International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.337-346
http://dx.doi.org/10.14257/ijsia.2015.9.7.31

Security Authentication Method of Terminal Trusted Access in Smart Grid

Yufeng Wang[1, a], Lie Wu[2, b] and Yun Yang[2, c]

*[1]State Grid Chongqing Electric Power Company Urban Power Supply Branch
Chongqing 400015, China*

[2]Dept. of Science & Information System, State Grid Chongqing Electric Power Company, Chongqing 400015, China

[a]yufengwangcq@163.com; [b]wuliely@163.com; [c]yangyunly@163.com

Abstract

A security authentication method in smart grid terminal is proposed in this paper. This method layers the terminal authentication system structure of smart grid so as to improve the simplicity and extensibility on system deployment and realize flexible communication mechanism and the interaction mechanism among systems. This paper aims at preventing terminal information from being destroyed and achieving terminal verification integrity. Besides, this kind of authentication method has no special requirements for terminal users.

Keywords: *Smart grid, Security authentication, Terminal trusted access*

1. Introduction

As a branch of the Internet of Things, smart grid is an important public application network. Smart grid delivers electricity between suppliers and consumers using two-way digital technology to control intelligent appliances at consumers' home or building to save energy, reduce cost and increase reliability, efficiency, and transparency [1-2]. In recent years, energy shortages, environmental pressures, and large-scale grid make the safe operation of existing power grid and power system operation model suffer from serious challenges. Thus, smart grid comes to the world. Smart grid is based on various physical powers such as generation equipment, electrical transmission, distribution networks, electrical equipment, and storage devices, which could combine with modern advanced sensor measurement technology, network technology, communication technology, computing technology, automation, and smart control technology and then build a new network. Smart grid trust access terminal authentication system is connected to an external network of smart grid’s first protective wall, by which it can control the user access to smart grid, and protect the identity of the trust access, access to safe process. Smart grid is not only a novel solution for the problems of four major aspects in power generation, transmission and distribution and consumption, but also the important application of the Internet of Things.

In order to solve the imbalance between the energy supply and the energy consumption structure and achieve sustainable development grid, smart grid research and practice aim at achieving the development of wind, solar and other renewable energy and large-scale utilization, and upgrading the utilization rate of traditional energy sources clean and efficient. smart grid technology has the application characteristics of informatization, automatization, and interaction, which can effectively address some of the existed shortcomings of traditional grid, especially the security, reliability, system operation and maintenance costs and other difficulties in the traditional grid. For historical problems in the traditional power grid, smart grid is designed to achieve the goal of reliability, safety, economic, efficiency, and environmentally friendly characteristics of grid, and achieve the smart interaction , generation, transmission, and distribution of electricity smart grid users.

With operation of the grid, service model will be a significant change, such as the significant increase in information and data interaction, smart terminal access growing, all of these changes are bound to introduce new security risks and challenges. So how to solve the smart grid trusted access terminal authentication has become a more and more important issue for the development of smart grid that needs to be solved. If it is unable to realize the smart grid trusted access, terminal will effectively influence the development of the smart grid, and may even lead to termination of the development of the smart grid. As traditional trusted access authentication method is only suitable for small simple network system, which is applied directly to the smart grid may cause the following problems:

An open radio channel characteristic makes smart grid easily be monitored, which result in the consequence that network information in the data transfer process is easy to be stolen, and the malicious attacker can steal information. As the increasing number of users, taking traditional authentication methods , may lead to authentication system collapse, but also may make the user authentication process slow, resulting in the accumulation of excessive users of the system so that users can not normally certified access to the smart grid.

Traditional terminal authentication may directly collect information to authenticate the legitimacy of the user, which may cause that the information will be tampered in the transmission process before arriving the authentication server, and bring the disclosure of user information, which affects the credibility, reliability and safety of the system.

Currently , there is a trusted access technology that can be implemented on the smart grid trusted authentication access terminal, however, because of their excessive system components, system level complexity and lack of reliable and scalable system, which cause the whole access authentication process becomes complex, slow, and also unable to meet the requirements of fast authentication access to a large amount of users of the smart grid , and at the same time, the credibility of its huge access technology system structure make the deployment of the system unable to achieve the requirements of precise and intelligence, which leads to the smart grid becoming an arrested development. So it is necessary to propose a compact, reliable, and secure access to the new certification system to meet the needs of the future smart grid development, while improving the convenience, security of smart grid users.

