Original Research Paper | Computer Science | Volume : 5 ¦ Issue : 9 ¦ Sep 2020 ¦ e-ISSN : 2456-5040

LIGHTWEIGHT SECURITY AUTHENTICATION SCHEME FOR SMART GRID COMMUNICATION

Kun Qian[1], Baoyuan Kang[1], YanBao Han[1]

[1]Tiangong University

ABSTRACT

With the introduction of smart grid technology as the next generation of power grid, the monitoring of power system is facing new challenges. Smart grid technology improves the reliability, security and efficiency of the grid, but due to its reliance on communication technology, protecting the data transmitted over the public communication network has always been a huge challenge. To solve this security problem, different authentication schemes have been proposed. However, most of them are still plagued by privacy or performance issues. This paper presents a lightweight security authentication scheme for smart grid communication, which enables smart meters and service providers in smart grid to authenticate each other and establish Shared session keys. Compared with the existing smart grid authentication scheme, the fast mutual authentication between smart meters and service providers is realized, and the traceability of smart meters is guaranteed and the performance of the scheme is improved.

KEYWORDS: smart grid; mutual authentication; key agreement

1. INTRODUCTION:

As a new mode of power management network, smart grid has attracted wide attention due to its reliability, efficiency and sustainability (Lu, Liang, Li, Lin, & Shen, 2012) .Compared with traditional power grid, smart power grid can dynamically adjust power consumption according to users' demands. This improves the efficiency and reliability of the grid. Smart grids work within the framework of a complex system that consists of three main types of entities: smart devices (such as smart meters), communication modules (such as substations and telegraph poles), and control centers (such as service providers) (Chen, Miao, Hao, & Hwang, 2017; Metke & Ekl, 2010). On the top are smart meters, electronic devices that regularly monitor power consumption and stability on the grid. The collected data will be transmitted to the corresponding service provider via the communication module. Smart grid service providers will provide users or utilities with power resources and services and charge them based on recorded information transmitted by smart meters (Chen, Li, Hao, Qian, & Humar, 2018).

Security has always been a big issue with this kind of infrastructure, because for most smart grid environments, they run on insecure publican networks. This will lead to a variety of security threats (Li, Aung, Williams, & Sanchez, 2014). For example, an adversary could easily intercept a message through simple eavesdropping and launch an attack to obtain private information about the user. If sensitive data is compromised by rivals, the grid could face greater security challenges. One good way to solve security problems in smart grids is through mutual authentication. Smart meters and corresponding service providers can authenticate each other and negotiate keys between them. This authentication and key agreement mechanism can effectively meet the security requirements of smart grid through insecure communication channels. In recent years, smart grid authentication and key protocol schemes have been widely studied. Although various schemes have been put forward, most of them still have security defects and cannot meet certain security requirements. Performance is another issue that smart grid security needs to address (Yan, Qian, Sharif, & Tipper, 2013). For example, elliptic curve cryptography is recommended for anonymous authentication and key protocols. However, they usually involve time-consuming operations such as bilinear pairs. This raises practical questions when they are used in smart grid environments due to their energy limitations. Therefore, how to design a low computation, authentication and key protocol scheme is always a difficult problem.

The scheme proposed in this paper not only solves the security problem by realizing the mutual authentication between smart meters and service providers, but also USES symmetric keys to encrypt the data with less computation and time.

2. PROPOSED SCHEME:

The scheme proposed in this paper consists of two parts: registration and login key agreement. The registration part is where the smart meter user registers with the service provider through secure channels or offline registration. The second part is that the smart meter user first logs in and authenticates, then authenticates with the service provider and generates a session key with it. The meanings of various symbols in the proposed scheme are shown in the following table:

Table 1
The meanings of various symbols in the proposed scheme

Symbol	Description
SM_i	The i-th smart meter in the smart grid
SP_j	The j-th service provider in smart grid
ID_i	Identity information of the i-th smart meter
PW_i	Password for the i-th smart meter
K_{sm}	The secret value of a smart meter
K_{sp}	The secret value of the service provider
a, b, c, d	High entropy random Numbers
$H(\bullet)$	Collision-resistant hash function
$\oplus$	Exclusive-or operation
$\|$	Concatenation operation
E_s / D_s	Encrypt/decrypt using a pre-shared symmetric key

1) Registration phase:

When a smart meter SM_i wants to access the corresponding service provider SP_j, it will perform the following registration process

A. The smart meter user(SM_i) first inputs the identity value ID_i and password PW_i, then selects a random number, then calculates it $A_i = h(ID_i \| a \| PW_i)$, and finally sends the identity value ID_i and random number a to the service provider (SP_j) through a secure channel.

B. When SP_j receives the message from the smart meter user, it should Calculate $M_i = D_s\left[ID_i \oplus h(ID_j \| K_{sp})\right]$、$G_i = D_s\left[a \oplus h(ID_j \| K_{sp})\right]$、$Q_i = h(ID_i \| a \oplus ID_j \| K_{sp})$. K_{sp} which is a secret value of the service provider. Then service provider sends the calculated value M_i 、 G_i to SM_i through a secure channel and stored Q_i in its own database.

