Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2017, 10, 307-315
http://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

Security and Privacy-Preserving Metering Service in the Smart Grid

Zhongwei Sun, Chuqi Song

School of Electrical and Electronic Engineering, North China Electric Power University, Beijing, China
Email: zwsun@ncepu.edu.cn, 843842759@qq.com

How to cite this paper: Sun, Z.W. and Song, C.Q. (2017) Security and Privacy-Preserving Metering Service in the Smart Grid. *Int. J. Communications, Network and System Sciences*, **10**, 307-315.
https://doi.org/10.4236/ijcns.2017.108B033

Received: August 7, 2017
Accepted: August 11, 2017
Published: August 14, 2017

Abstract

The deployment of smart metering provides an immense amount of data for power grid operators and energy providers. By using this data, a more efficient and flexible power grid can be realized. However, this data also raises privacy concerns since it contains very sensitive information about customers. In this paper, we present a security and privacy-preserving metering scheme for the community customers, by utilizing the password authenticated key exchange (PAKE) protocol and Elliptic Curve Cryptosystem (ECC). The proposed scheme will protect the community network from possible malicious behavior, and security analysis is also given in the paper.

Keywords

Community, Password Authentication, Elliptic Curve Cryptography (ECC), Privacy

1. Introduction

Today's electrical grid is changing rapidly into a smarter grid to address the demands of distributed generation. An important task for the smart grid is accurate monitoring of energy consumption and production. Smart metering is a crucial part for the realization of the vision of smart grid. In its most basic form, it describes a deployment of electric meters that enable two-way communication between meter and distribution system operator. This is often called the Advanced Metering Infrastructure (AMI).

Smart metering provides accurate, near real-time measurements of household consumption. Using this data, energy suppliers can plan their energy production more efficiently and provide users with real-time pricing. However, smart metering data also poses a threat to the privacy of people living in the measured households. Using nonintrusive load monitoring, anyone with access to smart

metering data can deduce highly private information [1] [2]. Even with measurements taken only every 15 minutes, patterns of usage for appliances can be deduced. Private information like working hours, personal habits and even religious beliefs are at risk of being no longer private through smart metering [3].

At present, extensive studies have been conducted on the information security of smart grid [4] [5] [6] [7]. However, most of the results achieved are not applicable to the privacy problems of the smart electricity meters. In this paper, we propose a security and privacy-preserving metering scheme for the community customers, by utilizing the password authenticated key exchange (PAKE) protocol [8] [9] [10] and Elliptic Curve Cryptosystem (ECC) [11] [12] [13]. The rest of this paper is organized as follows: Section 2 presents the related background knowledge. Section 3 describes our proposed scheme while its security analysis and algorithm comparison are proved in Section 4. Finally, Section 5 concludes the paper.

2. Background Knowledge

2.1. Community Energy Management System

In the architecture of smart grid, the user's power consumption data of a community is usually sent to the power grid control center via smart meters through community gateway. In a community with n homes, the gateway need to forward every home electricity consumption data to the grid control center at regular intervals, the control center can use these data to analyze the power usage condition of the energy community. The typical energy community architecture is shown in **Figure 1**.