2. Network Model, Security Threats and Requirements of Smart Grid

2.1. Network Model of Smart Grid

Smart grid is a new type of power network consisting of modern advanced sensing measurement technology, communication technology, information technology, computer technology and control technology and physical power network [3-5]. There are many security problems about smart grid, which conclude access control, authentication, non-repudiation, data confidentiality and data integrity [6-10]. A terminal security authentication method in smart grid is proposed in this paper. The structure of smart grid is shown in Figure 1. Smart gird improves the equipment utilization under the circumstance of ensuring its security stability and reliability and realizes the interaction between electricity generation and electricity utilization, as well as intermittent renewable energy access, so smart grid needs to solve many aspects of problems about information collection and information transmission, which are managed through the gradually developing IOT (Internet of Things) [11-13]. In the smart grid, power resource contains intranet and extranet, the terminal of electricity power belongs to extranet, and there are security isolation devices between intranet and extranet, for instance, firewall, intrusion detection system, security service gateway and so on. However, terminal users of smart grid need to communication with others via wireless internet and access to intranet, terminal of smart gird may be invaded in malicious programs or execute other rogue programs so that it will cause serious security threats.

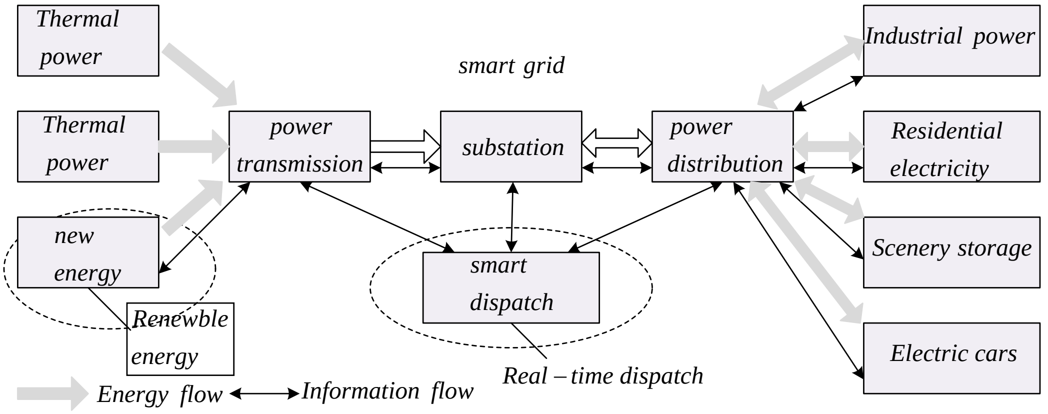

Figure 1. The Structure of Smart Grid

2.2. Security Threats of Smart Grid

The terminal of smart grid faces with many kinds of security risks, which are not solved yet. These security risks mainly display in following four aspects:

Login system of terminal users, the jurisdiction that users access to data relies on traditional password identification mechanism which can be easily broken by attackers, the lack of strong authentication methods leads to terminal can be illegally used by others.

The diversity of terminal accessing to network increases the possibility of intranet information in electric power communication system is stolen maliciously and the attackers can tamper with the important information which bring about system security risks.

The heterogeneity between the user terminal and the access network, the reuse of the storage space of power system and the sharing of the resources reduce the ability to examine the users' behaviors.

Smart grid which is accessed by attackers illegally and attacked deliberately will be a serious threat to the safety operation of electric power communication network and affect the safe and stable operation of power system.

2.3. Requirements Analysis of Smart Grid

In order to overcome existing security holes in smart grid and minimize the security threats, it is necessary to develop a series of security strategy to ensure business application safe and reliable [14-18]. Combining the terminal business scene and safe protection requirements, the following are some terminal requirements of smart grid.

Terminal of smart grid should takes measures to realize the integrity authentication of key components as also as system codes, thus ensuring a safe and reliable environment.

