ISSN: 2688-8645

A Lightweight, Dynamic Anonymous User Identity Authentication and Session Key Negotiation Scheme for V2G Networks

Shaomin Zhang, Zhenzhen Du, Baoyi Wang

North China Electric Power University, Baoding, 071003, China

Abstract

In the Vehicle-to-grid (V2G) network, to achieve user privacy protection during charging and discharging of electric vehicles, anonymous identity authentication of electric vehicle users is required. The existing anonymous identity authentication and session key negotiation schemes cannot effectively resist malicious attacks such as impersonation and offline password guessing, which exposes the user's living habits and even the privacy of the user's location and personal identity. Aiming at the problems, a lightweight, dynamic anonymous user identity authentication and session key negotiation scheme for V2G networks are proposed. The Identity authentication information includes two parts: biological characteristics and dynamic identity information. A fuzzy extractor is used to extract user biological characteristics, and the identity ID and random numbers are hashed to generate pseudonyms in anonymous authentication. Use a third-party key to encrypt the pseudonym and the current timestamp to generate a dynamic anonymous user identity. These two parts complete the user's dynamic anonymous user identity authentication together. The key agreement process is designed. The security of the scheme are proved in theory which can resist malicious attacks such as impersonation and offline password guessing, and can also ensure the security of mutual identity authentication and session key agreement of participants. Examples analysis shows that the scheme has lower computational overhead and higher security, and can be deployed in the actual V2G network environment.

Keywords

Dynamic anonymous identity authentication; Key agreement; Lightweight; Privacy protection; Vehicle-to-grid(V2G).

1. Introduction

V2G technology [1] can realize the two-way interaction and energy exchange between electric vehicles (EVs) and the grid under controlled conditions. According to the demand response strategy, on the premise of satisfying the normal driving demand of the EV, the surplus electric energy can be controlled and fed back to the power grid in two directions [2]. This method can not only play the role of "peak cutting and valley filling" for the power grid, but also bring additional benefits to EV users [3].

As an important application of the distribution end of the smart grid, EVs have exposed their private data information to unauthorized persons when users exchange information with the grid in both directions. For example, user name, grid service provider, account ID, EV identity, EV location, metering and charging data, user permission data, battery status, etc [4]. In the future, electric vehicles may become mainstream models, and charging piles will also appear in large numbers in various types of parking lots. At that time, a large number of EVs will be connected to the grid through charging piles, and their charging or discharging will have a huge

ISSN: 2688-8645

impact on the grid.So the privacy protection of electric vehicles is indispensable when large-scale electric vehicles respond to grid needs in seconds.

Researchers have conducted a lot of research on the privacy leakage of identity authentication in V2G networks, and have proposed different solutions. These solutions can be roughly divided into the following two categories.

The first category belongs to the static anonymous identity authentication scheme, that is, the real identity is protected by generating a pseudonym during the identity authentication process, but the pseudonym will not be updated in time with time, but always uses the same pseudonym. In 2011, Yang et al. [5] proposed a secure connection architecture using blind signature technology to achieve privacy protection. However, this scheme suffers from the key escrow problem inherent in identity-based public key encryption. In 2013, Nicanfar et al. [6] proposed a robust privacy protection authentication scheme that generates pseudonyms through system parameters and is used to protect privacy issues such as the location of EVs. In 2016, Chang and Le [7] proposed a smart card-based flexible authentication protocol for wireless sensor networks. However, in this anonymous authentication scheme, the EV always uses the same pseudonym and is vulnerable to session specific information leakage and offline password guessing attacks [8]. Turkanović et al. [9] designed an efficient authentication scheme, but the scheme uses a pseudonym generated by random numbers unchanged, which is susceptible to offline password guessing attack and impersonationattack, but their scheme does not preserve untraceability.Zhang et al. [10] designed an authentication protocol using only lightweight encryption primitives. This agreement can protect users' privacy, but cannot guarantee users' anonymity. In 2015, Abdallah [11] and others proposed a lightweight security and privacy protection protocol for V2G networks. In this protocol, electric vehicles protect user privacy by generating pseudo-identities. The grid can solve the problem of electric vehicle identity authentication by confirming the confidentiality and integrity of the information exchanged with electric vehicles during charging and discharging.In 2015, Wang et al. [12] proposed a privacy protection scheme using bilinear pairing and restricted partial blind signatures. However, bilinear pairing has higher computational overhead, which increases the operating burden of the V2G network system.In 2018, Chuang et al. [13] divided continuous identity authentication protocols into the user-to-device model and device-to-device model, and proposed a lightweight continuous identity authentication protocol that uses token technology and IoT device dynamics.

The second type belongs to the dynamic identity authentication scheme, that is, the pseudonym is converted into a dynamic identity during the identity authentication process to protect the user's real identity. The dynamic identity will be updated in time with the change of time, and the attacker cannot judge the true identity by the dynamic identity.In 2017, Abdallah and Shen [14] studied the lightweight key agreement and EV identity authentication protocol for V2Gnetworks, and proposed a lightweight and secure V2G privacy protection connection scheme.The scheme uses AKARI-2 (a lightweight pseudo-random number generator) to generate pseudonyms and symmetric keys, and each EV periodically changes its ID to obtain more anonymity.This scheme guarantees the confidentiality and integrity of the information exchanged during the charging process and overcomes the authentication problem of EVs, but the protocol only provides some informal security analysis.Shen et al. [15] proposed a practical and lightweight authentication protocol for V2Gnetworks in the Social Internet of Things.