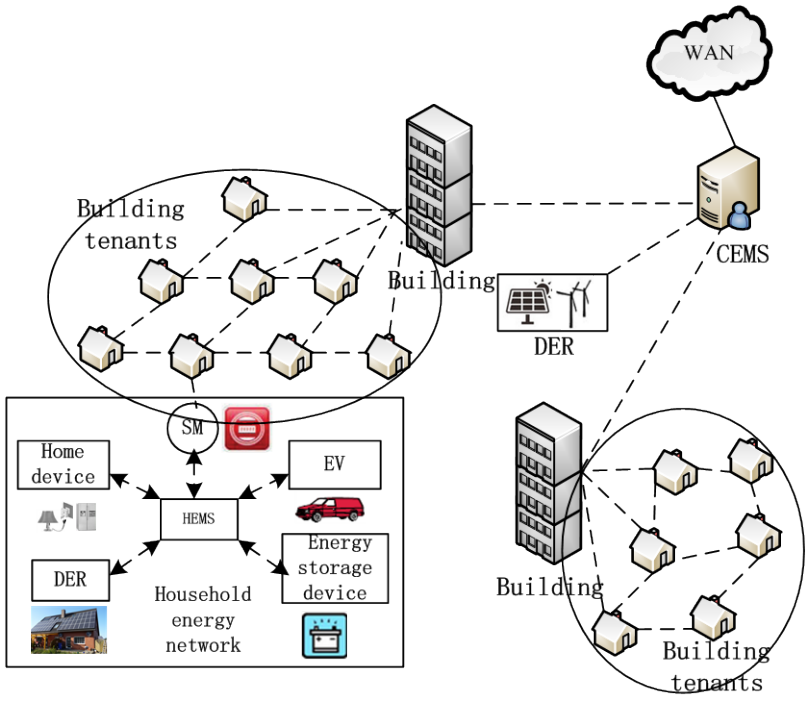

Figure 1. Smart community energy management system.

As shown in the figure, Community Energy Management System (CEMS) is an energy management center of the intelligent community, which is used to manage and record the community household energy consumption, collect user consumption data. Through the analysis of such information the energy suppliers are able to schedule and control of electrical equipment within the community, improve the electricity efficiency of the residents side, and eventually achieve the purpose of energy saving.

This paper takes the energy community as the research object to establish safety authentication between the smart meters, the community energy management system, and aggregate the user data in the community. Assuming that all the data are transferred in the encrypted form, for example, the gateway need to forward an encrypted user electricity to the grid control center at regular intervals, the control center can be used to analyze the power usage condition of the community after the decryption of the encrypted power consumption respectively. Obviously the cost of communication is relatively high, and if the adversary breached or compromised the server of control center, they can get the community electricity data of any user, which can analyze the user's habits or even worse.

After data aggregation, the energy management system will decrypt the energy consumption data first, and take aggregation operations. The aggregated data is then encrypted and sent to the power grid control center. Finally, the control center carries out the decryption of the received data to obtain the total electricity consumption of the community. This approach reduces the communication cost from community energy management system to the power grid control center, and the data stored in the control center server is the whole electricity consumption of the community instead of user's personal consumption. Therefore, the adversary cannot obtain the user's electricity consumption through the intrusion control center, so as to protect the user's privacy.

2.2. Data Privacy with Shielding Parameter

The electricity information in smart meters is a group of sensitive data to users, which need to preserve its privacy. In order to solve this problem, we introduce shielding parameters for data privacy process. User data statistics held in smart meters is aggregated to CEMS with shielding parameters. Illegal attacks against any user equipment can't obtain the real user consumption data, which ensure the user privacy and data security in the household energy network.

Supposing that a wireless network area contains n acquisition terminals, each terminal of the sensor nodes at the same time send packets to collection centers/aggregators, and no packet losses. As shown in **Figure 2**, detailed steps are describes as follows:

1) Choosing a set of data generated by data collection centre/aggregator as shield parameters, these parameters meet the condition $\sum_{i=0}^{i=n} R_i = 0$, shielding parameter R_i can be distributed randomly by the data acquisition center to terminal equipment.

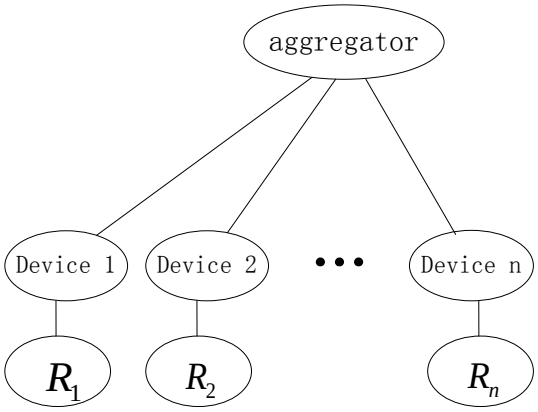

Figure 2. Data transmission with shielding parameters.

2) When the terminal devices send data M_i to the collection center, shielding parameter R_i will be added to the data M_i to hide the real information. Then the hidden data $\{M_i + R_i\}$ will be sending to collection center.

