SCADA 시스템 정보보안을 위한 대칭키 암호 적용

강동주, 김학만
한국전기연구원

Symmetric Encryption Application to Cyber Security of KEPCO SCADA Network

Dong-Joo Kang, Hak-man Kim
KERI

Abstract - SCADA (Supervisory Control and Data Acquisition) SCADA refers to the combination of telemetry and data acquisition [1]. SCADA system has been used for remote measurement and control on the critical infrastructures as well as modern industrial facilities.Electric Power system is a representative system using SCADA network for its communication. Integration between many networks and increasing threatens of terrorism have made the potential risk by cyber attacks real and bigger in power system. Recently, many researching efforts have been made on SCADA network for improving its security. In general aspect, there are already several ways to secure the system like encryption, firewall, authentication, etc. In this paper, we focus on symmetric encryption method and propose the proper key distribution method to reflect the unique characteristics of SCADA network communication.

1. Introduction

SCADA (Supervisory Control and Data Acquisition) is a system operation with coded signals over communication channels so as to provide control of RTU (Remote Terminal Unit) equipment [1]. Recently Intelligent Electronic Device (IED) which is control unit having communication function with master station is replacing the role of RTU. SCADA system has been used for remote measurement and control on the critical infrastructures such as electric power, gas and oil as well as modern industrial facilities such as chemical factories, manufacturing facilities. SCADA network has been exposed to cyber security problems with IT advancement and network growth. Especially, SCADA systems of energy industry such as electric power, gas and oil are vulnerable to targeted cyber attack and terrorism. Recently, research efforts to solve the problems have been progressed throughout the world. In the beginning stage, power system used its own private network, but it has been opened and connected to external networks, finally to the internet, because of saving the cost of building networks and reinforcing the new functions of power system like automation, intelligence, etc. Private network is still used on power system communication in Korea, but the network partly started to be connected to internet network for monitoring and maintenance problem of many stations. Figure 1 shows us overall configuration of Korea SCADA network.

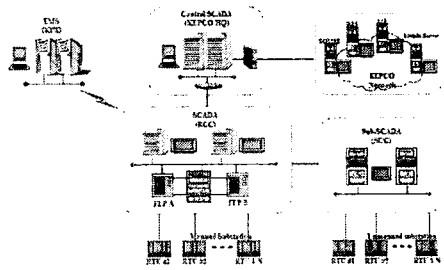

Fig. 1 SCADA system of KEPCO power system

Connection to the internet brings the improvement on economics in a positive aspect but also the escalation of vulnerability on system from cyber attacks. As cyber attacks increase on general communication networks, SCADA network has been also exposed to cyber security problems. Especially, SCADA systems of energy industry such as electric power, gas and oil are vulnerable to targeted cyber attack and terrorism. SCADA networkof power system has its own unique characteristics like data format and size, communication period, network topology, and etc. These kinds of inherent qualities in power system should be reflected into security policy, especially on encryption and decryption algorithm for SCADA network.

2. SCADA network and communication

Central SCADA communicates with RCC SCADA using TCP/IP protocol. TCP/IP protocol is also used in the communication between RCC SCADA and SCC SCADA. EMS (Energy Management System) uses ICCP to communicate with RCC SCADA. ICCP is the acronym of Inter-Control Center Communication Protocolwhich is one of the global standard communication protocols for wide area communication between centers of the electric power transmission network such as power plants and network control centers and substations [4]. ICCP is useful for the communication between control centers which transmit and receive a large scale of data periodically like real time measurement and control data. It is possible for different systems provided by various vendors to communicate each other and to be integrated into one entire system. RCC and SCC communicate with RTU or IED using DNP or Harris protocol. DNP is also

telecommunication standard with ICCP, which defines communication between master stations, remote telemetry units (RTUs) and other intelligent electronic devices (IEDs). DNP was developed to achieve interoperabilityamong systems, specifically for SCADA system in the electric utility, oil & gas, water/waste water and security industries [1]. Currently the SCADA system of KEPCO network only use its private network not connected to Internet for the communication, and has not considered any measure for the security. We just focus on the cyber security of the private network of KEPCO in this paper, although it is expected to be integrated into other networks or Internet sooner or later.

3. Security problem of SCADA network

The focus in this paper is about the encryption and decryption method of data and the flexible management of it. We choose to encrypt the whole data itself and do not consider the aspect of protocol modification. Only considering the private network, one of the probable methods to crack the SCADA system in current situation is to tap a communication line between RTU and master station as shown Figure 3.

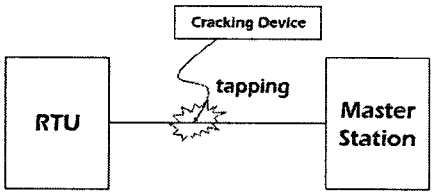

Fig. 3 Intrusion into the communication line

To cope with this intrusion we could encrypt the information by cryptography as shown in Figure 4. When intruders access and snap the information, the information is revealed as a distorted one. Enhancing the security has lots of methods which are all important and needed to be coordinated with each other. Cryptography is just one of those methods for securing the system, but the SCADA system is currently closed system to external networks, which makes the cryptography a main issue on considering the security problem.

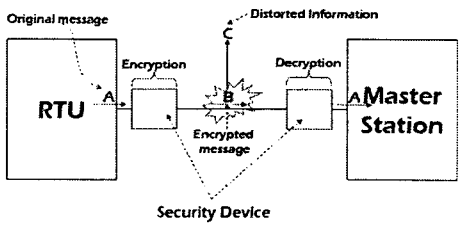

Fig. 4 Information encryption and decryption

4. Key distribution problem for symmetric encryption method on SCADA network

For symmetric encryption to work, two parties involved in communication must share the same key, and that key protected by access by others [3]. There are several ways of this kind of key distribution. Representatively we could think of two kinds. First one is that the communication initiator makes the key and sends it to the responder. We call this method decentralized key distribution.

