 O_a 연결한 값의 해쉬값 $H(ID_a \| O_a)$
- ID_a 의 코드값 : 아스키 코드와 값은 코드를 이용한 중개자의 식별자 ID_a 의 코드값 $C(ID_a)$
- 중개자의 비밀값 k_a

위 값들을 이용하여 중개자는 메시지 Ma , Sa 를 생성하고 전기자동차로부터 받은 메시지 Me , Se와 함께 서비스 제공자로 보낸다.

$$M_a = C(ID_a)H(O_a) \| H(ID_a \| O_a)$$
$$S_a = HMAC(O_a, M_a)$$
$$M_e = C(ID_e)H(O_e) \| H(ID_e \| O_e) \| g^{ke} \bmod q$$
$$S_e = HMAC(O_e, M_e)$$

중개자로부터 위 메시지를 받은 서비스 제공자는 미리 약속된 OTP 발생기를 통해 전기자동차, 중개자와 공통된 비밀값 Ose 와 Osa 를 각각 구하고 이 값의 해쉬값 H(Ose) 와 H(Osa)를 계산한다 . 해쉬함수의 종류 또한 미리 약속한다. Ma 메시지중 중개자 ID의 코드값과 Oa해쉬값의 곱인 C(IDa)H(Oa) 에 서비스제공자가 계산한 H(Osa)를 이용하여 중개자 ID의 코드값 C(IDa)를 구하고 이 중개자의 ID가 서비스제공자의 데이터베이스에 등록된 정상적인 중개자인지 확인한다. 전기자동차의 ID도 중개자와 같은 방식으로 데이터베이스에 등록되어 있는지 확인한다. 등록된 ID가 아닐 경우는 정상적인 사용자나 중개자가 아닌 것으로 판단하고 서비스를 시작하지 않는다. 이 경우는 사용자 ID가 위조되었거나 일회용 비밀값이 서로 일치하지 않는 경우이다. 서비스 제공자는 전기자동차와 중개자의 ID가 등록된 ID임을 확인하고 자신의 데이터베이스에 저장된 전기자동차와 중개자의 ID 값을 이용하여 H(IDe ‖ Ose) 와 H(IDa ‖ Osa) 를 구한다. 중개자로부터 온 메시지 Ma와Osa 를 이용하여 아래 값을 구한다.

$$S_{sa} = HMAC(O_{sa}, M_a)$$

H(IDa ‖ Osa)=H(IDa ‖ Oa) 이고 계산한 Ssa 값이 Sa 와 같다면 중개자의 신원이 확인되어 중개자의 인증이 완료된다. 또한 메시지 인증 코드로부터 중개자로부터 온 메시지의 무결성도 확인이 된다. Me 메시지중 H(IDe ‖ Oe) 와 서비스 제공자가 계산한 H(IDe ‖ Ose) 가 동일하고 계산한 값 Sse = HMAC(Ose, Me) 와 Se 의 값이 같다면 서비스망에 접속을 원하는 전기자동차의 신원도 확인이 되어 인증절차가 완료된다. 또한 메시지 인증 코드로 이 메시지의 무결성을 확인할 수 있다. 이러한 절차를 통해서 서비스 제공자는 전기자동차와 중개자에 대한 신원 확인 즉 인증을 수행함과 더불어 인증 메시지의 무결성 을 확인한다. 서비스제공자는 중개자에게 전기자동차가 정당한 서비스 가입자임을 알려주고 전기자동차와 중개자에게 서비스 제공자 자신의 신원을 확인시키기 위해 아래의 메시지를 중개자로 전송한다.

$$AT_a = H(SID_a \| O_{sa})$$
$$AT_e = H(SID_e \| O_{se})$$

중개자는 서비스 제공자로부터 받은 ATa 와 자신이 가지고 있는 정보로 계산한 값이 같은지 확인한다.

