스마트 그리드 보안 이슈

홍성혁*
백석대학교 정보통신학부

Security Issues on Smart Grid

Sunghyuck Hong*
Baekseok University, Division of Information and Communication

요 약 지구환경 개선을 위한 저탄소 배출 및 그린에너지에 관심이 높아지고 있으며, 이를 이루기 위한 기존의 전력망에 IT기술을 결합하여 보다 효율적이고 친환경적인 지능형 전력망을 이루는 스마트 그리드 사업이 전 세계적으로 활발히 전개되고 있다. 스마트 그리드는 양방향 디지털 기술을 사용하여 공급 업체와 소비자 사이에 전기를 제공하며, 소비자 집에 있는 지능형 가전이나, 에너지 절약 비용을 절감하고 안정성, 효율성 및 투명성을 높이기 위해 필요하며, 앞으로 지속적으로 발전될 것을 예상한다. 하지만, 스마트 그리드를 구축하기 위해서 반드시 선행되어야 하는 사항인 보안 모델을 구축하여 지능형 전력망을 안전하고 효율적으로 사용되도록 구축하는 방안을 제시하는 연구이다.

주제어 : 스마트 그리드, 보안 위협, 보안 모델, 안전한 스마트 그리드, 그리드 보안, 네트워크 보안

Abstract Improve the global environment for low carbon emissions and green energy, and the growing interest in IT technology, combined with the existing power grid to achieve this, to achieve more efficient and environment-friendly smart grid smart grid projects around the world actively being deployed. A smart grid is expected to be a modernization of the legacy electricity network. Therefore, this research provides a secure smart grid model so that it provides better monitoring, protecting and optimizing automatically to operation of the interconnected elements.

Key Words : Smart grid, security threats, security model, Secure Smart Grid, Grid security, network security

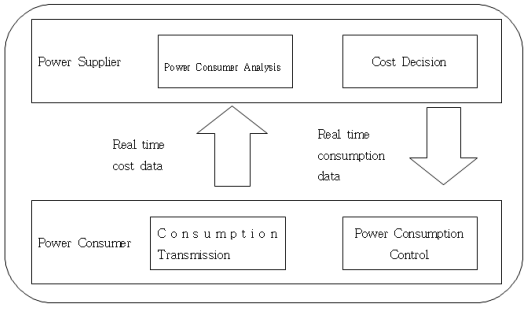
1. Introduction

The smart grid saves the energy. It is the cost the line, and the smart grid system is included in the government with the technology which delivers the electricity from the provider to the consumer in order to increase the reliability of the energizing by using the digital technology among the green growth core task. Also, the leading edge inspection of a meter infrastructure and high-speed Internet, home network cooperate-technology development and normalizing, IPTV, home server, user power control service development of the personal digital assistant base, and it is detail included into the development subject [1]. The existing distribution network delivered the electricity mostly produced in the thermal power or the atomic power plant, and etc. to the general consumer through the transformation of electric energy process of

Received 1 April 2013, Revised 20 April 2013
Accepted 20 April 2013
Email: shong@bu.ac.kr
ISSN: 1738-1916

the several steps with the one-way. However, it changes into the bidirectional power relay way that the residue electricity produced through the wind force in the person or company, sunlight, playback energy development, and etc. can be supplied to the power net in case the smart grid is spreaded. Figure 1 shows the fundamental concept of the intelligent power net.

However, the security problem of the various kinds exists, the smart grid system has to prepare the method concluding these problems [2].



[Fig. 1] Smart Grid Concept

1.1 The necessity of the research

Korean smart grid project group comprises the smart grid actual proof jar in the Cheju-do and runs, and it prepares the actual proof jar security measures in the national security research institute through the actual proof jar security WG(Work Group) and security center operation, security guide and security guideline presentation, each operation center security response development and transition, and etc. in various angles. The actual proof jar security WG the planning suffering from cold and actual proof jar security center promotes the business including the safe network construction method of the consideration actual proof jar, cyber TERROR simulation training, system and network security weakness analysis, and etc. the cyber security the practical business work including the actual proof jar security guide and security guideline establishment, cyber security crisis system of reaction construction, each consortium security measures establishment support, cyber TERROR simulation training, security vulnerability analysis, and etc.