Terminal of smart grid should make perfect safe control strategy and domain isolation strategy, which can realize identification authentication of users, access control of program and reliable communication among programs.

Users' terminals should sort and store the data and documents according to sensitivity of data and take different security measures for data and documents in different levels. At the same time, users terminals should define more perfect security-audit strategy to help find existing potential security risks and security incidents.

Terminal of smart grid should offer self-destruct mechanism after missing data, such as remote information lock and information destruction mechanism, thus clearing sensitive information and preventing sensitive data from leakage.

3. The Security Authentication Method of Smart Grid

It is provided that an smart grid trusted access terminal authentication method in this paper, which manages the users information comprehensively through information processing system(a small and efficient embedded computing systems) after receiving terminal users information, and then transmits information to the terminal trusted access authentication server, through which can we realize security and reliability in the process of information transmission in network and ensure more simple and transplantable system about trusted access in smart grid.

3.1. The Structure of Terminal Trusted Access System in Smart Grid

According to hierarchy deployment body area network system, the top layer is the information collection layer (ICL), followed by information processing layer (IPL), finally, message authentication layer (IAL). The message authentication layer wants to access the information collection layer terminal information collection to send the information to the information processing layer , after processing layer , the processing information is integrated, and ultimately transmitted to the information layer of authentication , the authentication information in the layer will complete the authentication , as shown in Figure 2 , the specific steps:

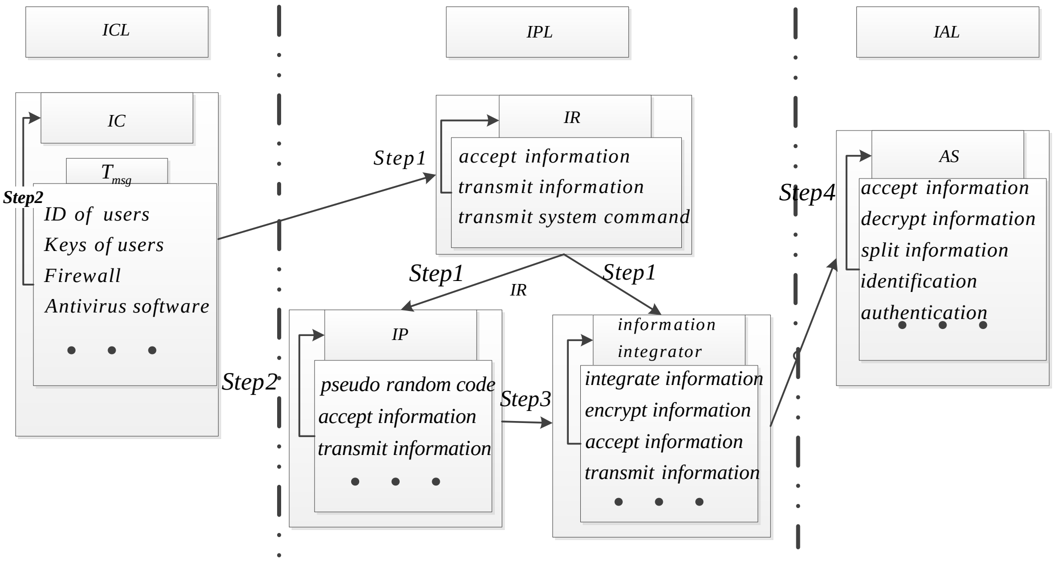

Figure 2. The Structure of Terminal Authentication System in Smart Grid

Step 1: According to the hierarchy in the deployment of smart grid terminal authentication systems, authentication systems respectively include information collection layer (ICL), the information processing layer (IPL) and information authentication layer (IAL). The information collection layer connects with the information processing layer and the processing layer connects with the message authentication layer;

Step 2: The information collection layer collects and sends the received information to the information collection processing layer.

Step 3: The information processing layer seals off, processes and encrypts the terminal information, eventually transmits the processed data to the information authentication layer.

Step 4: The information authentication layer decrypts, restores and verifies the received data to complete the authentication.