$$AT_a = H(SID_a \| O_a)$$

이면 중개자는 상대방이 정당한 서비스 제공자임을 확인할 수 있다. 서비스 제공자에 대한 인증 작업 후에 중개자는 서비스 제공자가 보내온 전기자동차에 대한 인증 정보를 확인하고 정상적인 가입자일 경우 AT_e 값과 중개자의 비밀값 $g^{ka} \bmod q$ 를 전기자동차로 전송한다. 전기자동차는 자신이 가지고 있는 값들을 이용하여

$$AT_e = H(SID_e \| O_e)$$

를 확인하여 서비스 제공자 자신이 가입한 정당한 서비스업체인 것을 확인한다. 그리고 중개자로부터 받은 비밀값 $g^{ka} \bmod q$ 와 자신의 비밀값 $g^{ke} \bmod q$를 이용하여 전기자동차와 중개자의 공통된 세션키

$$K_{ea} = g^{ka} \bmod q \times g^{ke} \bmod q = g^{kake} \bmod q$$

를 계산한다. 그림 3은 전기자동차, 중개자, 서비스제공자의 인증 메시지 흐름을 보여주고 있다.

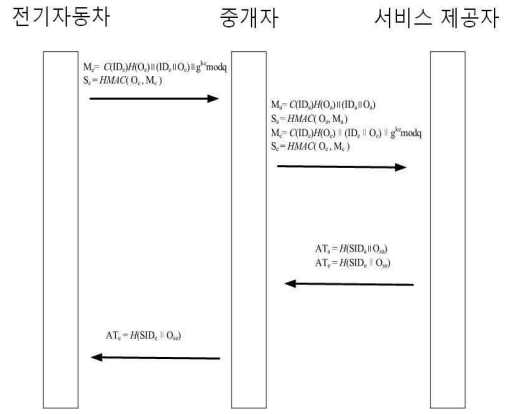

그림3 상호인증 메시지 흐름
Figure 3. Message flow for mutual authentication

전기자동차와 중개자 사이의 채널은 디피헬만 키교환 프로토콜을 사용하여 공유한 세션키 Kea 로 대칭키 암호알고리즘을 이용하여 암호화한다. 인증후의 통신과정에서는 전기자동차는 식별자로 H(IDe ‖ Oe)를 서비스 제공자는 H(SIDe ‖ Ose)를 사용한다. 중개자도 H(IDa ‖ Oa)를 식별자로 사용한다.

2) 충방전 서비스

스마트그리드 관리자는 현재 전력수요량을 기반으로 전기자동차에 전력을 공급할 것인지 혹은 전기자동차의 전력을 매입하여 사용할 것인지를 판단한다. 이를 기반으로 전력판매가격과 전력매입가격을 서비스제공자와 중개기를 통하여 전기자동차에게 알려준다. 이를 바탕으로 전기자동차 사용자는 자신의 식별자 정보(user ID) , 전력판매 혹은 구입여부 , 배터리 정보(state of charge)등의 정보를 암호화된 무선 채널을 통해 중개자로 보내고 중개자는 이를 스마트그리드 관리자와 서비스제공자로 보내면 서비스 제공자는 충방전 서비스를 시작한다. 전기자동차 사용자는 서비스 제공자에 미리 결제정보를 등록하였기 때문에 따로 신용카드나 은행계좌정보를 입력하지 않고 요금의 지불은 서비스내역에 따라 스마트그리드 관리자와 서비스제공자 사이에서 이루어진다.

III. 시스템 보안 및 개인정보보호 분석

전기자동차와 서비스 제공자의 통신망 중 가장 보안에 취약한 부분은 전기자동차와 중개기 사이의 무선망으로 이 채널은 전기자동차와 충방전 서비스제공자와의 상호 인증후 공유된 세션키를 사용하여 암호화 하여 통신을 수행한다. 충방전 기반시설 즉 중개기, 스마트그리드 관리자, 서비스 제공자 사이의 통신은 유선의 전용 채널을 사용하여 높은 보안성을 가진다.

