LUO YONGMEI
WANG YING
and
LI GEN

Research of a new security mechanism on energy internet

The sustainable exploitation and utilization of new energy is the basis of future development of mankind. As the core infrastructure for the efficient and secure utilization of renewable energy sources, the energy internet is an important strategic resource and an embodiment of the comprehensive national strength. This paper presents a new security mechanism based on Trusted Platform Module (TPM). Fistly, the analysis of the structure of the energy internet is discribed from two aspects of logic structure and network topological structure. Sencondly the existing research methods of energy internet security are divided into three classes: security demand-driven method, security model-driven method and system-theoretic method. The vulnerability of isolated research and lack of integrated solution is found out. Then the new security mechanism is propossed and the security model along with the consuming layer protocol are put forward. Finally the security analysis is processed. The results show that the new security mechanism can satisfy the security requirements of energy internet.

Keywords: Energy internet, trusted platform module, security mechanism, technique for order preference by similarity to ideal solution, trusted computing.

1.0 Introduction

Since the second industrial revolution in 19th century, productive forces of human society have developed speedily. However, the over-reliance on fossil caused fuels energy depletion, environmental pollution and other economic and social problems to continuously ferment. In this context, countries around the world are committed to renewable energy development, and actively combine it with the internet and other information technologies to realize efficient, secure and sustainable energy development, namely, energy Internet [1].

The idea of energy internet was first proposed in the book of "The third industrial revolution". Subsequently, the definition of the energy internet, network architecture and system composition are constantly enriched and improved by domestic and foreign scholars [2-4]. It is generally recognized in academia currently that the energy internet is a complex network system with smart grid as the core, new energy technology and information technology as the base, multi-energy networks (natural gas network, wind power network, etc.), transportation networks and information networks deeply integrated.

Under the current circumstances, information security and internet security have become extremely important strategic resources involved with national and social stability [5]. As the core infrastructure of new energy's sustainable development and utilization, energy internet is considered to be an extension of internet, as well as a complex merging with internet and other networks, thus its safety should be taken seriously and guaranteed [2]. However, the concept of the energy internet has just occurred and the related researches have just started, and studies on security are mainly concentrating on the smart grid. It should be noticed that the energy internet is the integration of the energy grid, transportation networks, natural gas networks, and other multi-network systems. As a result, its security is more complex than the smart grid, and existing researches are relatively few. Therefore, security of energy internet, the complex information and physical systems, remain to be further systematically studied.

In this paper, based on the analysis and summary of existing research results in related fields, current network mechanisms of energy internet are analyzed, and energy internet security along with available research works are classified. Subsequently TOPSIS method is exploited to probe security weaknesses and sabotages. Considering the characteristics of isolated and lack of integrated solutions, a new security mechanism based on Trusted Platform Module (TPM) is presented, and the model of the architecture and protocols are analyzed in detail.

2.0 A TPM-based security mechanism

2.1 The energy internet architecture

At present, governments and major research institutes

Blind peer reviews carried out

Messrs. Luo Yongmei, School of Computer Science and Technology, Tianjin University, Wang Ying, Troops 61660, and Li Gen, School of Electronic Information Engineering, Tianjin University, Tianjin 300072, China. E-mail: luoyongmei@tju.edu.cn / 18601193896@163.com / ligen@ tju.edu.cn

provide powerful support on research of the energy internet, for instance, the EU's future smart energy internet project, the German E-Energy programme, America's future renewable energy transmission and management projects and Beijing Yanqing energy internet demonstration [7]. The above-mentioned studies are analyzed and comparatively reviewed in literature [3, 7].

The energy internet was evolved from smart grid, and its system components and architecture also take smart grid for reference. A typical energy internet consists of five layers viewed from logical level: energy layer, routing layer, transport layer, control layer and consumption layer, as is shown in Fig.1.

Wherein energy layer realizes the distributed production of traditional fossil energy sources and a variety of renewable energy sources, including coal, wind, natural gas and solar energy; Routing layer employs routers [7] to achieve energy conversion and storage. Transport layer achieves large-scale long-distance transmission of energy as well as near-the-end energy consumption distribution by a variety of energy networks, as illustrated by high-voltage transmission lines and low-voltage distribution box. Consumer layer realizes the function of personal and company's energy trading, electric vehicle charging, etc. Control layer monitors and controls the entire energy internet via communication networks, such as SCADA systems.