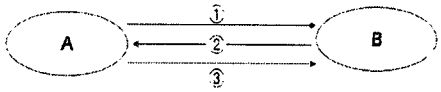

Fig. 5 Decentralized Key Distribution

There is no key distribution center on this method. Initiator A requests B to send the session key at ① process, and B responds to A with the key encrypted with master key already shared with A at ②. And finally A confirms the key distribution process at ③. Second one is that the third party makes the key and distributed to the initiator or both of them, which is called as centralized key distribution in Figure 6.

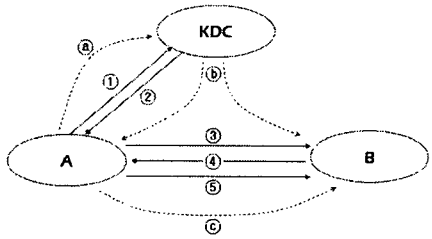

Fig. 6 Centralized Key Distribution

The flow notated with solid lines and Arabic numbers indicate the key distribution to only communication initiator A, while the one with dotted line and alphabets indicate the key distribution to both parties involved in communication. ① ②and ③are same processes also corresponding to ⓐand ⓑs in the decentralized key distribution of Figure 5. ④and ⑤re authentication processes for the session key shared by two parties. We don't have to have the KDC to deal with the key distribution on this network topology because thewhole communications of RTUs should be done with one master station. So we confine the key distribution model to decentralized model of Figure 8. Master station is the initiator in the communication of SCADA system, so the security devices on the RTU side have to generate session key, which corresponds to the process ① of Figure 7. Next it encrypts the key with master key and sends it to the security device of master station side, which corresponds to ②. Finally master station side confirms it has received and shared the session key with RTU side, which corresponds to ③. After sharing the key, two parties begin their communication.

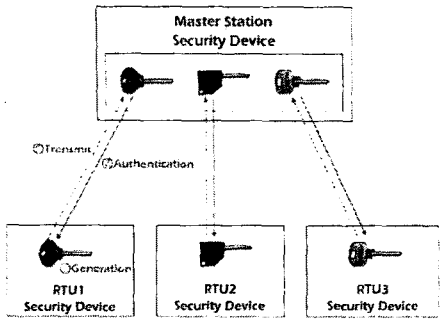

Fig. 7 Key creation and sharing process

Figure 7 shows this process for creating and sharing the key between master station and RTUs. There are two problems here. First one is if the master station uses the common secret key with all RTUs. Second one is how often the master station changes the secret key for security. If the secret is used for a long time, it will increase the possibility of being revealed. However we cannot change the key too often, because the frequent changes of the key increase the network traffic and communication failures. It is more critical in SCADA network because of itsunique characteristics on data size and communication frequency. In conclusion the security strength is proportional to how many keys to generate for RTUs and how often to change the key. However, the reinforcement of security using above method increases the traffic load of network, which makes the security weaker in the other aspect. The system will be vulnerable by heavy traffic load. Therefore we should find out the optimal point for the numbers of keys and the period of key distribution, or just one of them. For example if we fix the key as one common key for entire system, our consideration would be only the frequency of changing the key, and vice versa.

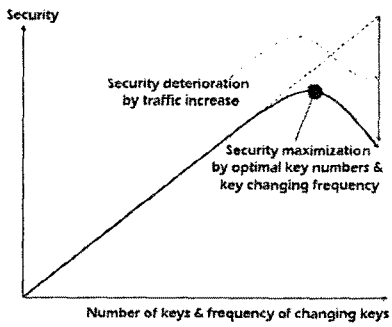

Fig. 8 Key policy for security maximization

We are not sure of the linearity on the security function of key numbers and distribution frequency, but it seems that there would be the maximum level of security when we try to secure the system by encryption and its related key policy. At some point the security would deteriorate by increased key numbers and traffic. This concept is illustrated in Figure 8, and formulated as follows.

$$Max_{n,t} S(n_{key}, t_{dist})$$

$$subject\ to\ n_{key} \le n_{RTU},\ t_{dist} \le t_{req}$$

Here n_{key} and t_{dist} mean the number of keys at the same time and time period for changing the keys respectively. n_{RTU} is the number of RTUs in the SCADA system and t_{req} is the communication frequency for SCADA master station to poll data from RTUs, which is the required level of key changing or distributionperiod. More specific mathematical formulation of this concept will be on future studies. Cyber security problems of SCADA network of critical infrastructures such as electric power, gas and oil are very important against cyber attack and terrorism. Recently, researching efforts to solve the problem are accelerating and bringing the improvement.

5. Conclusion

In this paper, we focus on the SCADA network of electric power system, especially on KEPCO power system in Korea. KEPCO has used its own private network for SCADA communication, which is not connected to Internet. Considering its simplicity of network topology we applied symmetric encryption method to the SCADA network for the cryptography of information. And then we propose a method for secret key policy for SCADA network and conceptual formulation for decision making based on symmetric encryption. We need more studies on mathematical formulation of security function and the application of asymmetric encryption method to this problem in future studies.

[참 고 문 헌]

[1] Gordon Clarke, Deon Reynders, Edwin Wright, Practical Modern SCADA Protocols, Newnes, 2004

[2] Michael LeMay, SCADA Protocols: Overview of DNP3

[3] William Stallings, Cryptography and Network Security · Principles and Practices, Pearson International Edition, 2006

[4] Dacfey Dzung, Mario Crevatin, Security for Industrial Co mmunication Systems, 2005 Proceedings of the IEEE