

A Secure Discharging Protocol for Plug in Electric Vehicle (SDP-V2G) in Smart Grid

Khaled Shuaib^(✉), Juhar Ahmed Abdella, Ezedin Barka, and Farag Sallabi

College of Information Technology, The United Arab Emirates University,
P.O Box 15551 Al-Ain, UAE
K.shuaib@uaeu.ac.ae

Abstract. Penetration of Plug in electric vehicles (PEVs) is expected to rise in the next few years especially in areas with new deployed smart power grid systems. Charging and discharging of PEVs will introduce several challenges related to load stabilization and information security. In this paper, we discuss a secure discharging protocol where users can be protected from possible information security and privacy attacks. The protocol also incorporates required remote authorization and payment transaction mechanisms. Our protocol is developed based on the use of encryption mechanisms and the dual signature approach. Using the security protocol verification tool, Automatic Verification and Analysis of Internet Security Protocols (AVISPA), the security aspects of the proposed protocol are verified. Our approach is robust against misuse of electric vehicles and unfair payment issues as it allows for user-based authentication in addition to the authentication of associated electric vehicles.

Keywords: Smart grid · Plug in electric vehicles · Information security · Protocol · Vehicle to grid

1 Introduction

One of the important components of Smart Grid (SG) systems is the Vehicle-to-Grid (V2G) network. The V2G network describes a network of power systems in which plug-in electric vehicles (PEVs) are connected to the SG as mobile distributed energy resources. V2G systems are capturing the attention of both the electricity providers and end users due to the various advantages gained by their deployment. On one hand, power suppliers benefit from utilizing PEVs to better manage demand response services and ancillary services (e.g. spinning reserves, reactive power support, frequency and voltage regulation) to stabilize the power system. On the other hand, users can get incentives from power providers by providing the aforementioned services. PEVs can store energy by charging their batteries during off-peak hours when the power supply from the grid or renewable energy resources is more than the demand. During peak hours when the energy demand exceeds the energy supply, PEVs can sell power back to the SG by discharging their batteries. The other advantage of V2G systems is that PEVs promote environmental benefits by reducing the CO₂ emissions. V2G networks are based on a SG system that supports a bi-directional flow of electricity and data communication [1].

The dependency of V2G networks on a two-way data communication allows efficient information exchange between different parties and provides a secure, flexible, responsive, and reliable payment system [2]. However, the reliance of V2G networks on two-way data communication gives rise to different kinds of security and privacy problems related to the confidentiality, integrity and availability of the system [3–7]. Some of the potential security attacks in V2G networks include but not limited to eavesdropping, DoS attacks, replay attacks and repudiation attacks. Moreover, the privacy of PEV owners could be violated by involved entities during discharging. This can take place when users' or vehicle based sensitive information such as the real user identity and vehicle identity submitted to the supplier for authentication and billing purposes. Furthermore, PEVs in V2G networks can be misused by adversaries for financial benefits by discharging PEVs of others [8, 9]. Therefore, charging protocols used between the SG and PEVs for charging/discharging should be equipped with end-to-end security and privacy preservation techniques. One of the challenging behaviors of V2G networks is that one-way authentication, where only the power company authenticates the PEV user, is not sufficient. In V2G networks, there is a requirement for mutual authentication. PEV users need to be able to sell power back to suppliers anywhere while getting credited for it by their contracted home suppliers. For this reason, to avoid impersonation attacks, a PEV user needs to be protected against dealing with illegitimate aggregators used as intermediators between PEVs and power suppliers. Protection is needed against any repudiation attacks by charging stations or aggregators. Therefore, any used charging station or aggregator needs to be properly authenticated. On the other hand, users of PEVs need to be authenticated to guarantee that only legitimate users can discharge their PEVs. By doing so, misuse of PEVs and any payment disputes will be avoided when multiple users are allowed to use a single PEV.