1.1.2 the overseas smart grid cyber security present condition

U.S prepares the EPACT05 and EISA07 bill, and etc. through the enormous blackout, in 2003, the middle eastern area blackout experience in 2001, and the great power outage promotes the various program which the acid, learning, kite, pipe participates in 2000. Particularly, while Obama Administration enters the various support plan including the financial support, technology inducement, standard preparation, and etc. [3] It is considered in the green new deal project dimension. Particularly, the effort for the cyber security intensification is more intensified through the smart meter malignant code occurrence possibility sidewalk of the March, power net malignant code breach accident, and etc. generated on April, 2009.

The European Technology Platform for Electricity Networks of the Future, also called Smart Grids ETP, is the key European forum for the crystallization of policy and technology research and development pathways for the smart grids sector, as well as the linking glue between EU-level related initiatives.

The Open Meter, that is the smart meter normalizing project in which 19 power companies of EU were gathered and which the Open Meter project be under way, announced the smart meter requirement including the security requirement in 2009. The existing IT national renewable security standard use of technology it demands the integrity, use of the certificate, and etc. and in which the safety, and etc. are already verified with AMI security technology and which is widely used is proposed. Therefore, smart grid project is world widely provided. Smart grid project is necessary to survive and develop on our power plant and consumption system.

The smart grid system doesn't come to the stage of commercialization. It is still the present condition in which the weaknesses are much reported as the system while developing recently. As to the power net

of the smart grid, the commercialization is impossible due to the condition where there is the weakness with the domain included in the national important facility. However, the measure research is constantly needed for the weakness in order to use the attractive effect of the smart grid.

By showing the improvement plan that can conclude these problems after analyze the security problems of the smart grid system in order to construct the safe smart grease system, the research was progressed.

2. The Security Problem and Improvement Plan

In the smart grid environment, while many systems get complicated intricately and it cooperates, it operate. The network for the information exchange between power supplier and consumer which is not existing simple power net are constructed. The techniques of the network attack used in the existing Internet network due to this structure can be used as it is. For example, the enormous DDoS (Distributed Denial of Service) attack which it is July, 2009 which it is past generated did the specific web site with the object [4]. Therefore, there were the inconvenience because of the web page admission reject and damage of the company because of the company smear on reputation and electronic commerce abort and person. However, the smart grid system is a goal to the attack of the same way. If it is the case, the damage because of this is the problem of is being generated until the threat to the national security.

The smart grid system is the structure where it is connected to the distribution network and personal terminal from the control system. For example, in our country 1,500 houses in case of using 4 smart electronics 60 million terminal devices are connected to the smart grid. It is easily accessible to this smart electronics in the smart grid system. The possibility of being easily exposed to the personal control, mistakenly, the worm would be that be high. As to this smart electronics, the smart meter, and etc. installed as the sensor for the electric distribution network monitoring, telemetry infrastructure (AMI : Advanced Metering Infrastructure), and last terminal in each home is included as the simple instrument which is installed in the final stage of each system ,device control, and etc. There is nearly no protection device for preventing the access of the attacker. Since being installed in the outside which the outside can approach easily, this terminal is very vulnerable to the attack. Furthermore, in the case of the small distributed power, the physical security management doesn't go well, through this, it can break into the smart grid core system.

By using the weakness of after central control system or operating system, the attacker broken into the smart grid network through the terminal equipment and distributed power dominates the smart grease system. Furthermore, recently, the smart grid weakness is continuously reported.