We propose a lightweight, dynamic anonymous user identity authentication and session key agreement scheme for V2G networks. Our scheme uses real-time or random (ROR) models [16] and Burrows-Abadi-Needham (BAN) logic [17] to verify the security of session keys and mutual authentication, and we also conducted informal Analysis shows that the proposed protocol can resist different types of attacks.

ISSN: 2688-8645

2. Methodology

2.1. Threat Model

In the identity authentication scheme in this paper, the widely accepted "Dolev-Yao (DY) threat model" [18] is used to analyze protocol security. Under the DY model, a malicious attacker can delete, insert, modify, or eavesdrop on messages transmitted over the Internet. Therefore, endpoint entities (IoT sensor nodes and users) cannot usually be trusted. We also consider the CK adversary model [19], which is a more powerful threat model and is regarded as the current de facto standard model when modeling key exchange protocols [20]. Under this model, the attacker can not only use all the functions under the DY model, but also destroy the security information such as session state, private key, and session key. Therefore, the key exchange protocol should ensure that in the case of short-term secret leakage, the impact on the security of the session key established between the V2G network entities in the authenticated key exchange protocol should be minimal [21].

We also follow the hypothetical scheme described by Amin et al. [22]. Legal users registered in the password-based user authentication protocol always use the words in the opponent's available dictionary as the password and identity A. In addition, guessing the secret key and random number in polynomial time is also computationally infeasible because they are high-entropy entities.

2.2. One-way Hash Function

The one-way Hash function[23] is a Hash function that works in one direction. It is easy to calculate the Hash value from the pre-mapped value, but it is difficult to generate a pre-mapped value such that its Hash value is equal to a special value. The design of encrypted one-way hash functions makes them highly sensitive to small disturbances in the input string.The pseudonym generation is used in identity authentication in this topic.

2.3. Fuzzy Extractor

The fuzzy extractor [24] is a technique for extracting data from a user's biometrics into a uniformly distributed random number required by a real cryptosystem. The fuzzy extractor can convert the noisy random source into a uniform random and accurately regenerated character string, which can be applied in the cryptosystem. It is based on the probability generation algorithm and the determination reproduction algorithm (Gen and Rep), respectively.

Gen is a "probabilistic algorithm". After receiving the input biometric information BIO_i, Gen(·) will output a random bit string b_i, which is called the biometric secret key and public reproduction parameter τ_i, such as $Gen(BIO_i) = (\tau_i, b_i)$.Rep is a "deterministic algorithm". With the help of the common reproduction parameter τ_i, Rep (·) is based on the criterion that the Hamming distance between the original biometric information BIO_i and the current biometric information BIO_i' does not exceed the fault tolerance threshold t to restore the original biometric key b_i. Such as $Rep(BIO_i',\tau_i)=b_i$.

Cheon etal. gave an estimate of the fault tolerance threshold [25] as follows. If the Hamming distance between the original biometric BIO_i and the current biometric BIO_i' is HD and the number of digits in the input string is b, then t = HD/b.This topic is used to extract biometrics in identity authentication.

3. V2G System Design

3.1. V2G System Construction

The V2G network contains four entities: (1) EV, (2) charging pile (CP), (3) aggregator (AGT), (4) Grid Control Center. As shown in Figure 1.

ISSN: 2688-8645

The EV sends the EV's identity, battery status, billing measurement data, user authority data, and other information to the charging pile. The AGT collects the data in the charging pile and verifies it, and forwards it to the smart grid after verification. At the same time, it is responsible for downloading the dispatching control instructions of the power grid control center, and the power grid can analyze the existing data and adopt a reasonable price when powering the EV.

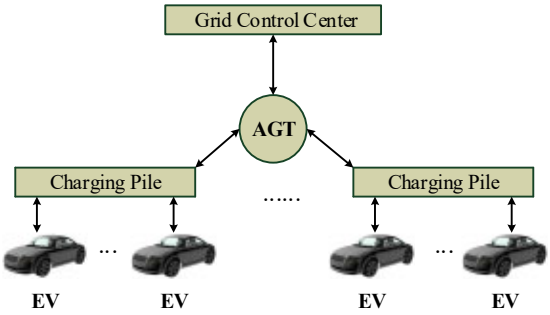

Figure 1. V2G network structure

3.2. V2G System Model

The charging pile is just a link between EV and AGT. The design can ignore the charging pile to simplify the system model. Reference [26] proposes the following system model. Our system model is mainly composed of four entities: (1) Vehicle owner (EVO), (2) EV, (3) Aggregator (AGT), (4) Trusted third party (TTP), as shown in Figure 2.

