A Lightweight Authentication Protocol for Smart Grid

A Lightweight Authentication Protocol for Smart Grid

Qianqian Wu[1,*] and Meihong Li [2]

[1]Computer and Information Technology Department, Beijing Jiaotong University, Beijing, China
[2]Computer and Information Technology Department, Beijing Jiaotong University, Beijing, China
16120339@bjtu.edu.cn

Abstract. Under the new situation of the "Smart Energy", with the rapid development of the smart grid, it is a key point to ensure the effective access control of devices so as to realize the information secruity of the whole system. Device access authentication is the precondition of system raliability. In this paper, a protocol for lightweight two-way device authentication of supervisory node and control node in the smart grid is proposed, based on the shared security key and random number, it authenticates the identity of both communtication parties, using the secruity key embeded in the device chip to determine the legitimacyy of the access device idenitity, avoid the use of certificates and other third-party services, effectively prevent the man-in-the-middle attack and replay attack to ensure the reliability of the system.

1 Introduction

Smart grid , the intellectualization of the traditional power, which is based on an integrated, high-speed two-way communciation network, through advanced sensing and measuring technology, progressive devices , control methods and decision support system to achieve the goal reliability, economy, safety efficiency, environment-friendly.

At present, the security of smart grid is facing tough challenges. Although smart grid has brought a lot of convenience to the soceity, improved the power market and boosted energy efficiency, there are still many inadequacies in the information acquisition of the exisiting system [1-3]. For example, many monitoring data system only focus on the collection of the device date while ignore the convinence of device management and the security of authentication. In addtion, once the smart grid is attacked by mailicious means, it will be seriously damaged and bring huge losses.

For example, in the smart grid information acquisition system, there are multiple times of communication between the smart meter and the collector. On one hand, smart meter collect all kinds of power information, including electricity, voltage, power comsumption etc., and upload them to the collector and its uplink bussiness system; on the other hand, the bussiness system issues control orders to adjust the state of the power side [4, 5]. In the communciation process. Once there is illegal device access malicious transimision of false control instructions, will lead to instability of the smart grid. Therefore, this paper analyses the problems exisiting in the current mainstreamm device authentication protocols and improves the design of the lightweight device authentication protocol is suitiable for smart meters and collectors so as to ensure the credibility of identities of communciation parties.

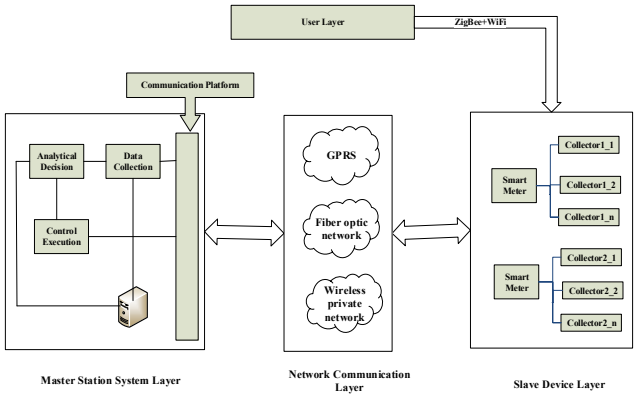

Fig. 1 Architecture of Information Acquisition System

2 Related Work

2.1 Existing Work

2.1.1 Certificate-based Authentication. At present, most authentication technologies in power grid are based on public key infrastructure (PKI). The common point is that they all run on the certificate mechanism of smard grid, which invokes third-party security services for digital signature. However, the management and update of certificates are relatively complex, which leads to relatively high computational overhead and communication costs. Several researchers haved demonstarted that the traditional certification technology will bring great load pressure to the communication system [6-8]. So certificate-based authentication not applicable to smart grids.

2.1.2 Identity-based authentication. Identity-based authentication has also been applied to smart grid. This approach also involves third-party private key generator(PKG), which uses the unique master key and user identity information of the system to calculate the user's private key and distribute it to the user. There is a small role-based smart grid security management and certification system. However, the application scope of this authentication system is limited to the power network between local regions of the host, and it can only complete the authentication of system instructions and system requests [9]. And the identity-based authentication system will not only guarantee the security of the system but also avoid the management and update of certificates, which will bring huge cost, so as to effectively reduce the load pressure of the system and have a very broad application prospect [10]. On this basis, a specific identity-based sign-secret scheme, which realizes end-to-end mutual authentication in smart grid and can effectively reduce system overhead [11]. Although compared with certificate-based device authentication, this method does not need to store and transmit digital certificates and verify the validity of certificates, it is also not suitable for smart grid information acquisition system.

