A note on PUF-Based Robust and Anonymous Authentication and Key Establishment Scheme for V2G Networks

Milad Seddigh[1] and Seyed Hamid Baghestani[2]

[1,2]Cyberspace Research Institute, University of Shahid Beheshti, Iran, Tehran
[1]Milladseddigh7@gmail.com
[2]se.baghestani@mail.sbu.ac.ir

February 17, 2024

Abstract

Vehicle-to-grid (V2G) provides effective charging services, allows bidirectional energy communication between the power grid and electric vehicle (EV), and reduces environmental pollution and energy crises. Recently, Sungjin Yu et al. proposed a PUF-based, robust, and anonymous authentication and key establishment scheme for V2G networks. In this paper, we show that the proposed protocol does not provide user anonymity and is vulnerable to tracing attack. We also found their scheme is vulnerable to ephemeral secret leakage attacks.

Keywords: Vehicle-to-grid, user anonymity, ephemeral

1 Introduction

After the development of “5G, smart grid (SG), and electric vehicle (EV)” technology, the vehicle-to-grid (V2G) is appearing as an attractive new network paradigm that has grasped the attention of scientific and industrial communities and has aroused their interest in using it [TOD17, YPL$^+$20, KO19]. Besides, V2G provides efficient charging services by creating two-way communication along with two-way electricity transmission between the power grid and electric vehicle (EV). But V2G networks are vulnerable to security threats since an attacker can control and eavesdrop on the transmitted messages in an insecure channel at any time [SGCV17, HX16].

Recently, Yu [YP24] has proposed a key agreement scheme for the vehicle-to-grid network, in which there are three entities: the electrical vehicle user (U_i), the utility service provider (USP), the fog server (FS), and the charging station (CS). USP is responsible for the registration of all participants and generates the secret credentials and parameters for all participants. An ordinary server can only process data from one vehicle at a time. For this reason, V2G requires a CS to perform parallel processing. Also, the FS controls and manages the CS and vehicle in real-time. When the vehicles move out of the smart city, the FS sends a message to the CS to connect to another FS. A user also communicates with CS and USP to be authenticated and obtain a session key. Although the scheme is fascinating, we find it flawed since it fails to maintain user anonymity and is vulnerable to tracing attacks. Also, this protocol cannot resist an ephemeral secret leakage attack [YP24].

2 Review of the Scheme

USP first selects a master private key MK_{USP} and comprises the h($\cdot$). After that, USP publishes the h($\cdot$) as public data. In this scheme, before the authentication key establishment (AKE) phase, U_i and CS have to be registered with USP to access the useful V2G services and obtain the credential from USP.

The registration phase includes two parts that are performed via a secure channel: CS and U_i registration phases.

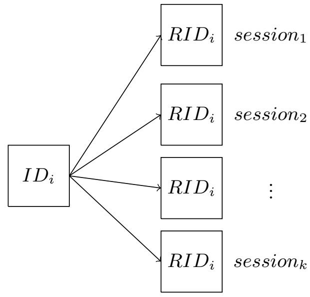

Figure 1: The false anonymity

1. Charging Station Registration Phase: CS generates an identity ID_{CS} and a set of (C_{CS}^x, R_{CS}^x). Later on, CS sends ID_{CS},(C_{CS}^x, R_{CS}^x) to the USP via a secure channel. Then, USP computes $Z_j = h(ID_{CS} \parallel ID_{USP} \parallel MK_{USP} \parallel R_{CS}^x)$ and $c_j = h(ID_{CS} \parallel MK_{USP})$ and sends it to the CS. Ultimately, USP discards Z_j and c_j and keeps $(C_{CS}^x, R_{CS}^x), ID_{CS}$ in the database (DB). CS also stores $(C_{CS}^x, R_{CS}^x), Z_j, c_j$ securely.

2. User Registration Phase: Before AKE phase, U_i registers within USP to access the useful V2G services and obtains the credential from USP.

   First, U_i generates ID_U and PW_i and imprints BIO. Later on, U_i selects a set of (C_U^x, R_U^x) and computes $RID_i = h(ID_i \parallel BIO)$ and $RPW_i = h(PW_i \parallel BIO)$ and then transmits $RID_i, RPW_i, (C_U^x, R_U^x)$ to the USP.

   Then, USP calculates $X_i = h(RID_i \parallel MK_{USP} \parallel R_U^x), Q_i = X_i \oplus h(RID_i \parallel R_U^x) \oplus RPW_i$, and $W_i = h(RID_i \parallel R_U^x \parallel X_i \parallel RPW_i)$. After that, USP keeps Q_i, W_i in the SC and sends the SC to the U_i. Then, USP_i calculates $E_i = X_i \oplus ID_{USP} \oplus MK_{USP}$ and stores $E_i, (C_U^x, R_U^x)$ in the DB [YP24].