Information collector includes collecting terminal information and verifying the validity of the terminal information. The information processing layer includes information receiver, information generation and information consolidator, and each of them completes the function of message receiving, transmitting, processing, encrypting and integrating. The information authentication layer consists of authentication server, which can decompile the processed information and restore the original information, while completing a trusted authentication access.

3.2. The Information Collection Layer

Terminal information is collected by the information collection layer, and specific process is shown as Figure 3. The steps of information collection layer collecting the terminal information and transmitting it to the information processing layers are shown as below:

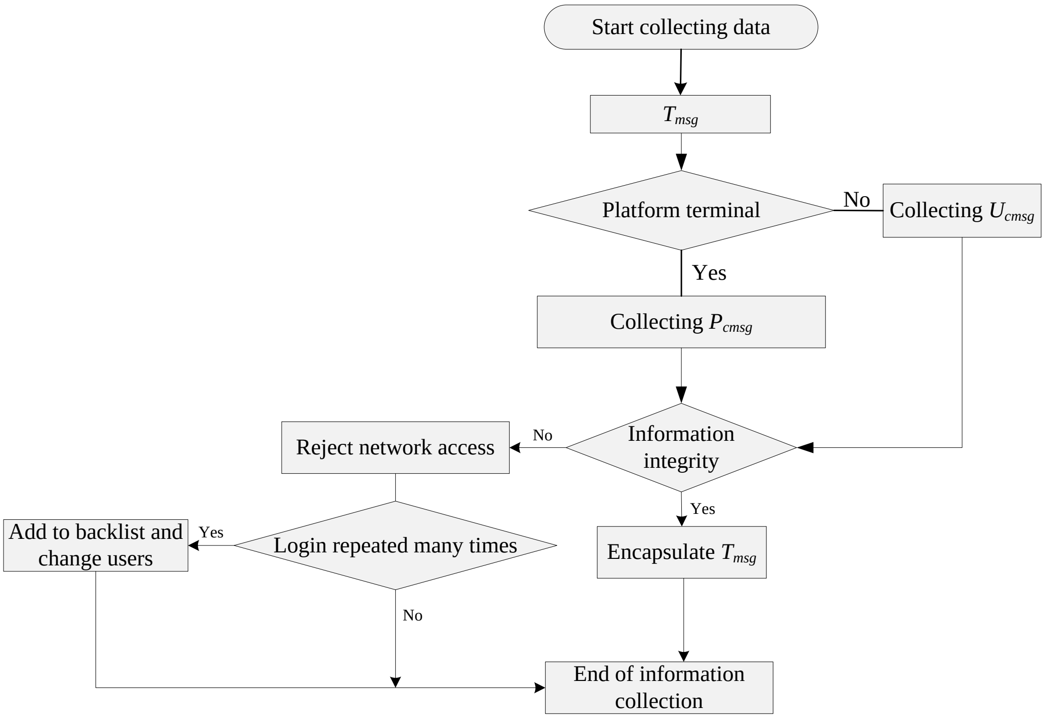

Figure 3. The Procedure of Information Collection in ICL

Step 1 : The terminal receives input information and checks its form.

Step 2 : Collecting different information according to different users input information, if it is accessed by platform terminal, then gathering its security information, including whether the firewall is opened and whether the specified anti-virus software is installed, etc.

Step3: Encapsulate those collected information into U_{cmsg} (user terminal information) or P_{cmsg} (platform terminal information), and then send it to the information processing layer.

Method for information collector to check user input information is: comparing it with the valid format, If the information is invalid, then saving the input time stamps and increasing the error flag (MF) AUTO. After that, checking the increments of error flag(MF) in two consecutive time stamps, once it is greater than the certain value, lock the user, otherwise the authentication is passed, then empty time stamps and reset the error flag(return MF to zero).

Method for locking the user: If the user authentication continuously fails in a short time, we will add the user into blacklist which will always be traversed before authentication. If the current user's information is found in blacklist, it will be refused. In addition, the files in blacklist will be reorganized regularly.

Method for reorganizing blacklist: A time stamp will be added when the new user authentication information is put in blacklist. Meanwhile, system will compare the time stamps saved in blacklist when information collector checks the time stamp in every hour or when accessed by a new terminal. If the time interval equals 24 hours or even more, delete this user' s information from blacklist, i.e. unlock the user.