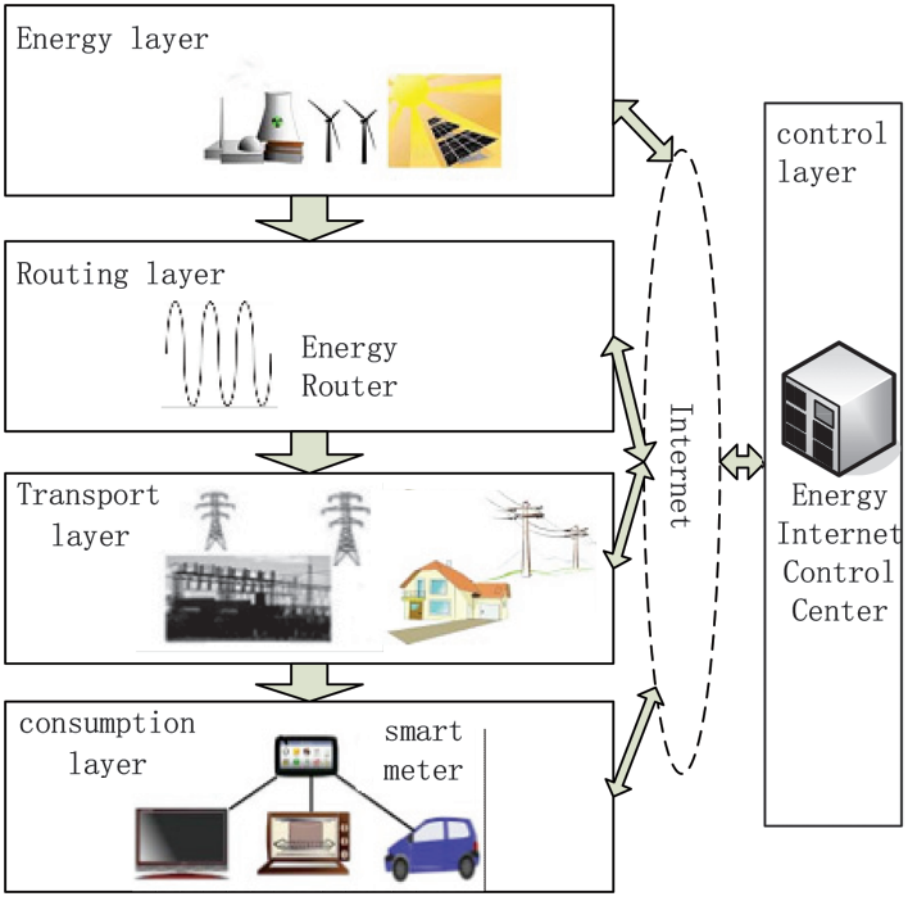


Fig.1: Logical structure of energy internet

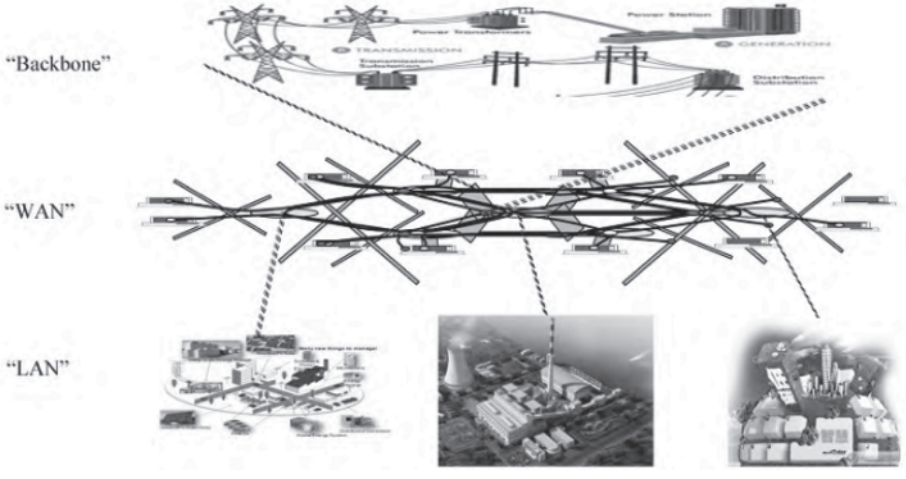


Fig.2: Network structure of energy internet

From the perspective of network topology level, energy internet national is marked with backbone of the energy network to be its top structure, regional level energy networks to be the backbone, various energy LAN connected to the terminal, and these energy LAN can operate grid-connected, as well as stand-alone, for instance, a small community of independent micro energy networks [8] as shown in Fig.2.