While there are several studies conducted on V2G networks [11–15], only few of them discuss PEV discharging protocols [11, 12]. The authors in [11] proposed an anonymous authentication protocol for V2G networks based on group signature and identity based restrictive partially blind signature technique to provide security and user privacy-preserving. The approach allows a charging station/aggregator to authenticate PEVs anonymously and to manage them dynamically. In addition, their system supports aggregation to reduce the communication overhead that may be caused by multiple PEVs communicating with the aggregator simultaneously. A mutual authentication scheme is suggested by [12] to avoid redirection and impersonation attacks that may exist in unilateral authentication. The system also supports anonymous authentication based on pseudonym IDs to protect users' privacy. However, there are some major issues which were not addressed by these two previous approaches. Both of these approaches do not include a payment mechanism and do not support user-based authentication but rely on vehicle-based authentication which may lead to misuse of PEVs and unfair payment issues. Moreover, the approach proposed in [11] does not support mutual authentication. In addition, both approaches achieve anonymous authentication by using methods such as pseudonym IDs and group signature which have their own drawbacks. According to [21], group signature based authentication is not suitable for V2G networks due to the dynamic nature of PEVs which will lead to spatial and temporal uncertainties. The pitfall of Pseudonym ID based authentication is that its management is difficult for large

number of vehicles as it usually requires frequent replacement of Pseudonym IDs [11]. In this paper, we propose a secure and privacy-aware PEV discharging protocol. The protocol supports anonymous mutual authentication and an anonymous payment mechanism achieved through the utilization of encryption mechanisms and a dual signature (DS) approach as used by the well-known Secure Electronic Transaction (SET) protocol [25]. Using the dual signature, we achieve anonymity without using complex techniques such as group based signature, Pseudonym ID or blind signature. Moreover, our approach is robust against misuse of electric vehicles and unfair payment problems as it allows for user-based authentication.

The remainder of this paper is organized as follows: We introduce the V2G discharging architecture in Sect. 2. Section 3 describes the proposed discharging protocol. Security analysis of the proposed protocol is presented in Sect. 4. Section 5 concludes the paper.

2 V2G Discharging Architecture

In this section, we describe the architecture of V2G networks. Figure 1 depicts a V2G architecture that shows the various entities involved in the discharging process and their interconnections. There are seven entities involved in the discharging process. A Service Provider (SP) is a utility company that provides electricity to end users who have established contracts with it. Aggregators (AGR) do not exist in the traditional power system architecture. Aggregators come into existence because of some new requirements imposed on the SG system as a result of integrating PEVs. When PEV users want to sell power back to the grid operators by discharging their batteries, the power discharged from a single PEV is not sufficient enough to provide ancillary service to the grid as PEVs have a limited battery capacity ranges from 10 kw to 40 kw. A certain minimum amount of power is required to become eligible for providing ancillary service. For example, the minimum amount of power that is required to provide ancillary service in the UK is 3 MW [4]. Hence, a new entity called Aggregator is introduced to act as an intermediary between PEVs and grid operators to accumulate the power discharged from distributed electric vehicle batteries into a single load or source and provide it to the power grid system [16–19]. Moreover, since PEV users visit charging stations randomly, uncontrolled PEV charging can cause unpredicted overload to the distribution system [20]. Therefore, Aggregators are also responsible for stabilizing, optimizing and controlling the charging process to protect the reliability of the power grid system. Aggregators need to frequently communicate with Distribution System Operators (DSO) to fulfill their objective. DSOs in turn have to communicate with the Transmission System Operators (TSO) on a regular basis to exchange supply/demand information. Aggregators usually sign contracts with suppliers and provide charging/discharging services for end customers. As can be seen from Fig. 1, PEV users can charge at different charging/discharging locations such as home charging point, offices or public charging stations (CS). A given charging location consists of a Smart Meter (SM) and one or more Electric Vehicle Supply Equipment (EVSEs). A SM is an electronic device that continuously records electric energy consumption and sends it to the supplier at some pre-defined

time intervals. The EVSE is an intelligent device that is used as a charging point connecting the PEV to the smart grid system. Charging locations could be connected to an aggregator that is located in one of the three locations: An aggregator situated in the user's home area referred to as Home Aggregator (HAG), outside the user's home area but inside its supplier network called Visiting Aggregator (VAG) and outside the user's supplier network known as External Aggregator (EAG). In the second case, the user is roaming but internally. This scenario is referred to as Internal Roaming Charging (IRC). The roaming in the third case is called External Roaming Charging (ERC) as the user is roaming in an external supplier network.