The IO Active corp., that is the American security company, confirmed to could attack the smart grid through the smart meter. It confirmed to could discontinue the connecting network and power supply due to the simple hacking techniques. In addition, the result that it can infect the smart meter of 15,000~20,000 houses within 24 hours because of introducing the worm virus which it is diffusible automatically between the smart meter and confirming by the worm simulation came out. In this way, the infected smart meter, at the same time, the electric supply can be interrupted. In addition, certainly the control system is needed for the kind of the power net in which the Information Technology the smart grid system is complex. If this control system is held, many damaged unit of state can be plated with many methods in the person including the leakage of personal information, power cut off, and etc [5].

If the long-term power supply is blocked, the following damage can be given. According to this data,

if the national power net 1 / 3 the power supply was interrupted, it ran out of 3 th shop goods and there was no fuel and the emergency generator operation was impossible. The 10 th population large range motion was initiated. We analyze that damage of the people riot and disaster level was generated if it became 3 months.

3. Improvement Plan

The smart grid terminal of the power companies and each home is distinguished by the original number in order to reduce the loss of money by that is the problem of the smart grid, leakage of personal information and hacker. Presently, its own name or resident registration number is used for the personal identification. Therefore, because the possibility that the leakage of personal information is more easily generated is high, the identical ID like the i-PIN replacing the name or resident registration number (I-Pin) and oneself internationally in common use uses the unique password and the amount of energy consumption, cost, and etc. are checked. And the consciousness and basic security recognition strengthening and problem of the center-concentrated module control system are solved through the protection system construction automatic in the personal digital assistant of the smart grid system through the physical security design to the control system and network security enhancement, system approach according to the user authority through the authentication and control authorization, and smart grid private use vaccine development about the virus attack like the worm and security education of the unit of state about the leakage of personal information and the remote control attack prevention through the physical security and hacking has to be done. And it corresponds to the security threat which runs the security center, and which it is generated in the future.

In the national energy technology research institute (National Energy Technology Laboratory, NETL) of the concrete United states department of energy (Department of Energy, DOE) subsidiary, the Modern Grid Initiative, that is the investigation of the perform heart burnings field of electric power transmission, mentions as the fundamental feature in which the smart grid will have to have 'one's recovery' 'the customer participation and triggering of motive' 'the opposition against the attack' 'the offer of the power quality which 21 century digital economy society requests' 'the option reception of the electric power generating and archiving facility' 'the market activation' 'the optimization of the property and efficient operation' 'the prediction about the system infringement and correspondence' in the systematical view. It can look at that there are lots of the features relating to the security among this fundamental features. Therefore, in order to satisfy the features related to this security, technologically the improvement plan has to be prepared.

4. Proposed Model

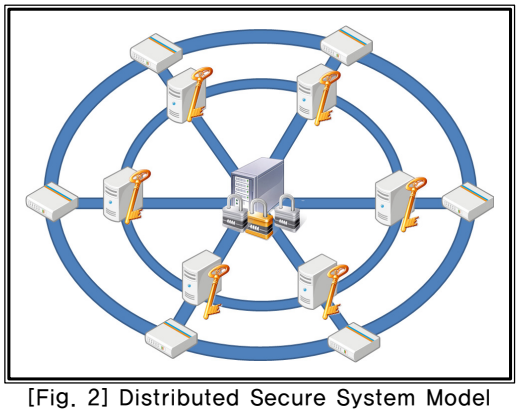
The smart grid control system receives the attack physically or it cannot control the smart grid system through the hacking and virus attack can be generated by building the dummy system in the countermeasure about the case that this situation is generated this remedy will be able to receive the protection about these attacks and thinks.

In case the problem is generated in the smart grid control system which is managed by building in the third of place where the administrator can know the smart grid control system that it is the dummy system, the managed control system is discontinued and the dummy system is driven and it energy-supply and the method that there is no problem.

4.1 the smart grid control system

It builds with the multi distributed system. When it

was attacked if the control system was concentrated on one, all authorities are lost. If the authority of the control system is lost by the attacker, we cannot expect if any damage is suffered. In addition, as to the physical attack, if the smart grid control system, that is the target of attack of the first rank of after cyber war, is destroyed, the enormous stoppage of power supply can occur. It will be good to build the multiple distributed control system in order to minimize the damage about this risk item. Figure 2 shows the future distributed secure system model for smart grid.