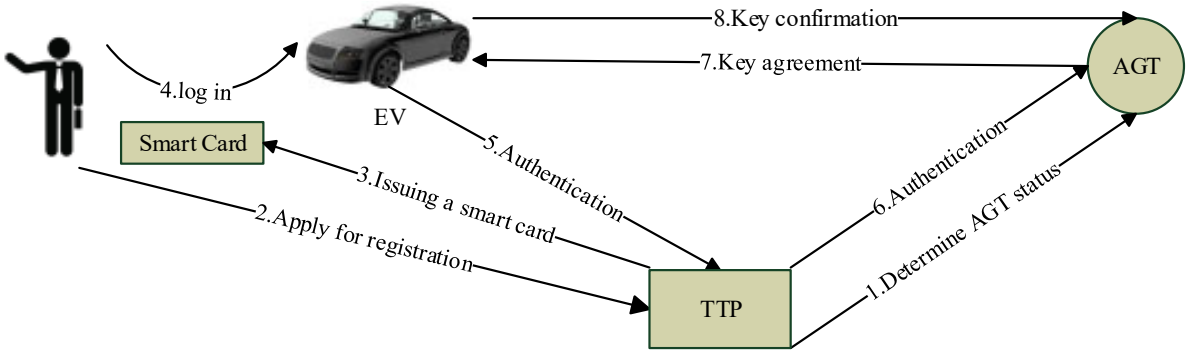

Figure 2. V2G system model

4. Design of User Identity Authentication and Session Key Agreement

The author of this paper studied the privacy-protected identity authentication and key agreement protocol in [15] and found that the protocol scheme only uses one-way hash function and bitwise exclusive-OR(XOR) operation. However, [27] pointed out that the protocol in [15] cannot withstand impersonation, privileged-insider, and offline password guessing attacks, and cannot guarantee secure mutual identity authentication, session key security, and perfect forward secrecy. In view of the above problems, this paper improves the literature [15]. By using the system model in Section 3.2, it provides a lightweight anonymous user authentication scheme that can withstand malicious attacks such as impersonation and offline password guessing for V2G networks.

To ensure resilience to replay attacks, current timestamps are utilized. It is assumed that the clocks of all involved entities are synchronized. This is a typical assumption (for example, the scheme proposed in [7] [28]). The protocol includes five phases: (1) EV user registration stage (2) EV user login stage (3) anonymous user identity authentication (4) session key negotiation process (5) session key confirmation and biometric update.

ISSN: 2688-8645

4.1. User Identity Authentication Design

The dynamic anonymous user registration process is shown in Figure 3, through the hashing and concatenation operation, the identity identifier and random number are generated pseudonyms, and the trusted third-party key LTS is used to encrypt the pseudonym and the current timestamp to generate the dynamic identity of the user.EVOi must register its EV on TTP before it can access V2G services. In this solution, TTP is stateless for registered users.

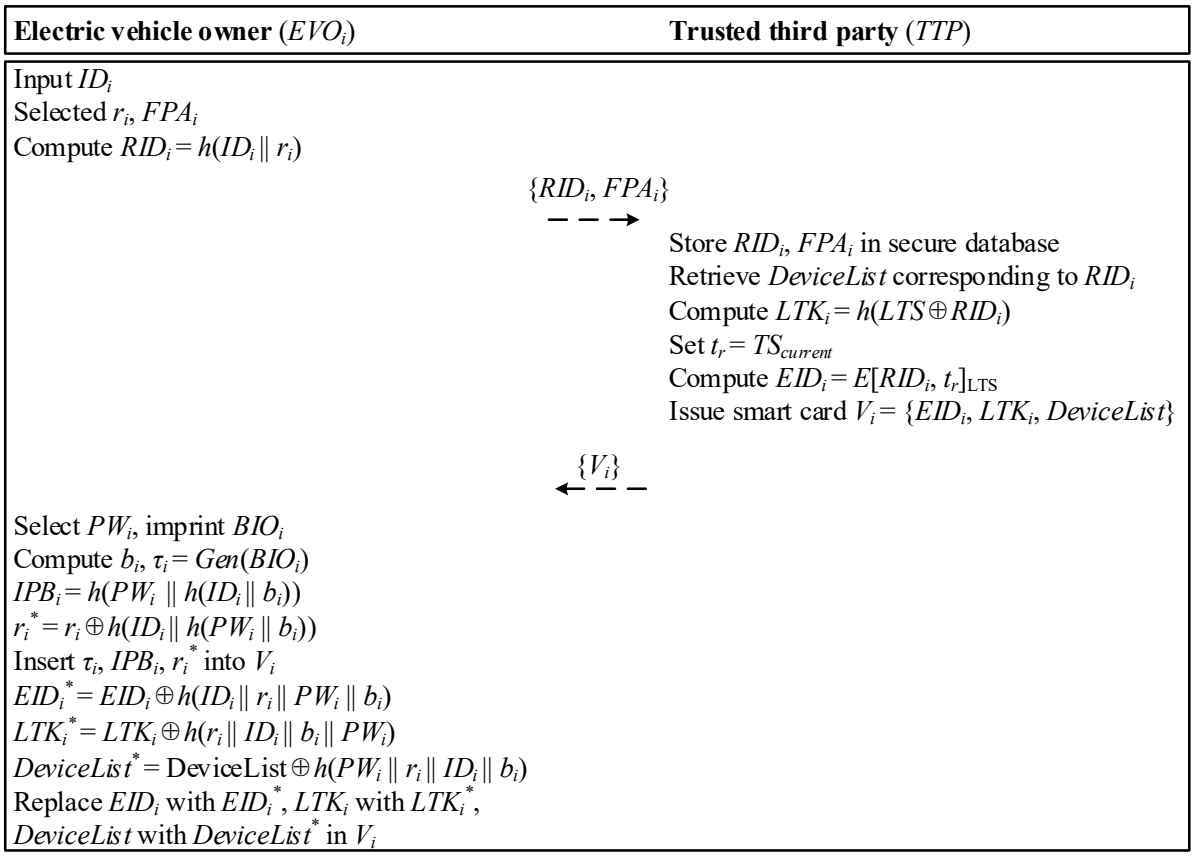

Figure 3. Dynamic anonymous user registration process

The registered EVOi can use the smart card and biometric technology issued by TTP to access the V2G service. The login process is shown in Figure 4.