3) Data collection centers aggregate data from terminal devices, these aggregation can be the real consumption that user use.

3. The ECC-Based Password Authentication and Privacy Preserving Scheme

To authenticate mutually network devices in the energy community, an enhanced ECC based password authentication scheme in is utilized. As shown in **Figure 3**. To ensure the reliability and confidentiality of data transferring, the mutual authentication between community energy management systems and smart meters is necessary. As shown in **Figure 3**, after a secure session has been established, the community user data can be gathered in hidden way, and the aggregated data is the total consumption of the community electricity, attacker can't get user's personal consumption data to pry user's privacy.

More specifically, this proposed scheme is divided into three stages: initialization phase, authentication phase, data privacy phase, which are described as follows.

3.1. Initialization Phase

Assuming that password Pw and secret key x are shared between CEMS and smart meters, and the CEMS A does not know the password Pw and $\pi = H(ID_A, ID_B, Pw, x)$ is stored in its database. On the other hand, smart meter B has the plain password and computes π in every session. Furthermore, the trusted center generated a safety elliptic curve. Its basic parameters can be defined as follows:

$$Para = \{F_q, E, G, n, H\}$$

where F_q is the prime field of the elliptic curve, E is the elliptic curve, G is the base point of the elliptic curve, n is a prime number and be the order of G, and H is a one-way mapping function that can map any string to domain F_q.

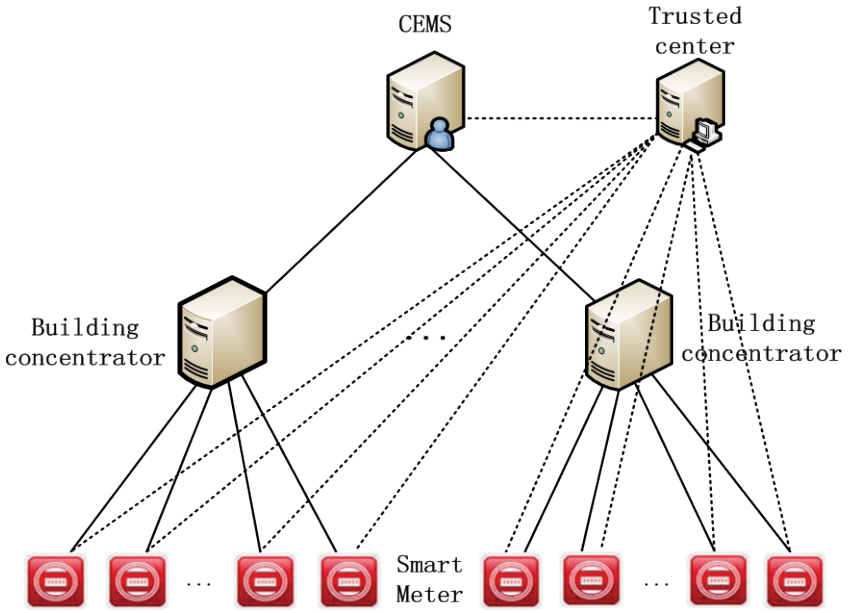

Figure 3. Intelligent community communication network.

3.2. Authentication Phase

After initialization, CEMS and smart meters must be authenticated mutually before communication. Now assuming that they have determined their public and private keys. Each intelligent device has its own identity ID, the trusted center store the hash value of all the smart meter ID instead of the meter ID, which can saving storage space of database. If a smart meter B want to communicate with CEMS, the meter need to calculate the H(ID_b) and sent to the trusted center, then the trusted center will compare the transmitted data with H(ID_b) stored in the database. If it has, then begin to authenticate. If not, then refuse authentication. Authentication steps are shown in **Figure 4**.

Step 1: Community EMS A select two random number $r_A \in F_q$, $s_a \in F_q$,and s_a is selected as its private key, and compute $P_A = s_a^{-1}G$ as its public key, then transmit ID_A and P_A to Smart Meter B.

