SCIENCE CHINA
Information Sciences

• LETTER •

September 2022, Vol. 65 199101:1–199101:3
https://doi.org/10.1007/s11432-019-2736-5

An anonymous key agreement protocol with robust authentication for smart grid infrastructure

Ting CHEN[1], Qingfeng CHENG[2] & Xinghua LI[1*]

[1]*School of Cyber Engineering, Xidian University, Xi'an* 710071*, China;*
[2]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou* 450001*, China*

Received 4 August 2019/Revised 2 October 2019/Accepted 9 December 2019/Published online 24 May 2021

Citation Chen T, Cheng Q F, Li X H. An anonymous key agreement protocol with robust authentication for smart grid infrastructure. Sci China Inf Sci, 2022, 65(9): 199101, https://doi.org/10.1007/s11432-019-2736-5

Dear editor,

The issue on how to ensure the smart grid environment's security and reliability has always been a focus in current research. The rapid expansion of the Internet of Things enables billions of smart devices to be involved in the smart grid, such as smart meters, who play a part in monitoring and recording consumers' power usage. The smart meter first amasses the information of energy consumption and then sends it to utility control. Utility control is responsible to collect the information, observe the trends of power consumption, and deliver the control commands. The exchange of information is transmitted in an insecure public smart grid environment. Thus, before exchanging information, two communicants are required to authenticate each other and generate a session key together, where the session key ensures the security of their session over the smart grid environment. To guarantee secure communication for the smart grid infrastructure, researchers have presented many authenticated key agreement protocols [1–4]. Most existing schemes for the smart grid, however, are found to exhibit various challenges.

Recently, for the sake of overcoming the challenges and improving the authentication in the smart grid, Mahmood et al. [5] designed an anonymous key agreement protocol, which ensured the secure communication between utility control and the smart meter. Mahmood et al. claimed that their scheme realized the smart meter's anonymous connection with utility control and provided reasonable security. Regrettably, we find Mahmood et al.'s protocol still has some security problems required to be solved. First, their scheme provides no perfect forward security. It fails to provide robust mutual authentication and suffers from an impersonation attack. Moreover, Mahmood et al.'s scheme could risk an ephemeral key compromise attack under the Canetti-Krawczyk (CK) threat model [6]. To overcome these blemishes, we propose a new security-enhanced key agreement scheme based on Mahmood et al.'s scheme, which changes the computing format of the session key and adds stronger mutual authentication between the smart meter and utility control. Additionally, we present a comparison of security properties with related work. A detailed introduction of Mahmood et al.'s scheme refers to [5].

Weaknesses of Mahmood et al.'s scheme. Detailed descriptions of those weaknesses existing in Mahmood et al.'s scheme are presented as follows.

(1) There is no perfect forward security. Perfect forward secrecy means that the exposure of the long-term master key or the user's long-term private key will not lead to the leakage of the historical session keys; thus, the lack of such property cannot guarantee the security of historical communications. In Mahmood et al.'s scheme, the produced session key is computed as $K_{ij} = H_2(Z^b) = H_2(e(M_2, S_i)^a) = H_2(e(M_1, S_j)^b) = H_2(e(P, P)^{ab})$, where M_1 and M_2 are transmitted in a public channel. Consequently, adversaries could obtain all M_1 and M_2 in previous sessions. M_1's value is $aP(s + H_1(\mathrm{ID}_j))$ and M_2 is equal to $bP(s + H_1(\mathrm{ID}_i))$, where $s + H_1(\mathrm{ID}_j)$ and $s + H_1(\mathrm{ID}_i)$ are stable values. If the long-term master key s is exposed to an attacker, then the attacker can acquire previous communication session keys between SM_i and UC_j by recalculating aP and bP according to previous sessions' M_1 and M_2.

The previous session key K_{ij} could be computed in the form of $H_2(e(aP, bP)){=}H_2(e(P, P)^{ab})$. Consequently, Mahmood et al.'s scheme fails to realize perfect forward security.

(2) Impersonation attack. It means that attackers impersonate one of the protocol participants to another participant and finally, share a session key with the participant. In the authentication phase of Mahmood et al.'s scheme, an adversary E is capable of impersonating utility control UC_j to deceive the smart meter SM_i.

The adversary could capture the message $\{M_1, Z\}$ sent to UC_j, randomly pick up a number b^* from Z_p^*, and successfully execute the protocol with SM_i. Finally, the adversary establishes a session key K_{ij}^* with SM_i. The detailed process is illustrated below.