2.2 Security analysis methods of existing energy internet

The energy internet combines a variety of physical systems such as power grids and heat networks, and a diverse range of information network involving information control network and electric vehicle network, etc., inevitably incurring more complex security issues. Study on the security of energy internet, a sophisticated physical system, is still in a primary stage, mostly focusing on smart grids, therefore further efforts need to be made to deepen and strengthen researches [2].

A. Security demand-driven method

Security demand of the energy internet primarily comprises confidentiality, integrity, availability, authentication, authorization, non-repudiation, auditability and so on [9]. Security demand-driven method starts from the analysis of possible sabotages and effects resulted from attacks to various energy internets, to refine, classify, analyze and summarize scenes of attacks and behaviours [9-11].

B. Security model-driven method

Sridhar S. et al. [12] established a control loop security model based on smart grid, as shown in Fig.3, and the existing security weaknesses and vulnerabilities are inspected form six aspects: physical parameter measurement, data acquisition, control information, data calculation and analysis, physical device and execution, following that, attacks are identified and categorized on the basis of the above analysis. In addition, some scholars employ the simplified control loop model, abstracting it into control systems and physical systems. Other security models include threat model [13], attack tree model [14], Markov model [15] and game theory model [16], etc.

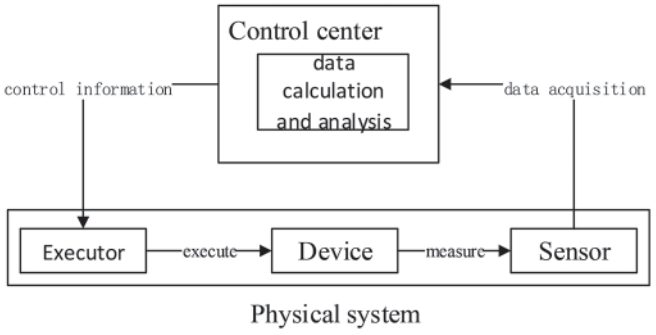


Fig.3: Control loop model

C. System-theoretic method

Aforementioned security research methods are unable to solve the problems in physical security systems, of which the energy internet is a complex one. System-theoretic model abstracts physical flow between various physical components within a system, giving a real-time view of security, to achieve accident analysis and system monitoring, making up for the shortage of the energy internet security research. This method contains generalized linear time-invariant systems [17], continuous-time linear dynamic systems [18], linear control systems [19], etc.

2.3 A new security mechanism based on TPM

In view of the discussion in section 2.3, existing researches on the energy internet security mechanism mostly are launched in isolation, concentrating on a single part of the problem in the energy internet security; hence do not form a unified security system (detailed discussion is described in section 3.1). Most of the studies exploit in theory and there is still a long way to get practical use. As the majority of them target at smart grid, security for energy internet, a multi-network, should be strengthened. Trusted computing which is rising in recent years [20], introduce a secure chip which is based on TPM [21] and a trust root to system, transferring trust relationship to other components or programmes of the entire system through trust chain, thereby forming overall system security solutions. At present, domestic and foreign companies have released many TPM products [22], facilitating a smooth and rapid deployment and application of the energy internet.

2.3.1 Model design

Participants in TPM-based security model of the energy internet include energy consumers and physical equipment of all layers. Due to limited space, the approach is mainly presented in consuming layer, as shown in Fig.4, but it can be easily extended to other layers.

The model is demonstrated on the assumption that all the participants have been embedded with TPM module. TPM2.0 chip supports symmetric encryption which performs better than asymmetric encryption in real-time communication scenarios; however, the chip is not compatible with TPM1.2. As TPM1.2 is still the mainstream in the chip market, the model realizes key distribution of symmetric encryption by TPM1.2 chip's asymmetric encryption algorithm. Security compensation equipment is also provided in the energy internet, to compensate the shortages of TPM-based architecture, such as wireless jamming attack to physical layer or attacks to physical system, which are undetectable through information technology.