Step 2: Smart Meter B select two random numbers $r_B \in F_q$, $s_b \in F_q$, and s_b is selected as its private key, and compute $P_B = s_b^{-1}G$ as its public key. B gets A's public key P_A, then computes $\pi = H(ID_A, ID_B, Pw, x)$, $S_B = r_B P_A$ and $S'_B = S_B \oplus \pi \oplus x$. Finally, sends its identifier ID_B together with P_B, S'_B and π to A.

Step 3: A receives the message from B, and checks if $\pi = H(ID_A, ID_B, Pw, x)$ extracted from A's database or not. If it is not verified, it halts the protocol run with error. Otherwise, it believes that another party has knowledge of the valid B's password and secret key x. A then compute $S'_B = S_B \oplus \pi \oplus x$. After got the real S_B, A constructs the session key as $K_{AB} = r_A s_a S_B$ using its private key s_a. A calculates $S_A = r_A P_B$, $S'_A = S_A \oplus \pi \oplus x$, $y = H(ID_A, ID_B, S_A, S_B, K_{AB})$, and sends S'_A, y to B.

Step 4: Smart Meter B get the message from A, and then acquires S_A as

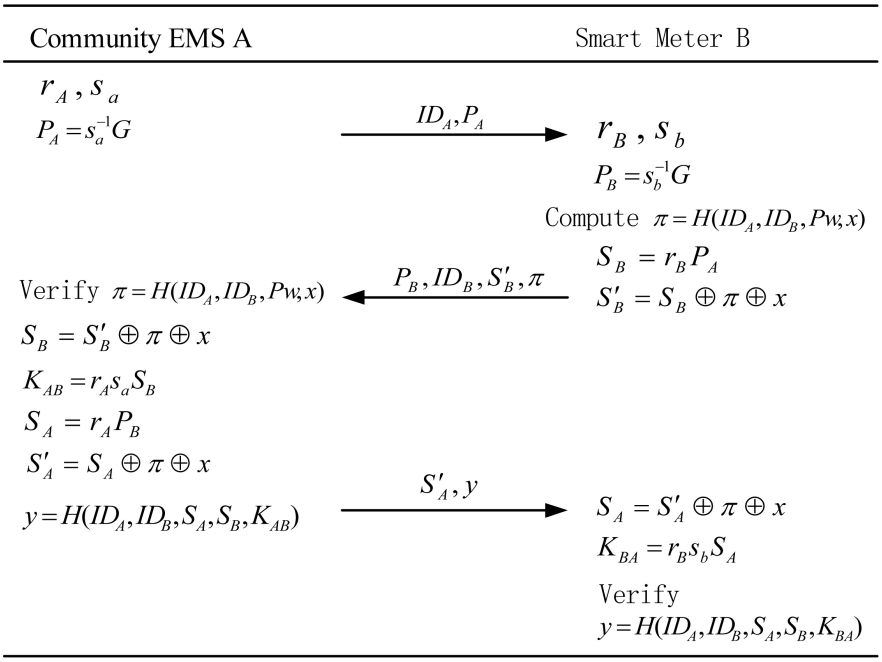

Figure 4. Protocol authentication process.

$S'_A = S_A \oplus \pi \oplus x$, generates the session key as $K_{BA} = r_B s_b S_A$ using its private key s_b. Later, B verifies $y = H(ID_A, ID_B, S_A, S_B, K_{BA})$ or not. If the equality is not satisfied, authentication fails with error that it means the opposite side ***A*** is not trustworthy. If it is verified, the authentication is successful, trusted parties can communicate securely, and the session key is

$K_{AB} = K_{BA} = r_B s_b S_A = r_B s_b r_A P_B = r_B r_A G$.

3.3. Data Privacy Phase

After the authentication, the agreement needs to be further strengthened to ensure the privacy of user data. In the energy community, smart meters are grouped in different buildings, shielding parameter R_i can be distributed randomly by the trusted center to all the smart meters. And the condition $\sum_{i=0}^{i=n} R_i = 0$ must be satisfied. Before the user's electricity data transmission begin, Shielding parameters are mixed into smart meters to hide real data $K'_i = K_i + R_i$, and then all the hidden consumption are posted to Community Energy Management System encrypted by the session key generated from the previous phase. CEMS aggregates all data received from smart meters $\sum K'_i = \sum (K_i + R_i) = \sum K_i + \sum R_i = \sum K_i$ to get the real total consumption.