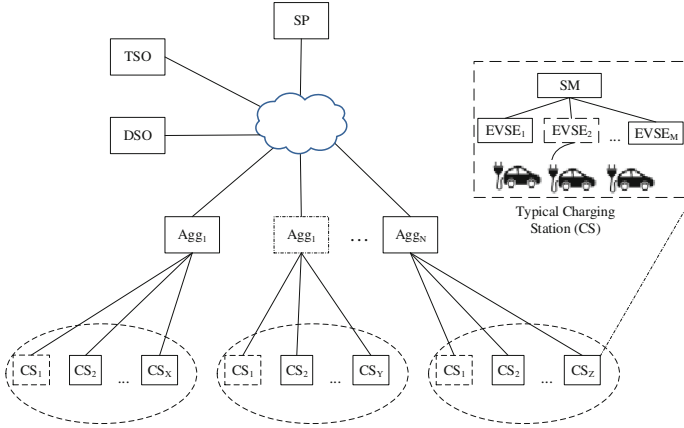


Fig. 1. V2G discharging architecture.

The discharging architecture and protocol presented in this paper supports only the first two cases. The ERC case will be incorporated as part of future work due to page limitation. Communications in a V2G architecture is based on real time communication between the various entities and can take place over different kinds of communication networks [24]. In our architecture, we assume that the PEV and EVSE are connected via Power Line Communication (PLC) and hence the communications between them is secure with no need for additional security configuration. EVSE and SM can be connected using wireless communication technologies such as ZigBee, Wi-Fi and or Wired technologies such as Ethernet. All other communications are assumed to be done through long haul wireless/wired networks such as 4G/LTE or fiber optics.

The V2G architecture demands a one-time system initialization in order to exchange information between system entities. Suppliers need to first obtain certificates from a Certificate Authority (CA) before they can issue certificates for users, AGRs, SMs and EVSEs under their territory. User registration involves generating a unique user ID (U_{ID}) for the user, issuing a smart card (SC) and registering the electric vehicles that the user is allowed to charge/discharge. The smart card provided to the user contains the public/private key pairs of the user, the U_{ID} and the public key of the supplier. The private key of the user will be used by the SC to sign charging/discharging messages on behalf of the user and it is stored encrypted using a PIN number known only to the user. The PIN

number is set by the user during the registration phase with the supplier. PEVs are identified by a unique Vehicle ID (V_{ID}) that is provided by the manufacturer during production. Suppliers register PEVs using this ID. We assume that the V_{ID} is also embedded into the PEV's firmware so that it can be used by the SC during charging. System initialization also includes installing the public key of the SM on the EVSE and vice versa. Moreover, the public key of the AGR is also installed on the SM. Aggregators establish an agreement with suppliers to provide charging/discharging service to end users. During the contract agreement, aggregators obtain the needed certificates from suppliers. Aggregators also get the list of public keys of smart meters in the area they are serving.

Suppliers hold a table of access control list (ACL) that associates users, PEVs and permissions to avoid misuse of PEVs and promote fair payment between multiple users of a single PEV. Let U and V represent the set of all users and PEVs registered by the supplier respectively such that $U = \{U_1, U_2, \dots, U_n\}$ and $V = \{V_1, V_2, \dots, V_m\}$. There are two kinds of permissions associated with PEVs, charging and discharging. Let P represents the set containing these two permissions i.e. $P = \{C, D\}$ where C represents charging and D discharging. Therefore, the elements of an ACL can be represented as: $ACL_i = \{U_j, V_k, P_l\}$ where $U_j \in U$, $V_k \in V$, $P_l \in P$ and ACL_i is the i^{th} element of ACL. For example, the set $\{U_1, V_3, C\}$ indicates that user U_1 is allowed to charge vehicle V_1 while $\{U_2, V_4, D\}$ shows that user U_2 is allowed to discharge vehicle V_4 .