2.3.2 Working mechanism

In the security model of consuming layer, participants comprise intelligent electronic devices including, smart meters and charging piles, etc. control centers and energy consumers or electric cars. Based on hardware TPM1.2, the model is built under the following preconditions: control center has public and private key pair (PK_{Con},SK_{Con}), and intelligent electronic devices have public and private key pair (PK_I,SK_I), while the end-users or electric vehicles have public and private key pair (PK_C,SK_C). Control center stores in a secure database the public key of intelligent electronic devices and users as, I_{id}, PK_I), C_{id}, PK_C), respectively. Each intelligent electronic device and user already has the public key of the control center.

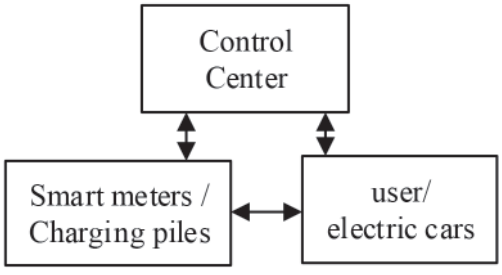


Fig.4: Security model of consuming layer

(1) System initialization. Within the energy internet, all equipment are powered on. A secure and reliable state from the BIOS to operating system to application software is achieved through the trust chain trusted technology on reliable computing platform [19].

(2) Scenario 1. (System monitoring). Control center monitor intelligent devices in real time, for example, device status of smart meters and operating environment information of charging pile. The above monitoring information has high real-time requirement, therefore need to employ symmetric encryption.

Step 1: Intelligent electronic device generates a session key SK_{Con-I} for symmetric encryption, and sends the following information:

$I \rightarrow Con: \{M_1 \| \{M_1\}SK_C\}PK_{Con}$

where M_1 is $I_{id} \| N_1 \| SK_{Con-I}$.

Step 2: Control center receives the message and uses its private key to decrypt it. Then retrieves the corresponding public key PK_I of I_{id} in the security database, meanwhile decrypts $\{M_1\}SK_C$. If the two are of the same value, the SK_{Con-I} is available and the following message will be sent:

$Con \rightarrow I: \{M_2 \| \{M_2\}SK_{Con}\}\ PK_C$,

where M_2 is $N_1 \| N_2$, N_2 is used to prevent replay attacks.

Step 3: The intelligent device receives the message, and uses its own private key to decrypt it, and then checks whether N_1 is equal to the previously transmitted N_1. If so, employs the public key of the control center to decrypt $\{M_2\}SK_{Con}$. If N_2 also equals to the original one, session key SK_{Con-I} is confirmed to encrypt subsequent transmitted data.

Step 4: Both sides employ SK_{Con-I} to encrypt data transmission.

(3) Scenario 2. (User to view the meter/electric vehicle charging)

End users need to check their meter data such as electricity consumption, surplus electricity, etc., or tram car need to be charged at the charging pile. In these cases, users are required to log into the control center and then verify identity for obtaining license of intelligent electronic devices. Within this scenario, users or electric cars tend to use more than once of the meter or the charging pile, hence utilize one-time pad symmetric encryption.

Step 1: Users share SK_{Con-C} with the control center through a protocol interaction method similar to that in scene 2, while Smart devices and the control center share SK_{Con-I} through a protocol interaction method discussed in Scene 2.

Step 2: The users request permission for usage of an intelligent device from the control center, and send the following message:

$C \rightarrow Con, C_{id} \| \{N_3 \| I_{id}\}SK_{Con-C}$.

Step 3: According to C_{id}, Control Center retrieves the key SK_{Con-C} and decrypts the message, obtaining the equipment which the user applied for and review if the user has corresponding permission, if so, send the following message:

$Con \rightarrow C: \{N_3 \| I_{id} \| SK_{I-C} \| CI\}SK_{Con-C} \| \{M_3\}SK_{Con-I}$,

where M_3 is $N_3 \| N_4 \| C_{id} \| SK_{I-C} \| CI$, SK_{I-C} is designated by the control center as the session key for the user C_{id} and the intelligent electronic device. CI is permission information, such as the key SK_{I-C} validity period, energy usage and authorized charge amount.