The main job for information collection layer is to collect the terminal information. However, in order to enhance the robustness of system security, the information should pass some simple integrity test. The invalid or malicious attacks information are not allowed to access the system, and the terminal which submits invalid information will be put under monitor for preventing the system from continuous and high strength attack.

3.3. The Information Processing Layer

After packaging information from information collection layer received by information processing layer, it will have a further handling before information is sent to the information authentication layer for authentication. The procedures are shown in Figure 4, that is to say that unpack, process and encrypt U_{cmsg} or P_{cmsg} .Then, the processed information PD_{msg} is sent to the information authentication layer. The following shows the specific steps:

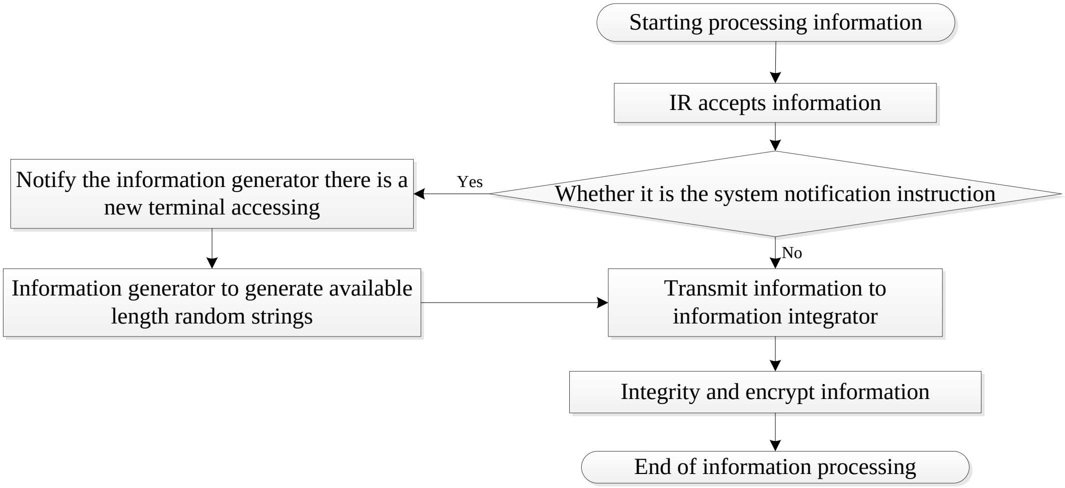
Starting processing information
IR accepts information
Whether it is the system notification instruction
Yes
Notify the information generator there is a new terminal accessing
Information generator to generate available length random strings
No
Transmit information to information integrator
Integrity and encrypt information
End of information processing

Figure 4. The Procedure of Information Processing in IPL

Step1 : The information acceptor in information processing layer is used to accept the terminal information, and inform the information generator that there is a new terminal wanting to access. At the same time, then sending received terminal information to the Information Integrator.

Step2: After the information generator received the notice, it parallelly produces a indefinite length random number $Vlrn$, then sends both of them to the information integrator and information authentication layer.

Step3: When the information integrator receives the terminal information, it will split the information into two sections, and wait for $Vlrn$ made by information generator.

Finally, combine $Vlrn$ with the terminal information and sent them to information authentication layer after encryption.

Method for information generator to produce indefinite length random number $Vlrn$ is that after receiving terminal access notice, three computational components work in parallel to produce three random strings($Vlrn1, Vlrn2$ and $Vlrn3$), which are no more than 128 bin long and consist of capital and lower-case letters, numbers and marks. Then it packages these three strings into a reducible completely string $Vlrn$, then send $Vlrn$ to information authentication layer and information integrator.

Method for information integrator to compose the final information is that it splits the terminal information into two parts, and packages it with the above three random strings($Vlrn1, Vlrn2$ and $Vlrn3$) orderly into a PD_{msg} . Then encrypt it by using the public key $K_p\{PD_{msg}\} = K_p\{Vlrn1, F_{msg}, Vlrn2, L_{msg}, Vlrn3\}$ before send it to the information authentication layer.