1. 상호 인증

상호 인증은 전기자동차와 충방전 서비스 기반시설 그리고 서비스 기반시설중 중개자와 서비스 제공자간에 이루어 진다. 미리 등록된 사용자 ID, 서비스ID 그리고 OTP 발생기를 이용하여 사용자와 중개자는 자신의 ID와 일회용 비밀값을 해쉬하여 서비스 제공자에게 보내고 서비스 제공자는 자신의 데이터 베이스에 저장된 상대방의 ID와 일회용 비밀값을 이용해 해쉬 값을 계산하고 이 값을 비교하여 상대방이 정당한 서비스 사용자나 중개자인 것을 확인한다. 서비스 제공자는 자신의 서비스ID와 일회용 비밀값을 해쉬하여 전기자동차와 중개자에게 보내고 이들도 서비스 제공자와 같은 절차를 거쳐서 상대방이 자신이 가입한 서비스제공자임을 확인한다. 이러한 과정을 통해 서비스 제공자, 중개기 그리고 전기자동차 사용자는 서로 상호 인증을 수행한다. 또한 인증 과정에서 해쉬된 메시지 인증 코드를 사용하기 때문에 전송된 메시지의 무결성 또한 확인할 수 있다.

2. 보안성 분석

충방전 서비스 기반시설의 통신 즉 중개자, 서비스 제공자, 스마트그리드 관리자간의 통신은 기존의 인터넷망이나 LTE 망을 통하여 연결 할 수 있고 인증후의 전기자동차와 중개자의 무선 채널도 암호화 되어 통신을 수행 때문에 외부 공격에 대해 강한편이다. 충방전 시스템의 통신망중 가장 취약한 부분은 전기자동차와 중개자 사이의 무선통신 채널로 특히 인증 작업전의 암호화 되지 않은 채널은 아래의 여러 형태의 공격에 노출되어 있다.

- 중간자공격 (Man In The Middle Attack)

전기자동차와 중개자 사이에서 전기자동차에 대해서는 중개자로 중개자에 대해서는 전기자동차로 행세

하는 공격으로 비밀키와 같은 정보를 알아내고 서로간의 메시지를 변조할수 있다. 중간자 공격은 서로에 대한 상호 인증이 수행되지 않아서 발생하며 제안한 시스템에서는 각자의 식별자와 OTP를 이용하여 인증을 수행하여 공격자가 상대방인 것처럼 속일수가 없다. 즉 공격자는 전기자동차가 중개자에 보내는 메시지

$$M_e = C(ID_e)H(O_e) \| H(ID_e \| O_e) \| g^{ke} \bmod q$$

$$S_e = HMAC(O_e, M_e)$$

를 위조할 수가 없다. 이 메시지를 위조 하기 위해서는 전기자동차 사용자와 서비스 제공자가 가지고 있는 사용자 식별자와 OTP 값을 알아야 한다. 사전에 이 정보를 미리 획득하지 않고서는 위조가 거의 불가능하다. 또한 해쉬된 메시지 인증 코드를 사용하기 때문에 메시지의 변조를 쉽게 알아 차릴수 있다.

- 위장 공격 (Impersonate Attack)

공격자가 시스템의 정상적인 구성원으로 가장하여 하는 공격 방법으로 공격자가 전기자동차의 식별자등의 개인정보를 취득하면 정상적인 사용자인 것처럼 서비스망에 접속하여 충방전 서비스를 받을 수 있다. 제안된 시스템에서는 혹 공격자가 사용자 식별자를 알아내더라도 OTP와 함께 해쉬하여 서비스 제공자에게 보내기 때문에 공격자는 OTP값을 알아내기 전에는 정상적인 사용자로 위장할 수가 없다. 공격자가 OTP 값을 알아낸다 하더라도 이 값은 일정 시간후에 바뀌기 때문에 지속적으로 사용 할 수가 없다.