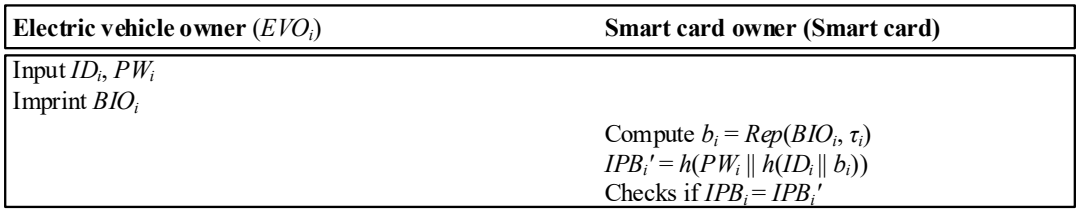

Figure 4. Anonymous user login process

The identity authentication process is shown in Figure 5.

ISSN: 2688-8645

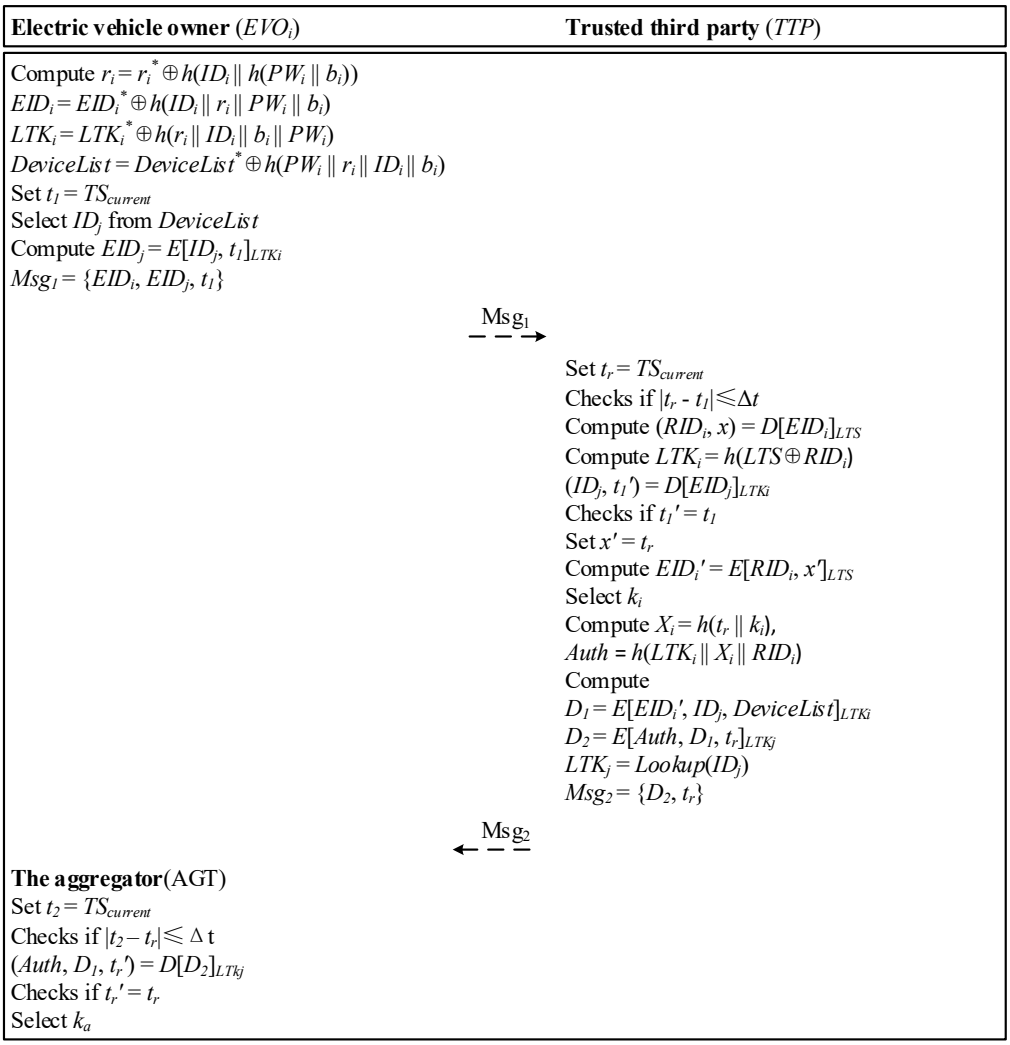

Figure 5. Identity authentication process

4.2. Session Key Agreement Design

The key agreement process is shown in Figure 6. Biometrics will be updated at this stage to protect user privacy and resist various attacks.