Method for information generator to produce the random string is that using the time stamp to produce a random number no more than 128bin, and picking up characters according to the number of the random number, then splicing them into a completely string, thus creating a group of strings ($Vlrn1$、 $Vlrn2$ and $Vlrn3$), which are no more than 128 bin and consist of capital letters, lower-case letters, numbers and marks.

3.4. The Information Authentication Layer

Information authentication layer will conduct a series of de-compilation on the received information to restore it, and then authenticate it, and the flow chart is shown on Figure 5. The steps of information authentication layer to decrypt, restore, verify, and finally complete the terminal access authentication is:

Step1: The authenticator will receive both $Vlrn$, which is produced by information generator and the encrypted information, which is sent by information integrator.

Step2: Decrypting the processed information and splitting it according to $Vlrn$ to restore the terminal information.

Step3: Validate the terminal information to implement the trusted access by comparing it with the information which stored in the server.

This method restores the real user information by recompiling the processed information which are processed by the information processing layer, meanwhile, applies senior authentication to improve the efficiency and safety of access authentication.

Method for authentication server to restore the terminal information is to decrypt the received processed information by using the public key firstly, thus getting the synthesized information PD_{msg} . Then, splitting PD_{msg} into five parts, including three parts of $Vlrn$ and two parts of terminal information, according received $Vlrn$, and the latter two parts will be restored to the terminal information T_{msg} .

After getting the terminal information, compare it with information from the server database. If it exists, success for authentication, else fail.

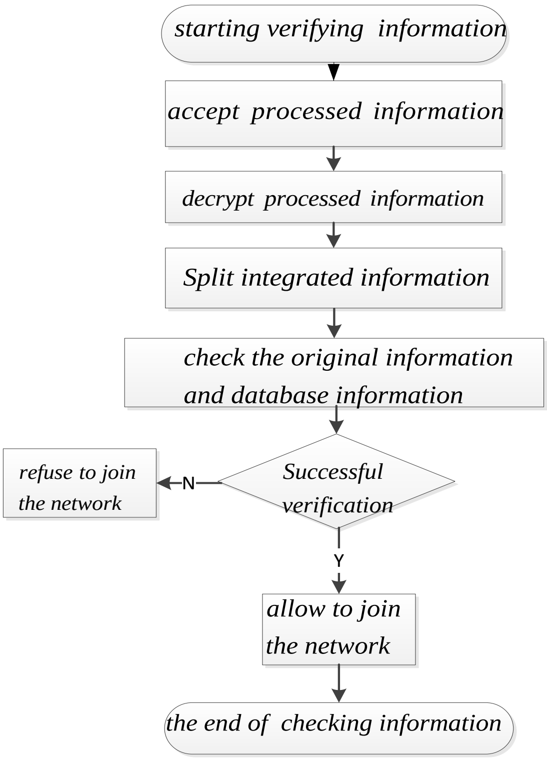
starting verifying information
accept processed information
decrypt processed information
Split integrated information
check the original information and database information
Successful verification
N
refuse to join the network
Y
allow to join the network
the end of checking information

Figure 5. The Procedure of Information Verification in IAL

4. Conclusions

A simple and efficient way is used to deal with the user's information in this paper according to characters of users and features of data, then users' information is transmitted to the network to protect the security of users' information in the process of network transmission and achieve the credit of smart grid on terminal access authentication process. It is easy to set up and deploy system because of the hierarchical structure, while making clear division of power system and improving the computational rate of the system.

Acknowledgements

This work is supported by the science and technology projects of Chongqing electric power company, China (An Application Research of Storage Virtualization Platform Based on Open Source, NO. 5220271400CK), the National Natural Science Foundation (Grant No. 61309032).

References

[1] B. Yang, X. Niu and S. Jia, “Applications of communication technology in smart grid”, Proceedings of 2013 4th International Conference on Digital Manufacturing and Automation, (**2013**), pp. 308-310.

[2] J. Liu, Y. Xiao and J. Gao, “Achieving accountability in smart grid”, IEEE Systems Journal, vol. 8, no. 2, (**2014**), pp. 493-508.