- After SM_i performs some related calculation and sends $\{M_1, Z\}$ to UC_j, the adversary E intercepts it.
- Then, E randomly selects $b^* \in Z_p^*$ and computes $K_{ij}^* =$

[*] Corresponding author (email: xhli1@mail.xidian.edu.cn)

Table 1 Comparison of security attributes with related schemes

Scheme	A_1	A_2	A_3	A_4	A_5	A_6	A_7
[1]	×	√	×	×	×	×	√
[2]	√	√	√	×	×	×	×
[5]	√	×	×	×	√	√	×
Ours	√	√	√	√	√	√	√

$H_2(Z^{b^*}) = H_2(e(P,P)^{ab^*})$. Afterwards, attacker E computes $R_i^* = H_3(\mathrm{ID}_i\|\mathrm{ID}_j\|Z\|K_{ij}^*\|M_1)$ and $Q_i^* = \frac{1}{b^*+R_i^*}S_e$, where S_e is a forged private key of E.

• Attacker E calculates $B_i = P_{\mathrm{pub}} + H_1(\mathrm{ID}_i)P$, $M_2^* = b^*{\cdot}B_i$, and $Y^*{=}\ K_{ij}^* \oplus (\mathrm{ID}_i\|Q_i^*\|M_2^*)$ and sends the forged message $\{M_2^*, Y^*\}$ to SM_i.

• From SM_i's viewpoint, there is no discrepancy of the received message. Thus, SM_i computes $K_{ij}^* = H_2(e(M_2^*, S_i)^a) = H_2(e(P,P)^{ab^*})$ and $\mathrm{ID}_i\|Q_i^*\|M_2^* = Y^*{\oplus}K_{ij}^*$.

• SM_i further verifies whether $M_2^{'} = M_2^*$ holds. It is obvious that the result is positive. After that, SM_i computes $G_i^* = H_4(K_{ij}^*\|\mathrm{ID}_i\|\mathrm{ID}_j\|Z)$ and responds E with $\{G_i^*\}$. After the analysis, we can see that the smart meter SM_i cannot distinguish the responder that communicates with it. SM_i believes it sets up a session key with utility control UC_j, but in reality, it shares K_{ij}^* with the attacker E. Thus, E can establish sessions with SM_i and obtain some information of the smart meter.

(3) Other possible security problems. This subpart exhibits other possible attacks existing in Mahmood et al.'s scheme, such as ephemeral key compromise attack, which denotes that the leakage of the user's ephemeral key could lead to the exposure of a session key and further result in the compromise of normal communication. In Mahmood et al.'s scheme, the session key could be computed as $K_{ij} = H_2(Z^b)$, where parameter Z could be obtained by intercepting $\{M_1, Z\}$ from the insecure public channel; thus, an adversary can compute K_{ij} if the utility control's ephemeral key b is known to the adversary. Mahmood et al.'s scheme, therefore, could risk the ephemeral key compromise attack under the CK-adversarial model.

The proposed scheme. Since the new proposed scheme is improved based on Mahmood et al.'s scheme, the system setup and registration of the new proposed scheme are similar to their scheme, whose detailed description refers to [5]. As Mahmood et al.'s scheme accepts the smart meter and utility control, the scheme also involves a trusted three party TA. TA executes some trusted operations, who is responsible for system setup and communicants' registration, but TA does not participate in the communicants' authentication. The following subpart will present the description of our scheme (related preliminaries and the explanations of the notions used in our scheme are seen in Appendixes A and B, respectively).

(1) System setup. The system setup of our scheme is like Mahmood et al.'s scheme. The only difference is the definition of the five hash functions. In the new scheme, TA defines H_1, H_3, and H_4 as $Z_p^* \to Z_p^*$. H_2 is defined as $G_2 \to Z_p^*$ and H_5 is defined as $Z_p^* \to G_1$.

(2) Registration. The concrete process of registration refers to [5]. The difference of SM_i's registration reflects in the choice of temporary keys. In the new scheme, after the smart meter receives its private key, SM_i determines $Z = g^{a+H_3(S_i\|x_1)}$, where parameters a and x_1 are random integers selected from Z_p^*.

(3) Authentication. The smart meter and utility control must achieve mutual authentication before they communicate with each other. In the authentication, the validity of the corresponding participants' identity is checked. In the end, SM_i and UC_j agree on the session key sk_{ij}. The steps are as follows.

• SM_i randomly picks up two integers $a, x_1 \in Z_p^*$, calculates $Z = e(P,P)^{a+H_3(S_i\|x_1)} =^{a+H_3(S_i\|x_1)}$, $A_j = P_{\mathrm{pub}} + H_1(\mathrm{ID}_j)P$, $M_1 = (a + H_3(S_i\|x_1)) \cdot A_j$, and $Y_1 = H_4(\mathrm{ID}_i\|\mathrm{ID}_j\|Z\|M_1)$, and sends $\{M_1, Y_1\}$ to UC_j.