3 Discharging Protocol

In this section we discuss the proposed discharging protocol. The protocol consists of three steps: discharging request, mutual authentication and payment capture. The following specific scenario will be used to explain the protocol: User U_1 who is driving vehicle V_1 visits a certain charging point to discharge his PEV's battery. We assume that various information related to charging/discharging is available on a display screen attached to the EVSE to help the user decide on whether to be served or not. The information displayed to the user on the screen includes: the available power type (Level1, Level2, Level3...), charging rate (CR), discharging rate (DR), maximum available amount of energy etc. CR and DR are the electricity price over some time period as it might change based on the dynamics in supply and demand. The CR and DR are pre-calculated by the AGR and communicated to the EVSE on a regular basis. If user U_1 decides to discharge his PEV battery selling back power to the grid based on the information available on the display screen, he can start the process by connecting his PEV to the EVSE and inserting his SC into the card reader (CRD). The next three subsections show the details of the steps taken to complete the discharging process securely.

3.1 Discharging Request

- (a) The SC prompts the user for a password/PIN to verify that the user holding the SC is the legitimate user and to invoke the use of the user's private key. If successful, the user will be directed to a screen that allows him to select the type of service he

is interested in (Charging or Discharging) and the amount of power in KW (power to be charged or power to be discharged). For our example, user U_1 selects discharging (D) and the amount of power to be discharged (PD). The user can only select a PD amount that is less than or equal to the maximum available battery power (MABP) of the PEV which is displayed to the user during the selection process. The MABP is calculated by the EVSE using the connection to the PEV. Once completed, a discharging request will be initiated between the user's SC (on behalf of the user) and the EVSE. An initial message (InMess) is sent from the user's SC to the EVSE which can be expressed as: $SC \rightarrow EVSE: = InMess$ where $InMess = D \parallel PD$ where \parallel represents the concatenation operator.

- (b) Upon receiving the initial message, the EVSE prepares an initial response message (InResMess) by concatenating the InMess with a unique transaction ID (TID), DR and the payment, P, the user will be credited for based on the PD and the discharge rate. The actual power discharged and the actual payment the user will receive may be different from PD and P as the user may decide to stop discharging in the middle before the maximum requested power is reached. This is represented as: $EVSE \rightarrow SC: = InResMess$ where $InResMess = D \parallel PD \parallel TID \parallel DR \parallel P$.
- (c) When the SC receives the initial response message, it prepares the discharging request (DReQ) using dual signature. The dual signature is made up of the User Related Information (URI) and Power Related Information (PRI). This is represented as: $DS = E_{KR_{U_1}} [h(h(PRI) \parallel h(URI))]$ where $URI = D \parallel TID \parallel V_1 \parallel U_1 \parallel P$, $PRI = D \parallel TID \parallel PD \parallel DR \parallel P$ and $h(x)$ is the hash of x . The process of generating the dual signature is shown in Fig. 2.

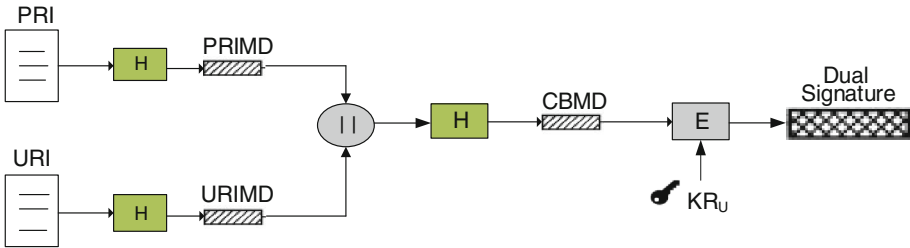


Fig. 2. Dual signature generation

- (d) The SC then prepares the discharging request (DReQ) message based on the generated DS. The DReQ is composed of two messages: a message targeted to the aggregator (AggM) and another one intended for the SP (SpM). The SpM is encrypted using SP's public key so that the AGR is not able to see its content. Hence, DReQ will be expressed as: $DReQ = AggM \parallel SpM \parallel Ts_1$ where $AggM = PRI \parallel DS \parallel h(URI)$, $SpM = E_{KU_{sp}} [URI \parallel DS \parallel h(PRI)]$, and Ts_1 is a time stamp.

