Journal of the Korean Institute of Illuminating and Electrical Installation Engineers Vol. 21, No.9, pp. 95~100 November 2007 (21-9-14)

Security Issues & Application in Korea SCADA

Hak-Man Kim* · Dong-Joo Kang

Abstract

The importance of communication security is increased in the power industry. The representative communication network of power industry is the SCADA (Supervisory Control and Data Acquisition) systems. The SCADA system has been used for remote measurement and control in the power industry. Recently, many studies of SCADA network security have been carried out around the world. In this paper, we introduce recent security issues in the SCADA network and propose the application of a symmetric encryption method to the Korea SCADA network.

Key Words : SCADA(Supervisory Control and Data Acquisition) systems, Security enhancement, Security issues, Korea SCADA network, symmetric encryption

1. Introduction

A stable electrical power supply is a very important issue in power systems. Power systems are composed of many facilities, control systems and communication networks.

Recently, the increment of cyber attacks and cyber worms and viruses threaten stable operations and supply. The interruption of power supply endangers the daily life of people and can generate dangerous situations throughout the world. For this reason, various efforts to ensure the stable operation of the power industry have been studied.

SCADA(Supervisory Control and Data Acquisition) systems have been used for remote measurement and control in the electrical power industry as well as other industrial applications such as gas, oil, water, transportation infrastructure and many industrial factories. The SCADA system is the technology that enables users to collect data from one or more distant facilities and/or send limited control instructions to those facilities [1]. To solve the problems of the vulnerability of SCADA systems, many research activities have been performed throughout the United States [2-4].

In this paper, we introduce the recent security issues of the SCADA network. Also, through consideration of the configuration and protocols of the Korea SCADA networks, we propose a symmetric encryption method for the Korea SCADA network.

* Main author : Korea Electrotechnology Research Institute, Korea
Tel : +82-31-420-6108, Fax : +82-31-420-6009
E-mail : hmkim@keri.re.kr
Date of submit : 2007. 9. 20
First assessment : 2007. 10. 2
Completion of assessment : 2007. 10. 22

2. SCADA Systems

SCADA systems are the most representative systems for the monitor and control of the power industry. They have been used for the remote measurement and control of many industrial applications. A SCADA system allows the operator to make set-point changes on distant process controllers, to open or close valves or switches, to monitor alarms, and to gather measurement information from a location central to a widely distributed process, such as groups of small hydroelectric generating stations, oil or gas production facilities, pipelines for gas, oil, chemicals and water, electrical power systems and so on [1].

A general SCADA system is composed of human operators, Man Machine Interfaces (MMI), Master Terminal Units (MTU), a means of communication and Intelligent Electronic Devices (IEDs) or remote terminal units (RTUs). The IED is a type of control element which includes sensors, relays, and control blocks / terminals with communication functions. Communication methods between the MTU and IED or RTU include radio, leased line, landline, and microwave. Fig. 1 shows the general configuration of a SCADA network in electrical power systems.

Fig. 2 shows communication protocols of the SCADA system for the Korean power system. A central SCADA communicates with the RCC (Regional Control Center) SCADA using TCP/IP protocol. TCP/IP protocol is also used in the communication between RCC SCADA and SCC (Sub-Control Center) SCADA. The EMS (Energy Management System) uses ICCP to communicate with RCC SCADA. ICCP (Inter-Control Center Communication Protocol) is a global standard communication protocol for wide area communication between centers of an electric power transmission network such as power plants, network control centers and substations [5]. ICCP is useful for the communication between control centers which transmit and receive a large scale of data periodically, such as real time measurements and control data.

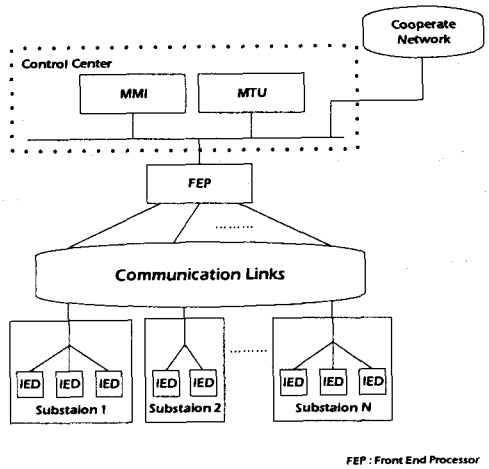

Fig. 1. SCADA system configuration

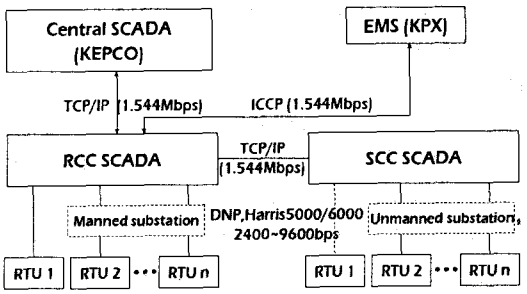

Fig. 2. Communication protocols of the Korea SCADA

It is possible for different systems provided by various vendors to communicate with each other and to be integrated into one entire system when they use a same protocol. RCC and SCC communicate with RTU or IED using DNP or the Harris protocol. DNP is also a telecommunications standard with ICCP, which defines communication