- 재전송 공격 (Replay Attack)

정상적으로 잘 실행된 메시지를 저장하였다가 정상적인 현재 메시지인 것처럼 전송하는 공격으로 인증 정보나 신용카드와 같은 메시지를 저장하였다가 정상적인 사용자인 것처럼 사용 할 수 있다. 제안된 시스템에서는 OTP를 사용하기 때문에 시간이 지나면 저장된 인증 메시지는 사용할 수가 없다. 또 타임스탬프나 고유번호를 부여하는 등의 방법으로도 재전송 공격을 막을수 있다.

- 부인 공격 (Impersonate Attack)

사용자가 서비스를 이용하거나 메시지를 보낸후 자기가 한 것이 아니라고 부인하는 공격으로 정상적인 전기자동차 사용자가 충전 서비스 이용후 서비스 사용을 부인하는 경우에 해당한다. 이 시스템에서는 사용자 식별자 뿐 아니라 서비스 제공자와 공유하는 OTP값을 이용하기 때문에 자신의 행위를 부인하기 어렵다. 이외에도 중개자로 수많은 인증 요청을 하여 시스템의 자원을 모두 사용하여 다른 전기자동차가 서비스를 사용하지 못하도록 하거나 충방전 기반 시설의 서버에 수많은 패킷을 전송하여 시스템이 제대로 작동하지 못하게 하는 서비스 거부공격 (Denial of Service, DoS)이 있다. 개체간의 통신 정보를 엿듣는 스니핑(sniffing) 공격은 전 통신망에 걸쳐 발생할 수 있으며 인증전의 전기자동차와 중개자의 무선 채널을 제외 하고는 모든 통신 채널이 암화화로 보호된다. 제안한 시스템에서는 서비스 거부 공격과 스니핑 공격에 대한 새로운 대책은 제시하지 않으며 이 공격들에 대해서는 일반적인 네트워크에서의 방어법이 사용된다고 가정한다.

3. 개인정보 보호

전기자동차 사용자는 ID와 패스워드, VIN 같은 정보를 서비스 제공자에 제공하여 인증과정을 거치고 여러 민감 정보를 서비스 제공자와 주고받아야 충방전 서비스를 이용할 수 있다. 이러한 개인 정보가 유출될 시에는 공격자는 전기자동차의 주행 패턴이나 행동 반경을 알수 있다. 대표적인 개인 정보로는 사용자 ID, 배터리 정보, 결재정보, 위치 정보 등이 있다[11].

- 사용자 ID

전기자동차 사용자는 사용자 ID를 서비스 사용전 미리 등록하고 인증을 위해 중개자를 거쳐 서비스 제공자에게 C(IDe)H(Oe) , H(IDe ‖ Oe) 값을 전송한다. 인증 후에는 H(IDe ‖ Oe) 값을 사용자 식별자로 사용한다. 중개자는 사용자의 일회용 비밀값 Oe 값을 알수 없기 때문에 접속하는 전기자동차의 IDe를 알수 없다. 공격자가 전기자동차와 중개자간의 패킷 H(IDe ‖ Oe) 값을 알더라도 OTP 값인Oe 가 시간에 따라 변하기 때문에 다음번 패킷에는 다른 식별자 값을 사용한다. 따라서 공격자는 전기자동차와 중개자 사이에 오고가는 정보로는 어떠한 전기자동차인지 알수없다. 이것은 중개자 또한 마찬가지로 접속하는 전기자동차의 정체를 알수 없다. 서비스제공자만이 이 전기 자동차의 사용자 ID정보와 OTP를 공유하기 때문에 전기 자동차의 신분을 알수 있다.