C. After receiving the message, SM_i will store the information{ A_i 、 M_i 、 G_i 、 a }secretly in the tamper-resistant device which is integrated with the smar meter .

2) Login and key agreement phase:

E. When the service provider receives the encrypted message ,then it decrypts the message to get $M_i^{'}$ 、 $G_i^{'}$、 $N_i^{'}$、 $L_1^{'}$ 、 T_i , the message refresh value ΔT is calculated first. If the value is within the range, the following operation is carried out ; otherwise, the service is denied. Then SP_j decrypts $M_i^{'}$ and $G_i^{'}$ to get $ID_i^{'} \oplus h(ID_j^{'} \| K_{sp}^{'})$ and $a^{''} = a^{'} \oplus h(ID_j^{'} \| K_{sp}^{'})$, computes $D_i^{''} = ID_i^{'} \oplus h(ID_j^{'} \| K_{sp}^{'}) \oplus h(ID_j \| K_{sp})$ 、 $a^{''} = a^{'} \oplus h(ID_j^{'} \| K_{sp}^{'}) \oplus h(ID_j \| K_{sp})$ 、 $Q_i^{'} = h(ID_i^{''} \| a^{''} \oplus ID_j \| K_{sp})$, and then SP_j verify that the calculated value $Q_i^{'}$ is equal to the value Q_i stored in own database that if the two values are equal you can prove that the messa ge came from a previously registered smart meter user, otherwise you deny service. Next, the service provider calculates $r^{'} = h(ID^{''} \| a^{''} \| N^{'})$, $L_1^{*} = h(N^{'} \| r^{'})$ and verifies $L_1^{*} = L_1^{'}$. If the two values are equal it can prove that the values in the encrypted message have not been tampered with; otherwise, the service is denied. Then the service provider selects two random Numbers c and d ,then calculates $U = h(K_{sp} * c) + d$ 、 $SK = h(ID_i^{''} \| a^{''} \| N \| U)$、 $L_2 = h(U \| SK)$. Finally, L_2 、 U 、 T_j is encrypted with the symmetric key S previously Shared by the smart meter and the service provider and then sent to the smart meter.

F. When smart meters SM_i receives an encrypted message, to decrypt the message to get $L_2^{'}$ 、 $U^{'}$ 、 T_j firstly, and then calculate refreshness value ΔT to see if the numerical value of ΔT within a domain, then calculate the $SK^{'} = h(ID_i^{*} \| a \| N \| U^{'})$ 、 $L_2^{''} = h(U^{'} \| SK^{'})$ and to verify whether $L_2^{''} = L_2^{'}$, if the two values are equal to the messages from the service provider and content has not been tampered with, or denial of service. $SK = h(ID_i \| a \| N \| U)$ is obtained as the session key, which can be used to encrypt the content of the session message for subsequent communications.

3. SAFETY ANALYSIS:

3.1 Replay attack:

Replay attack is a type of network attack in which an attacker maliciously or fraudulently repeats or delays the transmission of valid data. The repetition or delay of the transmitted data is performed by the sender or malicious entity, who intercepts the data and retransmits it. In our proposed scheme pattern, in o rder to prevent replay attacks in each transmission, we added the time-stamp T_i flag to check the freshness of incoming and incoming message refresh value ΔT . The timestamp T_i in each transmitted message is generated by the service provider or entity of the smart meter and then given to the other par ty for inspection. Therefore, placing the timestamp T_i in the transmitted message can effectively prevent the attacker from replay attack on the service provider or smart meter.

3.2 Man-in-the-middle attack:

In security and encryption, a man-in-the-middle attack is when an attacker secretly intercepts, relays a message, or alters the communication between two entiti

that believe they are communicating directly. The proposed scheme uses an effective mutual authentication mechanism and encrypts the transmitted messages using symmetric key. If the attacker can obtain the symmetric key and wants to tamper with the transmitted message, he needs to know the parameter a , but this parameter is protected by G_i during the transmission. For example, tampering with the value G_i will make the value Q_i unable to communicate again without verification at the service provider. So we propose a scheme to prevent man-in-the-middle attacks.

4. PERFORMANCE ANALYSIS:

In this part, we will compare our proposed scheme with other relevant advanced schemes in terms of function and cost calculation.

Table 2

	(Xia & Wang, 2012)	(Mohammadali, Haghighi, Tadayon, & Mohammadinodooshan, 2018)	(Mahmood et al., 2018)	(Kumar, Gurtov, Sain, Martin, & Ha, 2019)	ours
Replay attacks	√	√	√	√	√
Man-in-the-middle attacks	√	√	√	√	√
Perfect forward secrecy	√	√	√	√	√
Meet-in-the-middle attack	-	-	-	-	√
Impersonation attacks	×	√	√	√	√

√: Prevents the attack or provides the security property;

×: Does not prevent the attack or does not provide the property;

-: Does not discuss the security property.