After the registration phase, U$_i$ must have a mutual authentication with USP via CS and establish a session key (SK) among U$_i$, CS, and USP. This authentication key establishment (AKE) phase is performed over an insecure channel (Table 1).

3 The Loss of Anonymity and Untraceability:

The goal of anonymity is that an attacker cannot extract the ID of the electrical vehicle user by intercepting messages transmitted in an insecure communication channel, and at a higher level, the attacker may not even be capable of finding any relation between two specific sessions. [YP24] claim that the attacker that eavesdrops on the exchanged messages during the AKE phase is unable to extract the real ID of the electrical vehicle user without knowing the "biometric (BIO), secret credentials (X_i), and PUF secret value R_U^1.

We find the claim unsound and misleading. In fact, an attacker can directly retrieve the pseudo-identity RID by capturing messages transmitted via the insecure channel. Note that the pseudo-identity is sent by the user in the registration phase and is unchanged in various sessions. Thus, the attacker can attribute different sessions created by the user U_i to the pseudo-identity RID (Figure 1). Although the attacker cannot recover ID_i from the equation $RID_i = h(ID_i \parallel BIO)$, the exposure of RID_i cannot cause the anonymity of the user. In other words, identifier ID_i, characteristics of electrical vehicle user, uniquely corresponds to the pseudo-identifier RID_i, and the attacker can recognize the identity of the user by obtaining RID_i. As a result, after obtaining RID, the attacker can relate between the sessions and trace the user. In order to prevent this attack, the identity of the user must be changed and unique for each session.

Table 1: Summary of Authentication and Key Establishment Phase of R2AKE-V2G [YP24]

Electrical Vehicle User (u_i)	Charging Station (CS)	Utility Service Provider (USP)
Inputs ID_u, PW_i and imprints BIO in SC Computes $RID_i = h(ID_i \parallel BIO)$ $RPW_i = h(PW_i \parallel BIO)$ $X_i = Q_i \oplus h(RID_i \parallel R_U^x)$ $W_i^* = h(RID_i \parallel R_U^x \parallel X_i \parallel RPW_i)$ Checks $W_i^* = W_i$ Generates a random nonce R_1 and a timestamp T_1 Selects a pair of $(C_U^1, R_U^1) from (C_U^x, R_U^x)$ Computes $M_1 = (IDU \parallel R_1) \oplus h(X_i \parallel RID_i \parallel R_U^1 \parallel T_1)$ $Auth_U = h(IDU \parallel R_1 \parallel R_U^1 \parallel X_i \parallel T_1)$ $\xrightarrow{Msg_1 = RID_i, M_1, Auth_U, C_U^1, T_1}$	Checks $\lvert T_2 - T_1 \rvert \leq \Delta T_i$ Generates a random nonce R_2 and a timestamp T_2 Selects a pair of $(C_{CS}^1, R_{CS}^1) from (C_{CS}^x, R_{CS}^x)$ Computes $TK = h(Z_j \parallel R_{CS}^1)$ $M_2 = (R_2 \parallel Z_j) \oplus h(ID_{CS} \parallel R_{CS}^x \parallel c_j \parallel TK \parallel T_2)$ $Auth_{CS} = h(ID_{CS} \parallel R_{CS}^1 \parallel R_2 \parallel Z_j \parallel T_2)$ Encrypts $MI_1 = ETK(M_2, Auth_{CS}, RID_i, M_1, Auth_U)$ $\xrightarrow{Msg_2 = MI_1, ID_{CS}, C_{CS}^1, T_2, C_U^1, T_1}$	Verifies $\lvert T_3 - T_2 \rvert \leq \Delta T_i$ *and checks* $ID_{CS}^* = ID_{CS}$ *Retrieves* R_{CS}^1 *on the basis of* C_{CS}^1 $Zj = h(ID_{CS} \parallel ID_{USP} \parallel MK_{USP} \parallel R_{CS}^x)$ $TK = h(Z_j \parallel R_{CS}^1)$ $c_j = h(ID_{CS} \parallel MK_{USP})$ Decrypts $(M_2, Auth_{CS}, RID_i, M_1, Auth_U) = D_{TK}(MI_1)$ Computes $(R_2 \Vert Z_j) = M_2 \oplus h(ID_{CS} \parallel R_{CS}^x \parallel c_j \parallel TK \parallel T_2)$ $Auth_{CS}^* = h(ID_{CS} \oplus R_{CS}^1 \oplus R_2 \oplus Z_j \oplus T_2)$ *Checks* $Auth_{CS}^* = Auth_{CS}$ *Retrieves the* R_U^1 *on the basis of* C_U^1 Computes $X_i = E_i \oplus ID_{USP} \oplus MK_{USP}$ $(ID_U \parallel R_1) = M_1 \oplus h(X_i \parallel RID_i \parallel R_U^1 \parallel T_1)$ $Auth_U^* = h(ID_U \parallel R_{\parallel} R_U^1 \parallel X_i \parallel T_1)$ *Verifies* $Auth_U^* = Auth_U$ *Generates a random nonce* R_3 *and a timestamp* T_3 $M_3 = (R_1 \parallel R_3) \oplus h(T_K \parallel R_{CS}^1 \parallel Z_j \parallel R_2 \parallel ID_{CS})$ $Auth_{USP-CS} = h(ID_{CS} \parallel R_2 \parallel R_3 \parallel R_{CS}^1 \parallel Z_j \parallel T_3)$ $M_4 = (R_2 \parallel R_3) \oplus h(R_U^1 \parallel X_i \parallel R_1 \parallel ID_U)$ $Auth_{USP-U} = h(ID_U \parallel R_1 \parallel R_3 \parallel R_U^1 \parallel X_i \parallel T_3)$ *Encrypts* $MI_2 = E_{(TK \parallel R_2)}(M_3, Auth_{USP-CS}, M_4, Auth_{USP-U})$ $\xleftarrow{Msg_3 = MI_2, T_3}$
	Checks $\lvert T_4 - T_3 \rvert \leq \Delta T_i$ Decrypts $(M_3, Auth_{USP-CS}, M_4, Auth_{USP-U}) = D_{(TK \parallel R_2)}(MI_2)$ Computes $Auth_{USP-CS}^* = h(ID_{CS} \parallel R_2 \parallel R_3 \parallel R_{CS}^1 \parallel Z_j \parallel T_3)$ Verifies $Auth_{USP-CS}^* = Auth_{USP-CS}$ *Generates a timestamp* T_4 Computes $Auth_{CS-U} = h(ID_{CS} \parallel R_1 \parallel R_2 \parallel T_4)$ $\xleftarrow{Msg_4 = ID_{CS}, M_4, Auth_{USP-U}, Auth_{CS-U}, T_3, T_4}$	
Computes $(R_2 \parallel R_3) \oplus h(R_U^1 \parallel X_i \parallel R_1 \parallel ID_U)$ $Auth_{USP-U}^* = h(ID_U \parallel R_1 \parallel R_3 \parallel R_U^1 \parallel X_i \parallel T_3)$ Checks $Auth_{USP-U}^* = Auth_{USP-U}$ Computes $Auth_{CS-U}^* = h(ID_{CS} \parallel R_1 \parallel R_2 \parallel T_4)$ Checks $Auth_{CS-U}^* = Auth_{CS-U}$		
	U_i, CS, *and* USP *establish a common session key* $SK = h(R_1 \parallel R_2 \parallel R_3)$	