- 위치정보

전기자동차의 위치 정보는 중재자의 위치로 유추할 수 있다. 인증을 위해 중개자는 C(IDa)H(Oa) 와 H(IDa

‖Oa)를 서비스 제공자로 보내고 인증 후에는 H(IDa‖Oa)를 식별자로 사용한다. 공격자가 위 정보를 알아내더라도 OTP값을 알지 못하기 때문에 중개자의 ID는 알수 없으며 인증후의 중개자의 식별자는 OTP값으로 인해 시간마다 변하기 때문에 중개자의 식별자를 인지하기는 매우 어렵다. 따라서 전송되는 메시지만으로는 중개자의 신원을 확인하기는 거의 불가능하며 또한 식별자를 통한 중개자의 위치정보는 서비스제공자만이 알 수 있다.

- 배터리정보

전기자동차의 배터리 정보는 암호화된 무선 채널을 이용하여 서비스 네트워크로 전달되기 때문에 공격에 강한 내성을 가진다. 또한 전기자동차의 식별자가 시간에 따라 변하기 때문에 혹여 공격자가 배터리정보를 알아내더라도 어느 전기자동차의 배터리 정보인지 유추하기 어렵다.

- 결제정보

서비스 이용후 결제 정보는 서비스제공자와 스마트그리드 관리자 사이에서만 교환이 되고 전기자동차와 중개자는 결제 정보를 전혀 전송하지 않는다. 시스템 내부망은 보안에 매우 강한 통신망으로 공격자가 내부 통신망에 침투하여 결제 정보를 얻기는 매우 어렵다. 결제 정보의 유출은 전기자동차와 중개자에게서는 일어나지 않는다.

Ⅳ. 결 론

본고에서는 상호인증 프로토콜을 포함한 전기 자동차의 충/방전 서비스 시스템의 운영방안을 제안하였다. 제안된 시스템은 해쉬 함수와 일회용 비밀값(OTP)를 이용하여 상대방의 신원을 확인하여 공개키 기반의 인증체계보다 시스템의 부하가 낮다. 또한 시간에 따라 변하는 사용자 식별자를 사용하여 공격자가 사용자의 식별자 정보를 알게 되더라도 이정보가 어느 전기자동차의 정보인지 확인하기가 매우 어렵다. 또한 일반적인 서비스제공자의 사용자에 대한 인증뿐 아니라 사용자가 서비스 제공자의 신원을 확인할 수 있는 상호 인증 방식을 사용하여 중간자 공격등의 보안 위협에 대비하였다. 제안한 충/방전 서비스 시스템의 보안성과 개인정보보호에 대한 분석은 이 시스템이 외부 위협에 강한 내성을 가지고 있음을 보여준다.

References

[1] IEA, Global EV Outlook 2018
[2] 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
[3] 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
[4] Wenlin Han, Yang Xiao, "Privacy preservation for V2G networks in smart grid: A survey" Computer Communications, 91-92, pp.17-28,2016
[5] N Saxena, BJ Choi " Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks" IEEE Transactions on Information vol.11 issue7, pp.1438-1452
[6] Binod Vaidya, Dimitrios Makrakis, Hussein T. Mouftah "Multi-domain Public key infrastructure for Vehicle-to-Grid network", Proceedings of the IEEE Military Communications Conference, 2015
[7] H Li, G Dán, K Nahrsted "Proactive key dissemination-based fast authentication for in-motion inductive EV charging " Proceedings of the IEEE ICC, 2015
[8] Zhenyu Yang, Shucheng Yu, Wenjing Lou, Cong Liu " P^2: Privacy-Preserving Communication and Precise Reward Architecture for V2G Networks in Smart Grid" IEEE Transaction On Smart Grid, Vol.2, No.4 ,2011 pp. 697-706
[9] Stallings " Cryptography &Network Security" 5th edition, Prentice Hall
[10] Wikipedia, https://en.wikipedia.org/wiki/One-time_password
[11] Wenlin Han, Yang Xiao, "Privacy preservation for V2G networks in smart grid: A survey" Computer Communications, 91-92, pp.17-28,2016