4.1 Functional comparison:

Table 2 shows the comparison of functional safety between the proposed scheme and other advanced schemes in the other four relevant literatures recently proposed (Xia & Wang, 2012) (Mohammadali et al., 2018) (Kumar et al., 2019; Mahmood et al., 2018). The results show that the proposed scheme meets higher security requirements and can resist all kinds of known attacks. In particular, the scheme can resist medevac attack and has non-retroactive tracing, so as to realize security protection in the process of mutual authentication and key negotiation. These two security features are of great significance to the design of secure authentication key protocol in smart grid environment.

4.2 Computational cost comparison:

GOOSE and SV protocols for broadcasting multimedia messages over LAN use switched Ethernet. In the proposed pattern, the substation and the data center agree on the session key in less time than the transfer time required for these protocols. This section will analyze the performance of the proposed protocol from a time perspective. The results were derived in the system with E2200 2.20ghz Intel Pentium CPU, 2 GB of RAM. The operation times of each cipher element are listed in Table 3. Table 4 shows the calculation cost of the comparison.

Table 3

The operation time of the password element

Symbol	Description	Time-consuming（ms）
Th	The time to execute the hash function	≈0.002
Te/Td	The time at which a symmetric encryption/decryption operation is performed	≈0.042
Tm	The execution time of the dot product operation of elliptic curve	≈2.432
Ta	The execution time of elliptic curve point addition operation	≈0.029
Thmac	The time at which a hash based message authentication code (HMAC) operation is performed	≈0.005

Table 4
Computational cost comparison

Scheme	Smart meter	Service Provider	Total time-consuming
(Xia & Wang, 2012)	3Th +1Td≈0.047ms	3Th≈0.005ms	6Th +1Td≈0.052ms
(Mohammadali et al., 2018)	3Th+2Tm≈14.868ms	4Th+3Tm≈0.825ms	7Th+5Tm≈15.693ms
(Mahmood et al., 2018)	3Th+2Tm≈15.014ms	2Th+3Tm+1Ta≈0.851ms	5Th+5Tm+1Ta≈15.965ms
(Kumar et al., 2019)	3Th+1Te+1Td+2Tm+2Thmac≈16.346ms	4Th+1Te+1Td+3Tm+2Thmac≈0.976ms	7Th+2Te+2Td+5Tm+4Thmac≈17.306ms
Our scheme	6Th+1Te≈0.052ms	7Th+2Te+3Td≈0.222ms	13Th+3Te+3Td≈0.274

5. CONCLUSIONS:

This paper presents a security authentication scheme based on smart grid communication. The scheme realizes fast mutual authentication and key protocol between smart meters and service providers. In addition, in the process of authentication and key protocol, smart meters can achieve anonymity and untraceability at a lower computational cost. The security discussion shows that the scheme is secure. All these prove the applicability of our proposed scheme in the smart grid environment.

REFERENCES:

i. Chen, M., Li, W., Hao, Y., Qian, Y., & Humar, I. (2018). Edge cognitive computing based smart healthcare system. Future Generation Computer Systems, 86.

ii. Chen, M., Miao, Y., Hao, Y., & Hwang, K. (2017). Narrow Band Internet of Things. IEEE Access, 20557-20577.

iii. Kumar, P., Gurtov, A., Sain, M., Martin, A. J., & Ha, P. H. (2019). Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks. IEEE Transactions on Smart Grid, 10(4), 4349-4359.

iv. Li, D., Aung, Z., Williams, J., & Sanchez, A. (2014). P3: Privacy Preservation Protocol for Automatic Appliance Control Application in Smart Grid. IEEE Internet of Things Journal, 1(5), 414-429.

v. Lu, R., Liang, X., Li, X., Lin, X., & Shen, X. (2012). EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications. IEEE Transactions on Parallel & Distributed Systems, 23(9), 1621-1631.

vi. Mahmood, K., Chaudhry, S. A., Naqvi, H., Kumari, S., Li, X., & Sangaiah, A. K. (2018). An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. Future Generation Computer Systems, 81, 557-565.

vii. Metke, A. R., & Ekl, R. L. (2010). Security Technology for Smart Grid Networks. IEEE Transactions on Smart Grid, 1(1), 99-107.

viii. Mohammadali, A., Haghighi, M. S., Tadayon, M. H., & Mohammadinodooshan, A. (2018). A Novel Identity-Based Key Establishment Method for Advanced Metering Infrastructure in Smart Grid. IEEE Transactions on Smart Grid, 9(4), 2834-2842.

ix. Xia, J., & Wang, Y. (2012). Secure Key Distribution for the Smart Grid. IEEE Transactions on Smart Grid, 3(3), 1437-1443.

x. Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013). A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. IEEE Communications Surveys & Tutorials, 15(1), 5-20.