• After receiving $\{M_1, Y_1\}$ from SM_i, UC_j selects two random numbers b, x_2 from Z_p^*, computes $Z = e(M_1, S_j) = e(P,P)^{a+H_3(S_i\|x_1)}$, and verifies whether $Y_1 = H_4(\mathrm{ID}_i\|\mathrm{ID}_j\|Z\|M_1)$ is valid using the computed Z and the received M_1. If the result is negative, UC_j immediately terminates the authentication.

• Otherwise, utility control UC_j determines $V = e(P,P)^{b+H_3(S_j\|x_2)} = g^{b+H_3(S_j\|x_2)}$, further generates the subkey $K_{ij} = H_2(Z^{b+H_3(S_j\|x_2)})$, and uses the subkey to compute the session key $\mathrm{sk}_{ij} = H_4(\mathrm{ID}_i\|\mathrm{ID}_j\|Z\|V\|K_{ij})$.

• Afterwards, utility control calculates $B_i = P_{\mathrm{pub}} + H_1(\mathrm{ID}_i)P$, $M_2 = (b + H_3(S_j\|x_2)){\cdot}B_i$, and $Y_2 = H_4(\mathrm{ID}_i\|\mathrm{ID}_j\|V\|M_2)$ and replies SM_i with $\{M_2, Y_2\}$.

• Upon receiving $\{M_2, Y_2\}$ from UC_j, SM_i calculates $V = e(M_2, S_i) = e(P,P)^{b+H_3(S_j\|x_2)}$. Then, SM_i checks the correctness of the equation, whose value is $Y_2 = H_4(\mathrm{ID}_i\|\mathrm{ID}_j\|V\|M_2)$. If the result is negative, SM_i immediately ends the session.

• Otherwise, the smart meter SM_i further computes the subkey $K_{ij} = H_2(V^{a+H_3(S_i\|x_1)})$ and uses it to generate $\mathrm{sk}_{ij} = H_4(\mathrm{ID}_i\|\mathrm{ID}_j\|Z\|V\|K_{ij})$.

• The smart meter finally calculates $G_i = H_4(\mathrm{ID}_i\|\mathrm{ID}_j\|Z\|V\|\mathrm{sk}_{ij})$ and sends G_i to utility control.

• Finally, utility control verifies $G_i = H_4(\mathrm{ID}_i \parallel \mathrm{ID}_j \parallel Z \parallel V \parallel \mathrm{sk}_{ij})$ with its V and the computed Z and sk_{ij}. If it is valid, then UC_j can use sk_{ij} to communicate and exchange information with the smart meter. Otherwise, UC_j fails to agree on sk_{ij} with SM_i.

Security attributes comparison. Here we select [1, 2, 5] for comparison. Seven kinds of security properties are compared among those schemes. The result of the comparison is seen in Table 1. In the table, A_1–A_7 denote user anonymity, perfect forward secrecy, mutual authentication without TA's assistance, resistance to impersonation attack, resistance to replay attack, resistance to man-in-the-middle attack, and resistance to ephemeral key compromise attack under the CK-adversarial model. From the table, we can conclude that the new proposed scheme is more robust in security. For instance, Ref. [2] suffers from an impersonation attack, replay attack and man-in-the-middle attack, but our scheme withstands those attacks. Also, Ref. [5] suffers from an impersonation attack and lacks perfect forward secrecy, which is overcome and realized in our scheme. More details on the security analysis of the new proposed scheme are seen in Appendix C.

Conclusion. This letter claimed that Mahmood et al.'s scheme still exhibited some vulnerabilities. Concretely, their scheme cannot withstand an impersonation attack and fails to realize perfect forward secrecy and mutual authentication with the absence of the trusted authority. Moreover, their scheme could suffer from an ephemeral key compromise attack under the CK threat model. We, therefore, fixed those weaknesses and proposed a new security-enhanced scheme where we changed the session keys' format and added robust authentication between the smart meter and utility control. The computation cost, however, is higher in the new scheme (seen in Appendix D) and we do not solve the key escrow problem. In the future, we wish to design protocol with computation cost declined and give solutions to the key escrow problem for the smart grid infrastructure.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. U1708262, U1736203, 61872449).

Supporting information Appendixes A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Wang Y. Password protected smart card and memory stick authentication against off-line dictionary attacks. In: Proceedings of IFIP International Information Security Conference. Berlin: Springer, 2012. 489–500

2 Tsai J L, Lo N W. Secure anonymous key distribution scheme for smart grid. IEEE Trans Smart Grid, 2015, 7: 906–914

3 Chen Y, Martinez J F, Castillejo P, et al. A bilinear map pairing based authentication scheme for smart grid communications: PAuth. IEEE Access, 2019, 7: 22633–22643

4 Guan Z T, Zhang Y, Zhu L H, et al. EFFECT: an efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid. Sci China Inf Sci, 2019, 62: 032103

5 Mahmood K, Li X, Chaudhry S A, et al. Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure. Future Generation Comput Syst, 2018, 88: 491–500

6 Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2001. 453–474