[Fig. 2] Distributed Secure System Model

In any control system that it is the multi distributed system, the system where there is the approval of the other control system of the smallest majority, and which can process the business as to the item which the border / is the certain part modified is said. As to this system, the stability is high in the physical security as to the mutually different location.

It is not password authentication. The access privilege assignment through the complex authentication. Because the signal should be given and should be taken with the bidirectional through the smart grid terminal in case the smart grid system is constructed, the network has to be used. By using this point, the hackers can attack the personal information capture through the terminal, DDoS attack through the terminal, and attack like the quartz lamp of charge data. The access privilege about the terminal has to be given through the complex authentication which is not password authentication which is used in the existing in order to prevent this attack.

Literally, it is the complex authentication, it refers to mix more than two authentication methods and authenticate the user. For example, the way of giving the access privilege only when referring to the word registered in previous through the audio of the registered person when it gets the authentication so that the person registered in terminal can be given the access privilege about the terminal is referred to the smart grid system standard church and state.

Presently, the numerous direction of solutions related to the security problem of the smart grid had been being presented. The problem recognition about the cyber security gets better due to these many solution plans day by day. However, it is this smart grid cyber security problem due to member of the standard not to be solved. There is no standard and it hesitates about the investment in the cyber security. And the technology development direction decision of the makers is delayed. And because the problem that product produced in any kind of company is not compatible is generated, many power companies ins the world are regarded to has first to determine the common standard for the smart grid and the smart home environment which the whole world pushes ahead.

5. Conclusion

By proposing the security problem in the smart grid environment and improvement plan and new remedy enhances and provides the energy of the quality higher than one billion of the environment problem and automated electric power distribution the fare saving effect through the supply and real time billing system to the user to the user and is put through the stabilization of the prevention of leakage individual information through the smart grid terminal and system security and control system and will be able to

make the commercialization of the smart grid system earlier and it thinks the optimization of the energy efficiency, reliability rising about the energy generation cost down and energizing, and utilization coefficient of new and renewable energy as the supply of the more stable smart grid system.

However, as the smart grid system is spreaded, it thinks that possibility that the security vulnerabilities which aren't still discovered are generated is high. Because of that, the security vulnerability analysis on the smart grease system and plan for reaction is made actively, and the smart grid system will be able to be run to be safer.

REFERENCES

[1] Yong Wang; Da Ruan; Dawu Gu; Gao, J.; Daming Liu; Jianping Xu; Fang Chen; Fei Dai; Jinshi Yang, "Analysis of Smart Grid security standards," Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on , vol.4, no., pp.697,701, 10-12 June 2011.

[2] Ling, A.P.A.; Masao, M., "Selection of Model in Developing Information Security Criteria on Smart Grid Security System," Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on , vol., no., pp.91,98, 26-28 May 2011.

[3] P. Tsang and S.W. Smith, "Yasir: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems," Proc. IFIP TC 11 23rd Int'l Information Security Conf. (SEC 08), Springer, 2008, pp. 445 - 459.

[4] R. Bobba et al., "PBES: A Policy Based Encryption System with Application to Data Sharing in the Power Grid," Proc. 4th Int'l Symp. Information, Computer, and Communications Security (ASIACCS 09), ACM Press, 2009, pp. 262 - 275.

[5] Q. Wang et al., "Time-Valid One-Time Signature for Time- Critical Multicast Data Authentication," Proc. 28th IEEE Int'l Conf. Computer Communications (Infocom 09), IEEE Press, 2009, pp. 1233 - 1241.

홍 성 혁(Hong, Sung Hyuck)

- 1995년 2월 : 명지대학교 컴퓨터공학과(공학사)
- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 네트워코 보안, 해킹, 센서네트워크 보안
- E-Mail : shong@bu.ac.kr