4 Ephemeral Secret Leakage Attack

A protocol is resistant to an ephemeral secret leakage attack if all random session numbers are leaked and all of the sensitive session parameters, such as the session key, remain secure. However, the Yu et al. [YP24] scheme cannot resist an ephemeral attack. In the CK model, when all random session numbers such as R_1, R_2, and R_3 are leaked, the session key (SK = h($R_1 \parallel R_2 \parallel R_3$)) remains insecure.

5 Conclusion

In this article, the protocol presented by Sungjin Yu et al. [YP24] was analyzed, and the security analysis of the protocol demonstrated that their scheme is vulnerable to tracing attacks (loss of anonymity) and ephemeral secret leakage attacks. Since it does not meet proper anonymity standards, it is not optimal to implement on vehicle-to-grid networks.

References

[HX16] Wenlin Han and Yang Xiao. Privacy preservation for v2g networks in smart grid: A survey. *Computer Communications*, 91:17–28, 2016.

[KO19] Ismaila Adeniyi Kamil and Sunday Oyinlola Ogundoyin. Lightweight privacy-preserving power injection and communication over vehicular networks and 5g smart grid slice with provable security. *Internet of Things*, 8:100116, 2019.

[SGCV17] Neetesh Saxena, Santiago Grijalva, Victor Chukwuka, and Athanasios V Vasilakos. Network security and privacy challenges in smart vehicle-to-grid. *IEEE Wireless Communications*, 24(4):88–98, 2017.

[TOD17] Ming Tao, Kaoru Ota, and Mianxiong Dong. Foud: Integrating fog and cloud for 5g-enabled v2g networks. *IEEE Network*, 31(2):8–13, 2017.

[YP24] Sungjin Yu and Kisung Park. Puf-based robust and anonymous authentication and key establishment scheme for v2g networks. *IEEE Internet of Things Journal*, 2024.

[YPL+20] SungJin Yu, KiSung Park, JoonYoung Lee, YoungHo Park, YoHan Park, SangWoo Lee, and BoHeung Chung. Privacy-preserving lightweight authentication protocol for demand response management in smart grid environment. *Applied Sciences*, 10(5):1758, 2020.