Step 4: After receiving the message, the user decrypts its first part to get key SK_{I-C}, and employs the key to the application to intelligent electronic devices for energy usage, sending the following message:

$C \rightarrow I, R \| \{C_{id} \| N_3\}SK_{I-C} \| \{M_3\}SK_{Con-I}$, R is the identification of intelligent electronic device.

Step 5: After receiving the message, the intelligent electronic device decrypts the final part to obtain the session key SK_{I-C} which is designated by control center, and utilizes this key to decrypt the first part of the message. If $C_{id} \| N_3$ stays identical, then authorize the user according to CI information, for instance, subsequent usage of SK_{I-C} to transmit meter data and charging electric vehicle specified power in accordance with CI authorization.

3.0 Security analysis

3.1 TOPSIS-based security comparison of existing methods

Currently security measures of the energy internet chiefly contain data encryption, key management, authentication technology, access control, private data protection, equipment security, secure communications framework and intrusion detection, etc. Besides, other security technologies such as dynamic virtual honeypots, context-aware and intelligent tracking firewall are applied to the energy internet as well [23]. The above security methods can be divided into four categories: cryptography method to ensure system information security of the energy internet; wireless channel method specifically for denial of service attacks towards physical layer and MAC layer, which cryptographic methods are unable to protect; system-theoretic approach for protecting the security of the physic layer of the energy internet systems; equipment protection methods designed in particular to protect the physical security equipment, e.g. operating system virus protection.

Given the energy internet's multi-network fusion characteristic, single and isolated security method obviously does not satisfy the requirements. As a commonly used limited programme of multi-attribute decision analysis [24], TOPSIS It can provide decision support for selecting security solutions.

First, the issue has four optional solutions: A_1–A_4, corresponding to the above-mentioned four protection

Table 1: Multiple attribute decision-making matrix

	G_1	G_2	G_3	G_4	G_5	G_6
A_1	1	1	1	0	0	0
A_2	0	0	0	1	0	0
A_3	0	0	0	0	1	0
A_4	0	0	0	0	0	1
W	1	1	1	1	1	1

methods, respectively. The target attributes are symbolized as G_1-G_6, representing confidentiality, data integrity, authentication, wireless channel availability, physical security of the system and equipment safety, respectively. Decision Matrix $U_A = (u_{ij})_{m\times n}$ (Table 1). For calculation purposes, the target attribute values will be set to 1 if protectable and 0 otherwise, and each object attributes are of equally importance, so that $W_j = 1$, $1>j>n_o m=4$, $n=6$.

Step 1, normalize U_A in accordance with formula (1) to obtain a standardized matrix R, where $1>i>m$, $1>j>n$.

$$r_{ij} = \frac{u_{ij}}{\sqrt{\sum_{i=1}^{m} u_{ij}^2}} \quad \text{... (1)}$$

Step 2, calculate weighted norm matrix X, $X=(x_{ij})_{m\times n}=[w_j \bullet r_{ij}]_{m\times n}$. In this case, the calculated X = U.

Step 3, determine the ideal solution U^+ and negative ideal solution U^- by Equation (2), where J^+ and J^- are efficiency indicators set and cost index set, respectively.

$$\begin{aligned} \boldsymbol{U}^+ &= \{(\max_i x_{ij} \mid x_{ij} \in J^+), (\min_i x_{ij} \mid x_{ij} \in J^-)\} \\ \boldsymbol{U}^- &= \{(\min_i x_{ij} \mid x_{ij} \in J^+), (\max_i x_{ij} \mid x_{ij} \in J^-)\} \end{aligned} \quad \text{... (2)}$$

Step 4, calculated Euclidean distance between A_i and positive, negative ideal solution, respectively, by Equation (3) for each security method.

$$\begin{aligned} d_i^+ &= \sqrt{\sum_{j=1}^{n} (x_{ij} - u_j^+)^2} \\ d_i^- &= \sqrt{\sum_{j=1}^{n} (x_{ij} - u_j^-)^2} \end{aligned} \quad \text{... (3)}$$

Step 5, calculate the fitness C_i between security methods and the ideal by Equation (4). The smaller C_i is, the more excellent the solution is. Finally, the solutions are sorted.

$$c_i = \frac{d_i^+}{d_i^- + d_i^+} \quad \text{... (4)}$$

In this use case, ideal solution is adopted as the maximum value of each of the target attributes, and the negative ideal solution adopts the minimum. The calculated ideal solution is (1,1,1,1,1,1), while the negative ideal solution is (0,0,0,0,0,0). Apparently, all the existing security solutions have a certain Euclidean distance away from the ideal solution, namely, the fit is insufficient. For instance, C_1=0.5, C_2=0.69. Therefore, existing solutions need to be integrated and a unified overall security architecture should be proposed for energy internet protection.