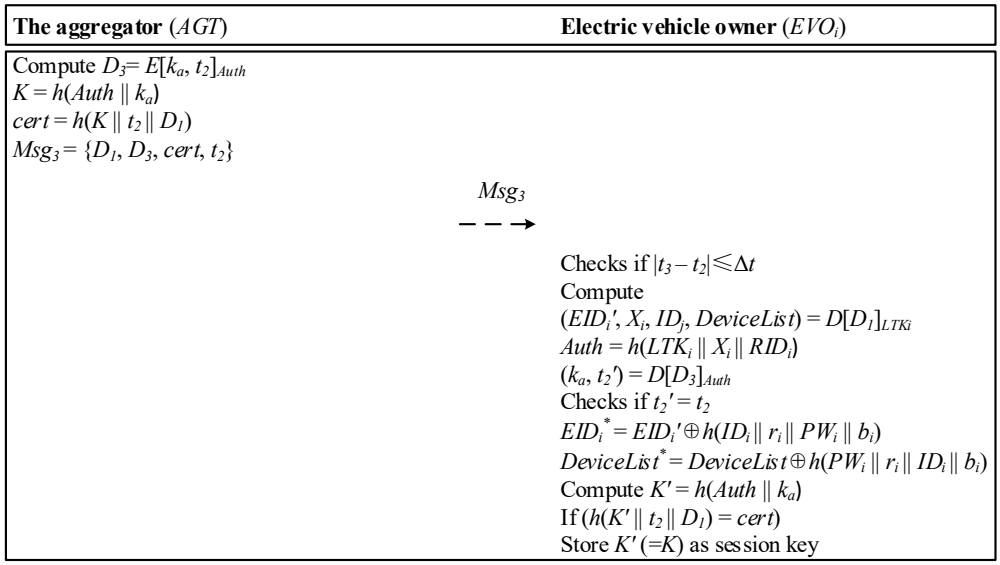

Figure 6. Session key negotiation process

ISSN: 2688-8645

5. Security Analysis

5.1. ROR Model-based Formal Security Analysis

In this section, we evaluate the security robustness using both formal and informal security analysis in this section. First, we prove that the proposed scheme provides session key security under the popular ROR model [16] and mutual authentication using BAN logic proof [17]. In addition, the informal (non-mathematical) security analysis also reveals that the proposed protocol is secure against other various attacks.

ROR model: Using the ROR model, we prove that the proposed protocol satisfies the "session key security (SK-security)". The main participants involved in the process of protocol registration, login, authentication, and key agreement are: user EVO_i, trusted third party TTP, and aggregator AGT. In the proposed protocol, EVO_i, TTP or AGT is considered as an instance (Pt). Because TTP is credible, cannot make a query of TTP damage. All communicating entities including can access a collision resistant hash function h(·). h(·) is modeled as a random oracle, say Hash.

Security Proof: "the size of password dictionary is generally much constrained in the sense that the users will not use the whole space of passwords, but rather a small space of the allowed characters space" [29], Zipf's law [30] is used for formal security analysis to prove the session key security of the proposed protocol.

Theorem 1: If Adv_A^{AKM} is the advantage function of adversary in breaking the SK-security of the proposed authentication key management (AKM) protocol, then q_h, q_s and |Hash| are "the number of Hash queries, the number of queries sent, the scope space of the hash function", l is the number of digits present in the EVO_i biometric key b_i, C' and s' represent Zipf parameters [29], we have

$$Adv_A^{AKM} \le \frac{q_h^2}{|Hash|} + 2max\left\{C' \cdot q_s^{s'}, \frac{q_s}{2^l}\right\}$$

Proof 1: We follow a similar proof of this theorem given in [29]. We need to define a sequence of four games, namely G_j(j=0,1,2,3). An event is defined in which " $\mathcal{A}$ can correctly guess the random bit *c* in the game G_j", and its success probability is defined by $Succ_A^{G_j}$. In addition, " 's advantage in winning the game G_j" is defined by $Adv_{A,G_j}^{AKM} = P_r[Succ_A^{G_j}]$.

Game G_0: This is the initial game, the actual attack performed by $\mathcal{A}$ against the protocol we proposed in the ROR model. Since bit c is randomly selected at the beginning of G_0, we get:

$$Adv_A^{AKM} = |2Adv_{A,G_0}^{AKM} - 1| \quad (1)$$

Game G_1: Corresponding to the eavesdropping attack performed by , use execute query [16], and intercept all communication messages Msg_1={EID_i, EID_j,t_1}, Msg_2={D_2,t_r} during the authentication phase of the scheme. After the game is over, can perform Reveal and Test queries to verify whether the session key $K=h(Auth||k_a)$ is a real session key or a random session key. Among them, $Auth= h(LTK_i||X_i||RID_i)$, $X_i= h(t_r||k_i)$, LTK_i, RID_i and k_i cannot be obtained by eavesdropping on the messages Msg_1 and Msg_2. Therefore, the winning probability of the game G_1 does not increase. Since the games G_0 and G_1 areindistinguishable, we have:

$$Adv_{A,G_1}^{AKM} = Adv_{A,G_0}^{AKM} \quad (2)$$

ISSN: 2688-8645

Game G_2: Compared with game G_1, this game adds a simulation of hash query and models it as an "active attack". In the message Msg_1, RID_i and RID_j are protected by $h(\cdot)$; in the message Msg_2, Auth is protected by $h(\cdot)$. Due to the collision resistance of $h(\cdot)$, deriving ID_i and ID_j from intercepted EID_i and EID_j, and deriving LTK_i and X_i from intercepted D_2 are not computationally feasible. It is worth noting that in the proposed scheme, all messages Msg_1, Msg_2, etc. are constructed in such a manner that all are dynamic in nature andno hash collision occurs. In addition to the simulation of the hash query contained in game G_2, games G_1 and G_2 are difficult to distinguish, so we have:

$$| Adv_{A,G_1}^{AKM} - Adv_{A,G_2}^{AKM} | \leq \frac{q_h^2}{2 | Hash |} \tag{3}$$

Game G_3: Simulated to execute a game that damages the smart card V_i and the aggregator AGT. Therefore, $\mathcal{A}$ will have credentials $\{EID_i^*, LTK_i^*, IPB_i^*, DeviceList^*, r_i^*, \tau_i\}$ and $\{ID_j, LTK_j\}$. cannot obtain the unknown numbers ID_i, PW_i and b_i, it becomes a 'computationally difficult problem for to guess password PW_i of EVO_i correctly'. The probability that opponent guesses the 1-bit biometric key bi is about $1/2^l$ [31]. It is worth noting that when there is no password/biometric guessing attack, the games G_2 and G_3 are the same. Therefore, using the Zipf password law [30], we have the following result:

$$| Adv_{A,G_2}^{AKM} - Adv_{A,G_3}^{AKM} | \leq max\left\{ C' \cdot q_s^{s'}, \frac{q_s}{2^l} \right\} \tag{4}$$

As all games are executed, after the test query, only the guess bit c remains to win the game. So follow:

$$Adv_{A,G_3}^{AKM} = \frac{1}{2} \tag{5}$$

From equations (1), (2), (5), we can get:

$$\frac{1}{2} Adv_A^{AKM} = | Adv_{A,G_0}^{AKM} - \frac{1}{2} | = | Adv_{A,G_1}^{AKM} - \frac{1}{2} | = | Adv_{A,G_1}^{AKM} - Adv_{A,G_3}^{AKM} | \tag{6}$$

From equations (3), (4), (6), we can get:

$$\begin{aligned} &\frac{1}{2} Adv_A^{AKM} = | Adv_{A,G_1}^{AKM} - Adv_{A,G_3}^{AKM} | \\ &= | Adv_{A,G_1}^{AKM} - Adv_{A,G_2}^{AKM} + Adv_{A,G_2}^{AKM} - Adv_{A,G_3}^{AKM} | \\ &\leq | Adv_{A,G_1}^{AKM} - Adv_{A,G_2}^{AKM} | + | Adv_{A,G_2}^{AKM} - Adv_{A,G_3}^{AKM} | \\ &\leq \frac{q_h^2}{2|Hash|} + max\left\{ C' \cdot q_s^{s'}, \frac{q_s}{2^l} \right\} \end{aligned} \tag{7}$$

Multiply both sides of (7) by 2, so the following result:

$$Adv_A^{AKM} \leq \frac{q_h^2}{| Hash |} + 2max\left\{ C' \cdot q_s^{s'}, \frac{q_s}{2^l} \right\}$$

ISSN: 2688-8645

5.2. Mutual Authentication Through BAN Logic

We implement widely recognized BAN logic [17] to verify the safe mutual authentication of the proposed protocol between EV_i and AGT_j. Following the meaning of the logical symbols in [17], we have:

From the fact that K = h(Auth ||k_a), we get the following results:

$$EV_i| \equiv EV_i \xleftrightarrow{K} AGT_j \quad \text{(Goal G1)}$$

Using the fact that K=h(Auth ||ka), we have:

$$AGT_j| \equiv EV_i \xleftrightarrow{K} AGT_j \quad \text{(Goal G1)}$$

Therefore, the protocol proposed by the targets G_1 and G_2 can ensure the safe mutual authentication between EV_i and AGT_j.

6. Results and Discussion

6.1. Functional Comparison

In this paper, one-way hash operation is used for calculation, which occupies less computing resources and has a faster calculation speed. Symmetric encryption has lower computational overhead in the process of encryption and decryption. This section compares with the features [12], [14], [15], and [27] in terms of functional characteristics and calculation costs.

Table 1. Comparison of functions and features

	[12]	[14]	[15]	[27]	Our
Impersonation Attack	√	√	×	√	√
Replay Attack	√	√	√	√	√
Man-in-the-middle attack	√	√	×	√	√
Safe mutual authentication	√	√	×	√	√
Offline password guessing Attack	—	—	×	√	√
Ephemeral Secret Leakage	√	×	×	√	√
ROR model security analysis	×	×	×	√	√
AGT simulated attack	×	×	×	×	√

As shown in Table 1, we compared the proposed protocol with the protocol [12], [14], [15], and [27] functional characteristics, and found that the protocol [12], [14], [15], and [27] cannot guarantee secure mutual authentication and prevent some common attacks.