The SC sends the DReQ to EVSE. The message is then delivered from EVSE to SM, then from SM to AGR and finally to SP. Starting from EVSE, the message is encrypted using the public key of the receiver and signed by the private key of the sender after

hashing. At the receiver end, the receiver verifies the integrity and source authenticity of the message using the public key of the sender. For example, the DReQ as it travels from EVSE to SM can be represented as: $EVSE \rightarrow SM: = \text{Sig}(EVSE, DReQ) \parallel E_{KU_{SM}}[DReQ]$, $\text{Sig}(X, M)$ is the signature of entity X over message M and is equal to $E_{KR_X}(h(M))$ where $h(M)$ is the hash of M and $E_{KR_X}(h(M))$ is the encryption of $h(M)$ with the private key of entity X . The verification of DReQ at the SM is performed as $\text{Ver}(DReQ, KU_{EVSE})$ where $\text{Ver}(M, KU_Y) \Rightarrow D_{KU_Y}(\text{Sig}(Y, M)) = h(M)$ and reads as the verification of message M using the public key of entity Y .

- (e) Upon receiving the DReQ message from the SM, the AGR saves the AggM for future use (e.g. payment disputes with the SP) and sends the message $SpM \parallel Ts_2$ to the SP. The interaction diagram for the discharging request is shown in Fig. 3.

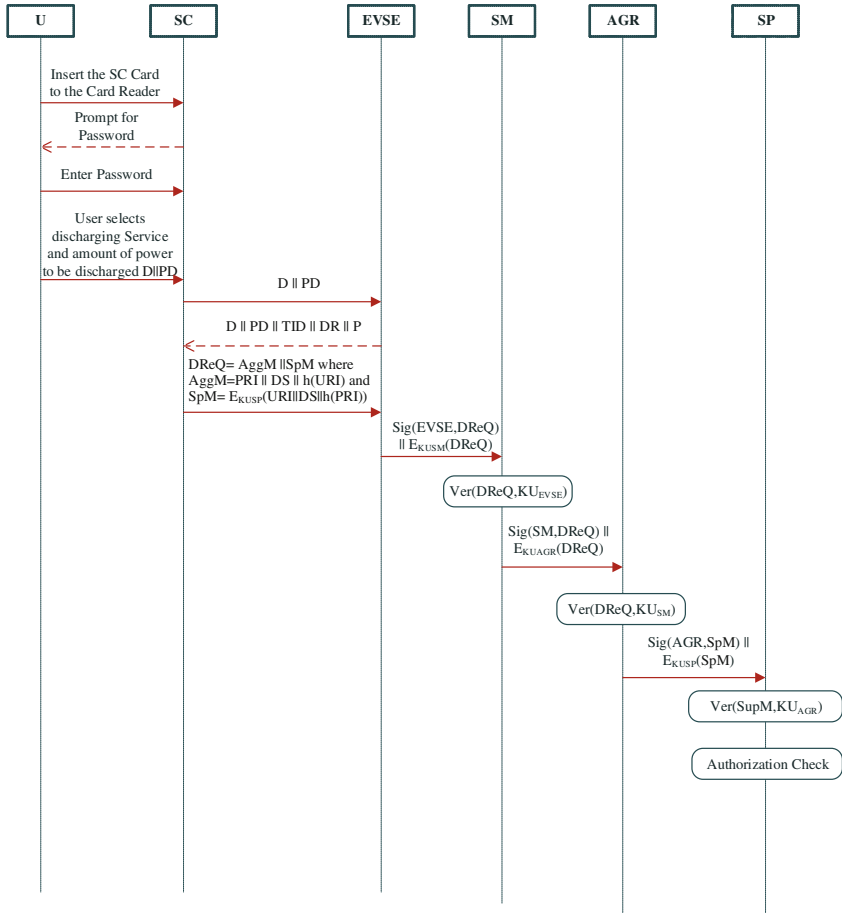


Fig. 3. Interaction diagram for discharging request

3.2 Mutual Authentication

In V2G networks, both the SP and the user should be mutually authenticated to verify that the user is legitimate and proper payments are done. After receiving the $SpM \parallel Ts_2$ from AGR, the SP decrypts it and gets the URI part which includes the user ID (U_1), the vehicle ID (V_1), and the requested service (D). The SP checks if there exists an entry $\{U_1, V_1, D\}$ in the ACL table to authenticate the user and verify his access rights. An authorization response (AuthRes) will be sent back which takes the following format:

$AuthRes = E_{K_{RSP}}[DEC \parallel D \parallel TID]$ where DEC stands for decision and takes two values, Allow or Deny. For example, the $AuthRes = Allow \parallel D \parallel TID$ conveys the meaning “Allow Discharging for the transaction with ID of TID”. The AuthRes is delivered to the user (SC) as shown on the interaction diagram in Fig. 4. When the AuthRes reaches the SC, the SC first verifies that the AuthRes was generated by the expected SP by using the SP’s public key. SC also makes sure that the TID in the AuthRes is the same as the

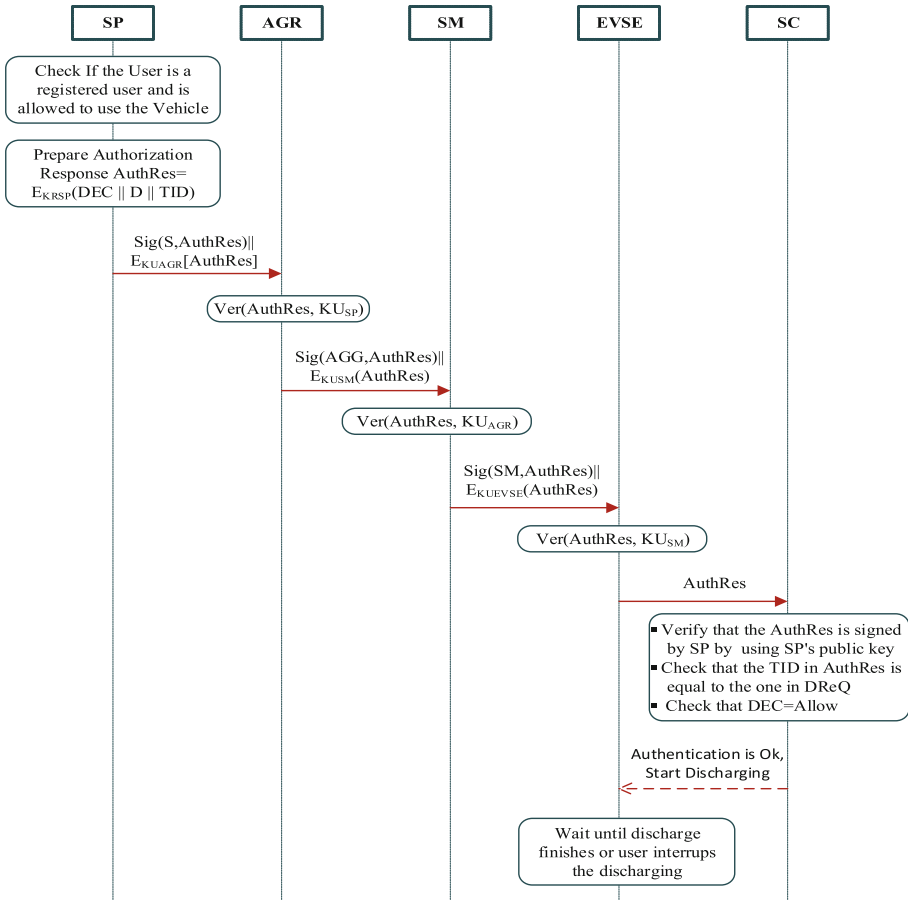


Fig. 4. Interaction diagram for mutual authentication

one sent in the DReQ. The SC then informs the EVSE of the decision (allow or Deny) with respect to the discharging request.

3.3 Payment Capture

The EVSE records the actual power discharged (APD) to the grid by the PEV. The EVSE will stop the discharging process if the PD amount mentioned in the DReQ is reached or the user deliberately interrupts the process. When discharging is completed, the EVSE prepares a power discharging report (PDR) containing the TID, the APD and the actual payment (AP) calculated based on the APD. EVSE then encrypts it with its private key and is sent to the SP as: $PDR = E_{K_{RESE}}[TID||APD||AP]$. The message is sent to the SP in a similar fashion as before (encrypting with the public key of the receiver and signing with private key of the sender). The EVSE also provides the user with a report containing the APD, the TID, and the AP.