3.2 Security analysis of TPM-based security mechanism

This section will discuss whether the proposed security mechanisms close to the ideal solution in section 3.1 to analyze its security.

1. Mutual authentication. In scenario 1, both sides use asymmetric encryption algorithms (RSA algorithm based on TPM). The message sender uses other's public key for encryption, while the receiver employs its own private key to decrypt the message, and the message always contains sender's signature generated by its own private key, hence ensures that the communication parties can authenticate each other. In Scenario 2, the user and the control center have the same pre-shared key to ensure mutual authentication in conversation. In follow-up protocol interaction, user and intelligent electronic devices accomplish mutual authentication through the trusted control center. Nonce in two scenes guarantees freshness of agreement, resisting replay attacks, meanwhile Nonce comparison in recipient is a secondary authentication method.
2. Confidentiality. All the protocol interactions in scenario 1 and scenario 2 utilize asymmetric encryption algorithms RSA or symmetric-key algorithm AES, and are configured correctly, thus ensuring the confidentiality of data.
3. Data integrity. Although HMAC algorithm which is commonly used to ensure data integrity is not employed in scenario 1 and scenario 2, with the signature by private key, or the usage of symmetric encryption, the integration of data can be guaranteed. Even if an attacker tampers with the message, the receiver will discover it by verifying signature wrong, decryption failure and the mismatch between decrypted message and the original, thus ensures data integrity.
4. Physical equipment security. Since all physical devices are using the trust chain technology, the security of the entire hardware system is ensured.
5. Availability. Availability is assured by the utilization of secure compensate equipment, such as frequency hopping communication mechanism set up in wireless device's physical layer to resist interference attacks.
6. Physical system security. Via secure compensation equipment, detection of aggressive behaviors within physical system is completed, including using the system-theoretic method.

Therefore, the presented TPM-based security mechanism provides preferable performance in the protection of the energy internet from above six aspects of view. Using the method discussed in section 2, it can be seen that the proposed mechanism is superior to the four other methods as it is closer to the ideal solution and the Euclidean distance is shorter.

4.0 Conclusion

With human's urgent demand for renewable energy and vision of the efficient and secure utilization of new energy, the energy internet will necessarily become a focus of research and the development direction of future energy industry. This paper analyzes in detail and models energy internet architecture from two aspects: logical level and network topological level. On the basis of the model, domestic and foreigner researches on energy internet security are reviewed, summarized and categorized, furthermore analyzed by TOPSIS method to found that the existing solutions are isolated and lack integrity in characteristic. Thus, a new security mechanism based on TPM is proposed. Typical system security model and protocol interaction model are described, and security features of the presented model are analyzed as well. The proposed model is illustrated to have better performance than existing methods through TOPSIS method.

5.0 Acknowledgements

The authors would like to thank the reviewers for their valuable comments and suggestions which have improved the presentation of the paper.

6.0 References

[1] Rifkin J. (2011): The Third Industrial Revolution: How Lateral Power is Transforming Energy, the Economy, and the Word [M]. New York, Palgrave Macmillan.

[2] Dong Zhaoyang, Zhao Junhua, Wen Fushuan, et al. Dong Zhaoyang, Zhao Junhua, Wen Fushuan, et al.(2014): From Smart Grid to Energy Internet: Basic Concept and Research Framework [J]. *Automation of Electric Power Systems*, 38(15), 1-11 (in Chinese) .

[3] Wang Jiye, Meng Kun, Cao Junwei, et al.(2012): Information Technology for Energy Internet: A Survey[J]. *Journal of Computer Research and Development*, 26(4), 39-45.

[4] Cheng F, Xu M, Xu Z, et al. (2015) : Development of Energy Internet and Key Technology Analysis[J].

[5] Shen Changxiang, Zhang Huanguo, Feng Dengguoÿet al. (2007): Overview of Cyber Security [J]. Science in China (Se-ries E: Information Sciences), 37(2), 129-150.