By improving the authentication and key agreement algorithm in [15], the protocol proposed in this paper only uses symmetric encryption, one-way hash function, and bitwise exclusive-OR(XOR) operation to achieve the legal identity of bidirectional authentication participants. It effectively defends against various common malicious attacks and provides higher security and more functional features.

Compared with the other four protocol schemes, the protocol proposed in this paper does not need to store specific user information on the gateway node, optimizes the steps of identity authentication and key agreement, and reduces the space for storing information and complex operations.

ISSN: 2688-8645

6.2. Computational Costs Comparison

As shown in Table 2, the calculation costs of the client (user) and server (AGT) during the execution of the relevant protocol are listed. Based on the experimental results of [32] and [33], the time required to perform T_h (one-way hash function) is approximately 0.0005s, and the time required to perform T_m (modular exponentiation) is approximately 0.063075s. The time required to perform T_{ecc} (elliptic curve point multiplication operation) is approximately 0.072311s, and the time required to perform T_{fe} (fuzzy extractor function) is approximately 0.063075s. The bitwise exclusive-OR(XOR) operation is not included in this analysis because it is different from other operations (T_m, T_{ecc}, T_{fe} and T_h) are negligible compared.

Table 2. Calculation cost of each agreement

Program	Client	Server	Total time
[12]	$4T_{ecc}+3T_m$	$2T_{ecc}+1T_m$	$6T_{ecc}+4T_m\approx0.686166s$
[14]	Algebraic operation	Algebraic operation	≈0.01518s
[15]	$6T_h$	$5T_h$	$11T_h\approx0.0055s$
[27]	$T_{fe}+11T_h$	$5T_h$	$T_{fe}+16T_h\approx0.071075s$
Our	$T_{fe}+9T_h$	$2T_h$	$T_{fe}+11T_h\approx0.068575s$

It can be observed that the scheme proposed in this paper not only has less total computational cost than the protocols in [12] and [27], but also realizes the protection of user privacy in less time and has extremely high security. Protocol [14] cannot prevent ESL attack, security analysis under the ROR model, smart device (AGT) simulation attack; protocol [15] can only prevent replay attack, and the algorithm has very low security performance. Compared with protocols [14] and [15], the calculation cost of this scheme is slightly higher, but the functional characteristics of the scheme proposed in this paper have been significantly improved, which can prevent impersonation attack, replay attack, man-in-the-middle attack, offline password guessing attack, and ESL attack, Intelligent equipment (AGT) simulation attack, ensuring safe mutual authentication and security analysis under the ROR model, the program security has been significantly improved.

Therefore, the lightweight V2G network anonymous user dynamic identity authentication and session key negotiation scheme proposed in this paper can achieve two-way authentication of participant identities, and has lower computational overhead and higher algorithm security, which can be effectively applied to practical In a V2G network environment.

7. Conclusion

In this article, we propose a more secure dynamic identity authentication and key agreement scheme to achieve privacy protection for users and devices. The BAN logic proves that the protocol guarantees secure mutual authentication between EV_i and AGT_j, and the formal security analysis of the ROR model proves that the protocol provides K security. Informal security analysis shows that the protocol effectively prevents a series of attacks such as impersonation attack, replay attack, offline guessing attack, and ESL attack. Performance analysis and security show that our protocol is more efficient and more secure, which makes it both applicable and feasible in a resource-constrained V2G network environment.

ISSN: 2688-8645

References

[1] J.Baek, Q. H. Vu, J. K. Liu, X. Huang, Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid", IEEE Trans. Cloud Comput., vol. 3, no. 2, pp. 233-244, Apr./Jun. 2015.

[2] J. Gao, Y. Xiao, J. Liu, W. Liang, C.L.P. Chen, A survey of communication/networking in smart grids, Future Gener. Comput. Syst. 28 (2) (2012) 391–404.

[3] YanXiaowen. Research on User Privacy Preserving in Vehicle to Grid Network[D]. North China Electric Power University. 2015.

[4] Wenlin Han, Yang Xiao, Privacy preservation for V2G networks in smart grid: A survey, Computer Communications, Vol. 91–92, 2016, pp.17-28.

[5] Z. Yang, S. Yu, W. Lou, C. Liu, " \$p^{2}\$: Privacy-preserving communication and precise reward architecture for V2G networks in smart grid ", IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 697-706, Dec. 2011.

[6] H.Nicanfar, S. Hosseininezhad, P. TalebiFard, V. C. M. Leung, "Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations", Proc. IEEE Conf. Comput. Commun.Workshops (INFOCOM WKSHPS), pp. 55-60, 2013.

[7] C.-C. Chang, H.-D. Le, "A provably secure efficient and flexible authentication scheme for ad hoc wireless sensor networks", IEEE Trans. Wireless Commun., vol. 15, no. 1, pp. 357-366, Jan. 2016.

[8] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, X. Huang, "Provably secure user authentication and key agreement scheme for wireless sensor networks", Security Commun. Netw., vol. 9, no. 16, pp. 3670-3687, 2016.

[9] M.Turkanović, B. Brumen, M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks based on the Internet of Things notion", Ad Hoc Netw., vol. 20, pp. 96-112, Sep. 2014.