2.1.3 Design principles. Devices such as sensors, RFIDs in the smart grid have the characteristics of small size, low price, limited resources and a large number of deployments, but their computing capacity is relatively weak and resources are limited.
Based on the above characteristics of smart grid, the device authentication protocol designed in this paper requires sufficient lightweight, that is, in the process of equipment certification [12-15], the following principles should be met:

- In the process of device authentication, the third-party services should be invoked as little as possible to reduce the uncertain risks brought by the security problems of the third party to the smart grid;
- Considering the processing capacity of communication equipment for security algorithm, under the condition of limited computing capacity of the terminal equipment, the algorithm is required

to be simple, the execution speed is fast, consume less computing resources, and avoid involving complex operations such as large primenumbers and exponents;

- The communication process of equipment certification should be as simple as possible, with as few times as possible, and the burden of communication link should be reduced.

3 Proposed Scheme

This paper analyzes the information acquisition system of smart grid and proposes a device authentication protocol. The specific pattern is shown in the figure below. In this scheme, only the supservisory node (*SN*) such as smart meter and the collector node (*CN*) such as collector are involved, and no third party is involved, a symmetric cryptographic algorithm with a fast calculation speed and a simple hash operation are adopted. The core is to use the challenge response protocol to prove that the entity is its declared identity, use the random number as the challenge code, use the shared key to encrypt the random number and other identity-representing information and abstract to ensure the confidentiality of the data.

3.1 Parameter Description

Table 1. Symbols and abbreviations.

Symblol	Description
SN	supservisory node ,such as smart meter etc.
CN	collector node, such as collector etc.
ID_s / ID_c	the physical number or address of the *SN/CN*
IP_s / IP_c	IP address of *SN/CN*
N_s / N_c	The random number of *SN/CN*
$K_{(s,c)} / K_{(c,s)}$	Shared security key of *SN/CN*
MAC_s / MAC_c	A message digest calculated using a simple Hash

3.2 System Initialization

The security of devices certification depends on the shared key. In the smart grid, the distribution of *SN* and *CN* is relatively uniform. Generally, the number of *SN* corresponding to *CN* is limited, and the topology is basically stable and the network structure is simple and unified.Therefore, in this method, a dedicated chip is added to both the *SN* and *CN* for securely storing the shared key.

The chip is solidified in the device, has special agencies to manage, produce and distribute, doesn't receive system internal threats, is not violenty extracted, and is completed controlled. Each device before access system, need a shared secret key, and the complete exchange of the key is completed throught physical channel. Before both sides communication, a shared key has been synchronized in place.

In addition, both *SN* and *CN* have a dedicated space security storage corresponding list $<ID_s, IP_s>$,$<IDc, IP_c>$,$<ID_s, K_{(s,c)}>$,$<ID_c, K_{(c,s)}>$ of communication devices, and the corresponding identification of the device can be found directly and quickly through *IP* address. When the smart meter is connected to the system, it already knows the address of the connected collector, so the list is initialized when the device is connected.

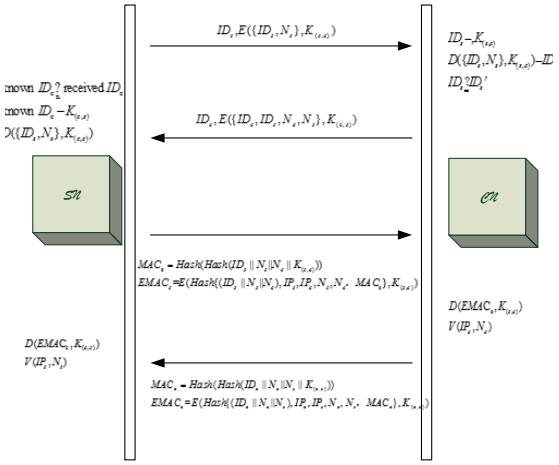

Fig. 2. Device Authentication Scheme

3.3 Legitimate Certification of Device

The security goal of the protocol is to complete the identity verification of both parties to the communication, prevent the access of illegal devices, and ensure the availability of the system. The protocol is initiated by the newly added device terminal and is mainly divided into two parts, namely random number generation and identity authentication. Specific steps are as follows:

- *SN* sends a request to *CN*. *SN* generates a random number N_s by itself. The request includes: $ID_s, E(\{ID_s, N_s\}, K_{(s,c)})$;
- After receiving the message ID_s, the *CN* looks up and extracts the corresponding shared key $K_{(s,c)}$ from the local chip according to the message. If it does not exist, the message is invalid. Otherwise, the decrypted message is obtained $\{ID_s, N_s\}$ and compared with the decrypted one ID_s, if it is consistent, then proceed to the next step; other wise, authentication fails;
- The *CN* generates a random numbers N_c, using the shared key $K_{(c,s)}$ to encrypt the device identification and random numbers of both parties, then sends the response $ID_c, E(\{ID_c, ID_s, N_c, N_s\}, K_{(c,s)})$;
- *SN* receives the message, then extracts the corresponding shared key $K_{(c,s)}$ in the local chip, and decrypts the data to get the messag including ID_c, ID_s, N_c, N_s;
- The *SN* needs to further verify its identity to *CN* and return random Numbers N_c and relevant identity information $E(Hash\{(ID_s \| N_s \| N_c), IP_s, IP_c, N_s, N_c, MAC_s\}, K_{(s,c)})$, the message digest integrated with the shared key MAC_s,the $MAC_s = Hash(Hash(ID_s \| N_s \| N_c \| K_{(s,c)}))$;
- The *CN* using the shared secret $K_{(s,c)}$ decrypts the date packets. First, the data is spliced and shared by the data other than MAC_s after decryption, and the message digest is calculated, checking the integrity of the data, and then to check IP_c and N_c, according to random number N_s and device identifier ID_s obtained in the step a), validation N_s and IP_s,calculate $Hash(ID_s \| N_s \| N_c)$. Next to compare their consistency, if the verification pass, proceed to the next step to the next step, otherwise, the authentication fails;
- This process is basically the same as step e), except that the subject changes from *SN* to *CN*.
- This process is basically the same as step f), except that the subject changes from *CN* to *SN*.

3.4 Update the Device Key

Security keys are embedded chip embedded device chip. After the device authentication is passed, it becomes the initial key for the communication data transmission. Device key update cycle can be defined by oneself, assuming that authentication key update once a month, after the last communication each month, the current data is encrypted, the key is written back to the device chip and it will be changed. In the subsequent devie certification process, the new key can be used for communication.

4 Safety Analysis

4.1 Functional Safety

4.1.1 Defend Against Man-in-the-middle Attacks. The key pair corresponds to the device one by one, and is embedded in the device system, aiming at the manin attack: since the information of the authentication process is encrypted by using the shared key and then tramsitted, the identification *ID* and random number cannot be decrypted or tampered with, the second one cannot be changed even if the first one is changed.

4.1.2 Resists Replay Attacks. The protocol uses random numbers to complete the inquiry and reponse. In the first four steps of device legitimacy authentication, both parties complete the safe exchange of random Numbers by sharing keys to prevent replay attacks in the subsequent authentication process. For replay attack: each device authentication will generate a new random number, which ensures that the random number used in each session is different.Even if the attacker had captured the session content, such as the session for random number exchange, replay it to the server, and the server decrypts it and finds that the random number has been used before, the authentication fails.Time stamps can also be used to prevent replay attacks, but random Numbers are used because of the high requirements on their hardware devices.

4.1.3 Ensure Data Integrity. Both MAC_s and MAC_c message digests are used to ensure the integrity of the data. The complex calculation is not involved, the calculation speed is fast, and the message is effectively prevented from being maliciously tampered. The message incorporates the shared keys $K_{(s,c)}$ and $K_{(s,c)}$, effectively preventing the offline collision of the digest algorithm, only the device holding the valid key can calculate the digest, further enhancing the security of the system.

4.2 Performance Safety

4.2.1 Symmetric Cipher Algorithm. In terms of data confidentiality, the protocol uses sym-metric cryptographic algorithm, which is computationally efficient and suitable for grid system with high real-time requirements.At the same time, about the key manage-ment problem in symmetric cryptography algorithm, the shared key designed by this protocol is embedded in the device chip, and there is no internal attack or force cracking, so there is no risk of key leakage.