4. Security Analysis of the Proposed Scheme

In this section, the security of proposed protocol is analyzed and it is shown that the proposed scheme has resilience to several well-known attacks, such as replay attack, dictionary attack and man-in the middle attack. Here, we briefly explain the security properties for the proposed protocol.

Known session key security: The session keys of different sessions are inde-

pendent from each other, and it is difficult for attackers to acquire a new session key from the revealed session keys of the past sessions. Because the session key K_{AB} is calculated from two random numbers r_A and r_B that are independently selected by Community EMS ***A*** and smart meter ***B***, respectively. These random numbers will change for every session. Therefore, the proposed protocol provides the known session key security properties.

The current session key security: In the security authentication stage, the selection of random number r_A, r_B and generation of session key K_{AB} occur inside their own devices of both parties without transmitting through the wireless channel, the attacker can't steal Meaningful results. In addition, because of the collision-resistant property of a one-way hash function, adversary can't obtain K_{AB} from the equation $y = H(ID_A, ID_B, S_A, S_B, K_{AB})$.

Resilience to dictionary attack: In the authentication phase between CEMS and smart meters, the password information Pw shared between the two sides does not appear in the transmission process, an attacker can't get a clear confirmation of the password. Assuming that the adversary guesses Pw' as a password of smart meter, but he/she does not have the pre-shared secret key x, so he/she cannot compute the expected values $\pi = H(ID_A, ID_B, Pw, x)$. Therefore, ***A*** cannot acquire the correct value π and obtains a different value and validates $\pi' = H(ID_A, ID_B, Pw', x')$. Obviously, ***A*** recognizes that the opposite party is not the real one, the attack take places and then ***A*** stops protocol run with error, so the attack on password is discernible.

Resilience to password compromised impersonation attack: It is assumed that the smart meter's password Pw leaks, the attacker knows Pw, but doesn't aware the pre-shared keys x, the correct π is still unknown. Thus the check fails and the attack cannot be carried out. Moreover, even if calibration is successful, and get the right S_B from equation $S_B' = S_B \oplus \pi \oplus x$, the attacker cannot get the selected random number r_B from formula $S_B = r_B P_A$ because of the difficulty of solving ECDLP. Consequently, the password compromise impersonation attack cannot take place on the proposed protocol.

Resilience to illegal devices masquerading attack: Each device in the network has its unique ID, before the authentication phase, all smart meter ID's hash value will be stored in the database of the trusted center. If an attacker with illegal equipment want to camouflage smart meter to communicate with CEMS, he/she need to send the device ID of the hash function H(ID) to a trusted center to check first. If no hash function satisfies the requirement, the protocol can be stopped.

Resilience to replay attack: In this protocol, Two random numbers r_A and r_B generated from ***A*** and ***B*** separately are used in constructing the session key and other factors. The selection of random number ensures the novelty of session, and guarantees us that the proposed scheme is secure against replay attack.

Resilience to key compromise impersonation attack: Suppose that private key s_a of energy management system compromises, the attacker still cannot get the correct session key K_{AB}. Because the attacker does not know the random

number EMS selected r_A, and also can't get the corresponding password $\boldsymbol{Pw}$ and pre distribution key $\boldsymbol{x}$ from the smart meter, unable to get the correct S_B from the S'_B. Therefore, the correct session key $K_{AB} = r_A s_a S_B$ is not calculated. Similarly, even if the smart meter's private key s_b leaks, the results also cannot solve the correct session key.

Privacy preserving: This scheme adopts the way of adding shielding parameters, hiding the real power data of the users, and cannot get the valid data from the users, user's actual energy consumption is only in the community energy management system, nor can it be a threat to the user's behavior and the stability of the power grid.