[10] P. Zhang, C. Lin, Y. Jiang, Y. Fan, X. Shen, "A lightweight encryption scheme for network-coded mobile ad hoc networks", IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 9, pp. 2211-2221, Sep. 2014.

[11] Asmaa Abdallah, Xuemin (Sherman) Shen. Lightweight Security and Privacy-Preserving Scheme for V2G Connection[C].IEEE Global Telecommunications Conference (GLOBECOM).San Diego, CA. 2015.

[12] H. Wang, B. Qin, Q. Wu, L. Xu, J. Domingo-Ferrer, "TPP: Traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids", IEEE Trans. Inf. Forensics Security, vol. 10, no. 11, pp. 2340-2351, Nov. 2015.

[13] Y. H. Chuang, N. W. Lo, C. Y. Yang, S. W. Tang, "A lightweight continuous authentication protocol for the Internet of Things", Sensors, vol. 18, no. 4, pp. 1-26, 2018.

[14] A. Abdallah, X. S. Shen, "Lightweight authentication and privacy-preserving scheme for V2G connections", IEEE Trans. Veh. Technol., vol. 66, no. 3, pp. 2615-2629, Mar. 2017.

[15] J. Shen, T. Zhou, F. Wei, X. Sun, Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things", IEEE Internet Things J., vol. 5, no. 4, pp. 2526-2536, Aug. 2018.

[16] M. Abdalla, P.A. Fouque, D. Pointcheval, "Password-based authenticated key exchange in the three-party setting", Proc. 8th Int. Workshop Theory Pract.Public Key Cryptography (PKC), vol. 3386, pp. 65-84, 2005.

[17] M. Burrows, M. Abadi, R. Needham, "A logic of authentication", ACM Trans. Comput. Syst., vol. 8, no. 1, pp. 18-36, 1990.

[18] D.Dolev, A. C. Yao, "On the security of public key protocols", IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 198-208, Mar. 1983.

[19] R. Canetti, H. Krawczyk, "Universally composable notions of key exchange and secure channels", Proc. Int. Conf. Theory Appl. Cryptograph. Techn., pp. 337-351, 2002.

[20] A.Dua, N. Kumar, A. K. Das, W. Susilo, "Secure message communication protocol among vehicles in smart city", IEEE Trans. Veh. Technol., vol. 67, no. 5, pp. 4359-4373, May 2018.

[21] V.Odelu, A. K. Das, M. Wazid, M. Conti, "Provably secure authenticated key agreement scheme for smart grid", IEEE Trans. Smart Grid, vol. 9, no. 3, pp. 1900-1910, May 2018.

[22] R. Amin, S. K. H. Islam, N. Kumar, K.-K. R. Choo, "An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks", J. Netw. Comput. Appl., vol. 104, pp. 133-144, Feb. 2018.

[23] M.Wazid, A. K. Das, V. Odelu, N. Kumar, W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment", IEEE Trans. Dependable Secure Comput..

[24] Y.Dodis, L. Reyzin, A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", Proc. Int. Conf. Theory Appl. Cryptograph. Techn., pp. 523-540, 2004.

[25] J. H. Cheon, J. Jeong, D. Kim, J. Lee, " A reusable fuzzy extractor with practical storage size: Modifying Canetti et al .'s construction " in Information Security and Privacy, Wollongong, NSW, Australia:Springer, vol. 10946, pp. 28-44, 2018.

[26] S. Banerjee et al., "A Provably Secure and Lightweight Anonymous User Authenticated Session Key Exchange Scheme for Internet of Things Deployment," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8739-8752, Oct. 2019.

[27] K. Park, Y. Park, A. K. Das, S. Yu, J. Lee and Y. Park, "A Dynamic Privacy-Preserving Key Management Protocol for V2G in Social Internet of Things," in IEEE Access, vol. 7, pp. 76812-76832, 2019.

[28] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, J. J. P. C. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment", IEEE Internet Things J., vol. 5, no. 6, pp. 4900-4913, Dec. 2018.

[29] D. Wang, H. Cheng, P. Wang, X. Huang, G. Jian, "Zipf's law in passwords", IEEE Trans. Inf. Forensics Security, vol. 12, no. 11, pp. 2776-2791, Nov. 2017.

[30] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J.Rodrigues, "Provably Secure Fine-Grained Data Access Control overMultiple Cloud Servers in Mobile CloudComputing Based HealthcareApplications," IEEE Transactions on Industrial Informatics, vol. 15,no. 1, pp. 457–468, 2019.

[31] V .Odelu, A. K. Das, and A. Goswami, "A Secure Biometrics-BasedMulti-Server Authentication Protocol Using Smart Cards," IEEE Trans-actions on Information F orensics and Security, vol. 10, no. 9, pp. 1953–1966, 2015.

[32] Q.Xie, D. Hong, M. Bao, N. Dong, D. S. Wong, "Privacy-preserving mobile roaming authentication with security proof in global mobility networks", Int. J. Distrib. Sensor Netw., vol. 2014, pp. 7, May 2014.

[33] J.-S. Lee, C.-C.Chang, "Secure communications for cluster-based ad hoc networks using node identities", J. Netw.Comput.Appl., vol. 30, no. 4, pp. 1377-1396, 2007.