4.2.2 Simple one-way hash. In terms of guarantee data integrity, protocol uses a simple one-way hash, and imcoporates key information to solve the offline collision problem of the hash algo-rithm, while avoiding the HMAC key preprocessing and pattern string of initialization and two rounds of the hash computation, significantly improve the computing speed of the message digest and efficiency of the authentica-tion.

In conclusion, the device in the process of the au-thentication protocol, only the symmetric cryptographic algorithm and the digest algorithm need to be excuted as well as two random numbers, which reduces the band-width requirement for communication network, reduces the computing to the both sides of communication, on the whole to reduce the complexity of device authentica-tion protocol implementation, simplify the key manage-ment, reduce the equipment calculation of pressure and resource consumption, more suitable for smart grid.

5 Summarize

What is proposed in this paper is suitable for smart grid information acquisition system of lightweight two-way authentication protocol, protocol based on shared security keys and the random number to com-municate both sides authentication, use of chip embed-ded device security keys to determine the legitimacy of access devices status, avoid to use certificates and other third-party services, effectively prevent man-in-the-middle attack and replay attack to ensure the reliability of the system.Finally, the paper analyzes the proposed scheme from the two aspects of functional safety and performance safety.

The analysis shows that this scheme can achieve the purpose of effective certifi-cation and improve the certification security of smart grid.

6 References

[1] Lu Z, Lu X, Wang W, et al. Review and evaluation of security threats on the communication networks in the smart grid. C. *Military Communications Conference*. (2010).
[2] H. Khurana, et al. Smart-Grid Security Issues: *IEEE Security & Privacy*, **8** (2010), pp.81-85.
[3] Mcdaniel P, Mclaughlin S. Security and Privacy Challenges in the Smart Grid. J.
[4] *IEEE Security & Privacy*, **7(3)** (2009):75-77.
[5] Barenghi A, Pelosi G. Security and Privacy in Smart Grid Infrastructures. C. *International Workshop on Database & Expert Systems Applications*. IEEE, (2012).
[6] Setiawan A B, Syamsudin A, Rosmansyah Y. Assessment of information technology security governance for Supervisory Control and Data Acquisition (SCADA) on the Smart Grid electricity. C. *International Conference on Information Technology Systems & Innovation*. IEEE, (2016).
[7] Lee S, Bong J, Shin S, et al. A security mechanism of Smart Grid AMI network through smart device mutual authentication. C. *International Conference on Information Networking*. (2014):592-595.
[8] Zhang L, Tang S, Jiang Y, et al. Robust and Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Smart Grids. C. *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing. IEEE,* (2013): 2089-2093.
[9] Sha K, Alatrash N, Wang Z. A Secure and Efficient Framework to Read Isolated Smart Grid Devices. J. IEEE Transactions on Smart Grid, (2016):1-13.
[10] Fouda M M, Fadlullah Z M, Kato N, et al. A Lightweight Message Authentication Scheme for Smart Grid Communications. J. IEEE Transactions on Smart Grid, **2(4)** (2011):675-685.
[11] MAO W B. An identity-based non-interactive authentication framework for computational girds. R. Hewlett –Packard Laboratories, Technical Report HPL-(2004)-96.
[12] So H K H , Kwok S H M , Lam E Y , et al. Zero-Configuration Identity-Based Signcryption Scheme for Smart Grid. C. *International Conference on Smart Grid Communications*. IEEE, 2010.
[13] Hamlyn A, Cheung H, Mander T, et al. Network Security Management and Authentication of Actions for Smart Grids Operations. C. *Electrical Power Conference*, 2007. EPC 2007. IEEsE Canada. IEEE, (2008):31-36.
[14] Asmaa R. Abdallah, Xuemin Sherman Shen, A lightweight lattice-based security and privacy-preserving scheme for smart grid. *Global Communications Conference IEEE*, pp. 668-674, (2014).
[15] Nicanfar H, Jokar P, Beznosov K, et al. Efficient Authentication and Key Management Mechanisms for Smart Grid Communications. J. Systems Journal IEEE, **8(2)** (2014): 629-640.
[16] Paverd A J, Martin A P. Hardware Security for Device Authentication in the Smart Grid. M. Smart Grid Security. Springer Berlin Heidelberg, (2012):72-84.
[17] Ayday E, Rajagopal S. Secure, intuitive and low-cost device authentication for Smart Grid networks. C. Consumer Communications and NETWORKING Conference. IEEE, (2011):1161-1165.