[3] X. Miao, K. Zhang, X. Chen, X. Zhang, S.-b. Sun, G.-l. Wu, Z.-m. Zhou and S.-m. Tian, “Development countermeasure of constructing smart grid”, Electric Power Construction, vol. 30, no. 6, (**2009**), pp. 6-10.

[4] S. Chen, S. Song, L. Li and J. Shen, “Survey on smart grid technology”, Power System Technology, vol. 33, no. 8, (**2009**), pp. 1-7.

[5] B. Falahati, Y. Fu and L. Wu, “Reliability assessment of smart grid considering direct cyber-power interdependencies”, IEEE Transactions on Smart Grid, vol. 3, no. 3, (**2012**), pp. 1515-1524.

[6] L. Wei, “Network security and key technology”, World Telecommunications, vol. 17, no. 3, (**2004**), pp. 28-32.

[7] D. Ding, "Electric power and communications system vulnerability and basic concept of strategic power infrastructure defense (SPID) system", Electric Power, vol. 37, no. 8, (**2004**), pp. 1-6.

[8] J. W. Cao and Y. X. Wan, "Information system architecture for smart grids", Chinese Journal of Computers, vol. 36, no. 1, (**2013**), pp. 143-167.

[9] J. J. Wu and M. W. Fang, "Trusted anonymous authentication scheme for trusted network connection in mobile environment", Journal of Networks, vol. 7, no. 9, (**2012**), pp. 1341-1348.

[10] S. Deng, W. M. Lin and T. Zhang, "Research on security access of power terminal based on trusted network connection", Telecommunications for Electric Power System, vol. 33, no. 231, (**2012**), pp. 78-81.

[11] Y. Lin, J. Zhong and F. Wu, "Discussion on smart grid supporting technologies", Power System Technology, vol. 33, no. 12, (**2009**), pp. 8-14.

[12] X. Hu, "Smart grid-A development trend of future power grid", Power System Technology, vol. 33, no. 14, (**2009**), pp. 1-5.

[13] W. L. Zhang, Z. Z. Liu and MingJun Wang, "Research status and development trend of smart grid", Power System Technology, vol. 33, no. 13, (**2009**), pp. 1-11.

[14] Mohammad Fathi, Vafa Maihami, Parham Moradi, "Reinforcement learning for multiple access control in wireless sensor networks: Review, model, and open issues", Wireless Personal Communications, vol. 72, no. 1, (**2013**), pp. 535-547.

[15] Ping Guo, Jin Wang, Jie Zhong Zhu, Ya Ping Cheng, Jeong-Uk Kim, "Construction of trusted wireless sensor networks with lightweight bilateral authentication", International Journal of Security and its Applications, vol. 7, no. 5, (**2013**), pp. 225-236.

[16] Zhuo Ma, Jianfeng Ma, Sangjae Moon, Xinghua Li, "An efficient authentication protocol for WLAN mesh networks in trusted environment", IEICE Transactions on Information and Systems, vol. E93-D, no. 3, (**2010**), pp. 430-437.

[17] Ayman Tajeddine, Ayman Kayssi, Ali Chehab, Imad Elhajj, Wassim Itani, "CENTERA: A centralized trust-based efficient routing protocol with authentication for wireless sensor networks", Sensors, vol. 15, no. 2, (**2015**), pp. 3299-3333.

[18] Anish Prasad Shrestha, Dong-You Choi, Goo Rak Kwon, Seung-Jo Han, "Kerberos based authentication for inter-domain roaming in wireless heterogeneous network", Computers and Mathematics with Applications, vol. 60, no. 2, (**2010**), pp. 245-255.

Authors

Yufeng Wang, He was born in 1978 in Sichuan, China. He received the Bachelor's degree in Computer Science in 2000 from Southwest China Normal University, China. His research interests include information security management, network and information security, and the security of electric power system.

Lie Wu, He was born in 1982 in Chongqing, China. He received the Bachelor's degree in Computer network in 2009 from Chongqing University, China. His research interests include the information security of electric power system, the reliability of the smart grid, and network and information security.

Yun Yang, He was born in 1964 in Shanghai, China. He received the Master's degree in Master of Business Administration in 2009 from Chongqing University, China. His research interests include the information security of electric power system, the reliability of the smart grid, and network and information security, information security management.