[6] Huang Renle, Pu Tianjiao, Liu Kenwen, et al. (2015) : Design of Hierarchy and Functions of Regional Energy Internet and Its Demonstration Applications[J]. *Automation of Electric Power Systems,* 39(9), 26-40 (in Chi-nese).

[7] Tian ShimingÿLuan Wenpeng, Zhang Dongxia, et al. (2015): Technical Forms and Key Technologies on Energy Inter-net [J]. Proceedings of the CSEE 35(14), 3482-3494 (in Chinese).

[8] Cai Wei, Zhao Hai, Wang Jinfaÿet al. (2015): A Unifying Network Topological Model of the Energy Internet Macro-scope Structure[J]. Proceedings of the CSEE, 35(14), 3503-3510 (in Chinese) .

[9] Komninos N., Philippou E., Pitsillides A., et al. (2014) : Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures[J]. *IEEE Communications Surveys & Tutorials*, 16(4), 1933-1954.

[10] Mo Yilin, Kim T.H.-J., Brancik K., et al. (2012): Cyber-Physical Security of A Smart Grid Infrastructure[J]. Proceedings of the IEEE, 100(1), 195-209.

[11] Wang Wenye, Lu Zhuo. (2013): Cyber Security in The Smart Grid: Survey and Challenges[J]. *Computer Networks*, 57(5), 1344-1371.

[12] Sridhar S., Hahn A., Govindarasu M., et al. (2012): Cyber-Physical System Security for The Electric Power Grid [J]. Proceedings of the IEEE, 100(1), 210-224.

[13] Carlos M C, Martina J E, Price G, et al.(2013): An updated threat model for security ceremonies[C]//Proceedings of the 28th Annual ACM Symposium on Applied Computing. ACM, 1836-1843.

[14] Jie X, Hongjun B, Yun L. (2013): Research on Security Threat Assessment Method Based on The Attack Tree Model of The Internet of Things[J]. *Journal of Convergence Information Technology,* 8(3).

[15] Cao Y, Li Y, Coleman S, et al. (2015) : Adaptive hidden Markov model with anomaly states for price manipulation detection[J]. Neural Networks and Learning Systems, IEEE Transactions on, 26(2): 318-330.

[16] Liang X, Xiao Y. (2013): Game theory for network security[J]. Communications Surveys & Tutorials, *IEEE,* 15(1): 472-486.

[17] Pasqualetti F., Dorfler F., Bullo F. (2013): Attack Detection and Identification in Cyber-Physical Systems [J]. IEEE Transactions on Automatic Control, 58(11), 2715-2729.

[18] Pasqualetti F., Zhu Qi. (2015) : Design and Operation of Secure Cyber-Physical Systems[J]. *IEEE Embedded Systems Letters*, 7(1), 3-6.

[19] Horowitz B.M., Pierce K.M.. The Integration of Diverse-ly Redundant Designs, Dynamic System Models, and State Estimation Technology to The Cyber Security of Physical Systems[J]. *Systems Engineering*, 2013, 16(4), 401-412.

[20] Kamil S N S, Thomas N. Performance analysis of the Trusted Cloud Computing Platform[C]//31st UK Performance Engineering Workshop 17 September 2015. 2015: 33.

[21] TCG. TPM Main Specification [EB/OL], http://www.trustedcomputinggroup.org/resources/tpm_main_specificationÿ2015-10-31.

[22] Zhang Huanguo, Zhao Bo. Trusted Computing [M]. Wuhan, Wuhan University Press, 2011(in Chi-nese).

[23] Vollmer T., Manic M. Cyber-Physical System Security with Deceptive Virtual Hosts for Industrial Control Net-works [J]. *IEEE Transactions on Industrial Informatics*, 2014, 10(2), 1337-1347.

[24] Hu Chengfeng, Fang Shucherng. Set Covering-based Topsis Method for Solving Sup-T Equation Constrained Multi-objective Optimization Problems[J]. *Journal of Systems Science and Systems Engineering*, 2015, 24(3), 258-275.

Printed by Pradip Kumar Chanda at The Indian Press Pvt. Ltd. 93A Lenin Sarani, Kolkata 700 013 and published by him for Books & Journals Pvt. Ltd. from 62 Lenin Sarani, Kolkata 700 013