4 Security Analysis

One of the security issues associated with PEVs is the lack of access control mechanisms for charging and discharging. The usage of PEVs by multiple drivers, such as in the cases of fleet management or in car renting companies, can lead to the misuse of the vehicles and can result in unfair payments if access to PEVs is not properly controlled/managed. Adversaries may try to charge/discharge the PEV to gain financial benefits taking advantage of the price changes due to supply and demand. For example, a dishonest employee using a company's vehicle will conduct multiple charging/discharging at different charging locations and times at the expense of the PEV owner for personal benefits. Therefore, there is a need to authenticate users who are allowed to use a PEV while controlling their access rights on the PEV i.e. charging/discharging. In addition, messages exchanged between all entities need to be protected against any possible passive or active attacks such as traffic analysis, message content modification, intentional delays and others while not violating the privacy of users and the confidentiality of exchanged information. As was seen in the above description of the proposed protocol, this can be achieved through the utilization of proper encryption techniques, the use of time stamps and hash functions.

4.1 Formal Verification Using AVISPA

One of the important criteria for security protocols is their robustness against various security attacks. In this section, we present the formal verification of the proposed discharging protocol to show that it is safe from several security attacks. The formal verification of our protocol is performed by using the well-known security protocol verification tool known as Automatic Verification and Analysis of Internet Security Protocols (AVISPA) [22]. AVISPA verification works under the assumption that the intruder has full control over the communication channels. To analyze a protocol using

AVISPA, it has to be described in a language called High Level Protocols Specification Language (HLPSL) [23]. AVISPA is composed of four back end servers for verification (OFMC, CL-AtSe, SATMC and TA4SP). Verification of a protocol can be performed by using any one of the four back-end servers. We verified our protocol based on OFMC and CL-AtSe and the test results show that the protocol is safe from attacks such as confidentiality breaches, message modification, nonrepudiation, source authentication, and replay attacks as shown in Table 1.

Table 1. Attacks which were tested for using AVISPA

Attack type	Safe
Message secrecy attacks	✓
Message integrity attacks	✓
Impersonation	✓
Replay attacks	✓
Repudiation	✓

5 Conclusions

Charging and Discharging of PEVs in a smart grid environment where two-way communication is needed implies the need for additional information security measures to be implemented to ensure confidentiality, integrity, availability and accountability. In this paper, we have introduced a secure protocol which can be used to guarantee these security features when PEVs discharge their batteries selling power back to the grid. The protocol was based on the use of the dual signature mechanism and validated using AVISPA to show that it is safe from certain possible information based security attacks.

Acknowledgment. This research was funded by a United Arab Emirates University, research grant, UPAR, number 31T060.

References

1. Chan, A.C.F., Zhou, J.: A secure, intelligent electric vehicle ecosystem for safe integration with the smart grid. *IEEE Trans. Intell. Transp. Syst.* **16**(6), 3367–3376 (2015)
2. Fan, Z., et al.: Smart grid communications: overview of research challenges, solutions, and standardization activities. *IEEE Commun. Surv. Tutorials* **15**(1), 21–38 (2013)
3. Chaudhry, H., Bohn, T.: Security concerns of a plug-in vehicle. In: 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, pp. 1–6 (2012)
4. Mustafa, M.A., Zhang, N., Kalogridis, G., Fan, Z.: Smart electric vehicle charging: security analysis. In: 2013 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC (2013)
5. Carryl, C., Ilyas, M., Mahgoub, I., Rathod, M.: The PEV security challenges to the smart grid: analysis of threats and mitigation strategies. In: 2013 International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, pp. 300–305 (2013)