5. Conclusion

In this paper, the password authentication and elliptic curve cryptography are combined to realize the two-way secure authentication between smart meter and community energy management system in energy community. Under the premise of ensuring the security, reliability and non-repudiation of communication, the user's privacy is protected. The security of the ECC based password authentication algorithm is better under the condition of the same key length because of the particularity of the short distance wireless communication. Compared with other encryption algorithm, elliptic curve cryptography (ECC) has great advantages in computational demand, key length and security, especially suitable for resource constrained environment. Due to the intractability of the elliptic curve discrete logarithm problem, the protocol can effectively resist the impersonation attack, replay attack, password compromise impersonation attack, dictionary attack etc.

References

[1] Finster, S., Baumgart, I., Lin, H. and Tian, S. (2014) Privacy-Aware Smart Metering: A Survey. *IEEE Communication Surveys and Tutorials*, **16**, 1732-1745. https://doi.org/10.1109/SURV.2014.052914.00090

[2] Elderberry: A Peer-to-Peer, Privacy-Aware Smart Metering Protocol.

[3] Shen, H. and Zhang, M. (2016) A Privacy-Preserving Multi-Level Users Electricity Consumption Aggregation and Control Scheme in Smart Grids. *Journal of Cryptologic Research*, **3**, 171-191.

[4] Quinn, E.L. (2009) Privacy and the New Energy Infrastructure. *Ssrn Electronic Journal*, 2009. https://doi.org/10.2139/ssrn.1370731

[5] Dutta, M., Singh, A.K. and Kumar, A. (2013) An Efficient Signcryption Scheme Based on ECC with Forward Secrecy and Encrypted Message Authentication. 3rd *IEEE International Advance Computing Conference*, Ghaziabad, 22-23 February 2013, 399-403. https://doi.org/10.1109/IAdCC.2013.6514258

[6] Alshinina, R. and Elleithy, K. (2015) An Efficient Message Authentication and Source Privacy with a Hidden Generator Point Based on ECC. *IEEE International Advance Computing Conference*, Farmingdale, 1-1 May 2015, 257-302. https://doi.org/10.1109/LISAT.2015.7160220

[7] Saeed, M., Mackvandi, A., Naddafiun, M. and Karimnejad, H.R. (2012) An Enhanced Password Authenticated Key Exchange Protocol without Server Public Keys.

ICTC 2012, Jeju Island, 15-17 October 2012, 87-91.
https://doi.org/10.1109/ICTC.2012.6386785

[8] Ding, X., Ma, C. and Cheng, Q. (2009) Password Authenticated Key Exchange Protocol with Stronger Security. *IEEE* 1*st International Workshop on Education Technology and Computer Science*, 2009, 678-681.

[9] Strangio, M.A. (2006) An Optimal Round Two-Party Password-Authenticated Key Agreement Protocol. *Proceeding of the* 1*st IEEE International Conference on Availability*, *Reliability*, *and Security* (*ARES*'06), Vienna, 20-22 April 2006, 216-223.
https://doi.org/10.1109/ARES.2006.29

[10] Singh, V., Dahiya, P. and Singh, S. (2014) Smart Card Based Password Authentication and User Anonymity Scheme Using ECC and Steganography. *IEEE* 2014 *International Conference on Advances in Computing*, *Communications and Informatics* (*ICACCI*), New Delhi, 24-27 September 2014, 1614-1621.
https://doi.org/10.1109/ICACCI.2014.6968403

[11] Chang, Q., Zhang, Y.P. and Qin, L.L. (2010) A Node Authentication Protocol Based on ECC in WSN. *IEEE* 2010 *International Conference on Computer Design and Applications* (*ICCDA*), Qinhuangdao, 25-27 June 2010, 606-609.
https://doi.org/10.1109/ICCDA.2010.5541288

[12] Raj, S.P. and Renold, A.P. (2015) An Enhanced Elliptic Curve Algorithm for Secured Data Transmission in Wireless Sensor Network. *IEEE* 2015 *Global Conference on Communication Technologies* (*GCCT*), Thuckalay, 23-24 April 2015.
https://doi.org/10.1109/GCCT.2015.7342790

[13] Nicanfar, H. and Leung, V.C.M. (2013) Multilayer Consensus ECC-Based Password Authenticated Key-Exchange (MCEPAK) Protocol for Smart Grid System. *IEEE Transactions on Smart Grid*, **4**,253-264. https://doi.org/10.1109/TSG.2012.2226252