6. Aloula, F., Al-Alia, A.R., Al-Dalkya, R., Al-Mardinia, M., El-Hajj, W.: Smart grid security: threats, vulnerabilities and solutions. *Int. J. Smart Grid Clean Energy* **1**(1) (2012)
7. Han, W., Xiao, Y.: Privacy preservation for V2G networks in smart grid: a survey. *Comput. Commun.* **91–92**(1), 17–28 (2016)
8. Mustafa, M.A., Zhang, N., Kalogridis, G., Fan, Z.: Roaming electric vehicle charging and billing: An anonymous multi-user protocol. In: *Smart 2014 IEEE International Conference on Grid Communications*, Venice, pp. 939–945 (2014)
9. Shuaib, K., Barka, E., Ahmed Abdella, J., Sallabi, F.: Secure charging and payment protocol (SCPP) for roaming plug-in electric vehicles. In: *Proceeding of the 4th International Conference on Control, Decision and Information Technologies (CoDIT 2017)*, Barcelona, Spain, 5–7 April 2017
10. Liu, H., Ning, H., Zhang, Y., Xiong, Q., Yang, L.T.: Role-dependent privacy preservation for secure V2G networks in the smart grid. *IEEE Trans. Inf. Forensics Secur.* **9**(2), 208–220 (2014)
11. Chen, J., Zhang, Y., Su, W.: An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-Grid (V2G) networks. *China Commun.* **12**(3), 9–19 (2015)
12. Saxena, N., Choi, B.J.: Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks. *IEEE Trans. Inf. Forensics Secur.* **11**(7), 1438–1452 (2016)
13. Liu, H., Ning, H., Zhang, Y., Guizani, M.: Battery status-aware authentication scheme for v2 g networks in smart grid. *IEEE Trans. Smart Grid* **4**(1), 99–110 (2013)
14. He, M., Zhang, K., Shen, X.: PMQC: a privacy-preserving multi-quality charging scheme in v2g network. In: *2014 IEEE (GLOBECOM 2014)*, Austin, USA, pp. 675–680 (2014)
15. Hoang, D.T., Wang, P., Niyato, D., Hossain, E.: Charging and discharging of plug-in electric vehicles (PEVs) in vehicle-to-grid (V2G) systems: a cyber insurance-based model. *IEEE Access* **5**, 732–754 (2017)
16. García-Villalobos, J., Zamora, I., San Martín, J.I., Asensio, F.J., Aperribay, V.: Plug-in electric vehicles in electric distribution networks: a review of smart charging approaches. *Renew. Sustain. Energy Rev.* **38**, 717–731 (2014)
17. San Román, T.G., Momber, I., Abbad, M.R., Miralles, Á.S.: Regulatory framework and business models for charging plug-in electric vehicles: infrastructure, agents, and commercial relationships. *Energy Policy* **39**(10), 6360–6375 (2011)
18. Guille, C., Gross, G.: Design of a conceptual framework for the V2G implementation. In: *2008 IEEE Energy 2030 Conference*, Atlanta, GA (2008)
19. Bessa, R.J., Matos, M.A.: The role of an aggregator agent for EV in the electricity market. In: *The Seventh Mediterranean Conference and Exhibition on Power Generation, Transmission, Distribution and Energy Conversion*, (MedPower 2010). IET, AgiaNapa, Cyprus 2010, pp. 123–131 (2010)
20. Shuaib, K., Sallabi, F., Al Hussien, N., Abdel-Hafez, M.: Simulation of PEV service admission control (PEVSAC) model for smart grid using MATLAB. *SoutheastCon 2016*, Norfolk, VA (2016)
21. Hajj, S., Zargar, M., Yaghmaee, M.: Privacy preserving via group signature in smart grid. http://confbank.um.ac.ir/modules/conf_display/conferences/eiac2013/207_2.pdf. Last accessed 2 Feb 2017
22. AVISPA -automated validation of internet security protocols and applications (2006). <http://www.avispa-project.org/>. Last accessed 23 Jan 2017
23. AVISPA. Deliverable 2.1: The High-Level Protocol Specification Language (2003). <http://www.avispa-project.org/>. Last accessed 23 Jan 2017

24. Shuaib, K., Barka, E., Al Hussien, N., Abdel-Hafez, M., Alahmad, M.: Cognitive radio for smart grid with security considerations. *Computers* **5**(2) (2016)
25. Stalling, W.: *Cryptography and Network Security: Principles and Practice*, 6th edn. Prentice Hall Inc, Upper Saddle River (2014). ISBN:13:978-0133354690

ICT Innovations 2017

Data-Driven Innovation. 9th International Conference,

ICT Innovations 2017, Skopje, Macedonia, September

18-23, 2017, Proceedings

Trajanov, D.; Bakeva, V. (Eds.)

2017, XVII, 286 p. 94 illus., Softcover

ISBN: 978-3-319-67596-1