between master stations, RTUs and other IEDs.

Currently the SCADA system for the Korean network uses only a private network not connected to the Internet for communication, and measures for security have not been considered. This paper only focuses on the cyber security of the private Korean network, although it is expected at some point to be integrated into other networks or the Internet.

3. SCADA Network Vulnerability and Protection

The use of IT within the SCADA systems of critical infrastructures such as electric power systems has exposed them to cyber security issues and they have been the target of cyber attacks. According to [6] and [7], cyber risk for SCADA systems has been increased by the following:

- The adoption of standardized technologies with known vulnerabilities, such as the use of common operating systems, like Microsoft Windows and UNIX, in SCADA and control system platforms
- The connectivity of SCADA systems to other networks by demand from corporate users for operational data on a near-real-time basis, etc.
- Insecure remote connections
- The widespread availability of technical information about the SCADA system
- The increased use of TCP/IP communication

According to [8], the general types of attack on SCADA systems are the following:

- Denial of service attacks by delaying or blocking the flow of information through control networks
- Unauthorized changes made to programmed instructions in IEDs at remote sites, resulting in damage to equipment, premature shutdown of processes, or even the disabling of control equipment
- False information sent to control system operators to disguise unauthorized changes or to initiate inappropriate actions by system operators
- Modification of the control system software, producing unpredictable results
- Interference with the operation of safety systems

Fig. 3 shows an example of intrusion into the communication network line of SCADA, called 'tapping'.

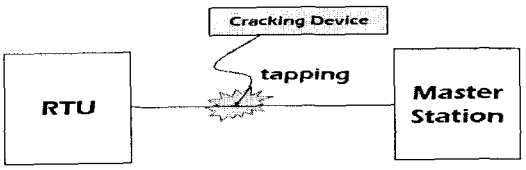

Fig. 3. Intrusion into the communication line of SCADA

To protect the SCADA system from this intrusion the information could be encrypted by cryptography as shown in Fig. 4.

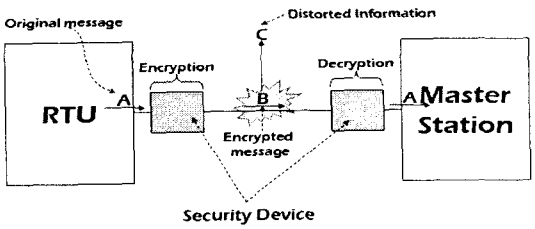

Fig. 4. Information encryption and decryption

4. Security Application to the Korea SCADA Network

In general, there are several security methods used, such as:

- Access control

- Firewalls and intrusion detection systems
- Cryptography and key management
- OS security

Out of these methods, cryptography and key management are the strongest, most common methods of securing the system. There are two fundamental alternatives for the location of encryption gear or devices: link encryption and end-to-end encryption [9]. However end-to-end encryption is adequate for the Korean SCADA network when considering its network topology as shown in Fig. 2.

There are various cryptographic methods already developed for the encryption and decryption of information. These cryptographic algorithms are principally categorized into two different kinds: symmetric and asymmetric encryption algorithms.

Symmetric encryption for SCADA is proposed in this paper because of two following reasons.

The first reason is the number of communication combinations in the SCADA network, which differs greatly from the one used in usual networks. The SCADA network is a radial network and communication occurs only between one master station and multiple RTUs, which means the communication combination only increases in proportion to the number of RTUs.

Assuming N hosts, there are [N(N-1)]/2 cases for the pairs of communication in usual networks such as the Ethernet or Internet in which each host can communicate with any other host in the network. By increasing the number of hosts in a general network or the Internet, the number of communication combinations increases (N-1)N/2 when assuming the number of hosts is N, which is a quadratic functional increase of N. On the SCADA network, however, one additional RTU adds only one communication combination to the previous combinations.

Therefore this increases linearly as the number of RTUs increases, because all RTUs communicate with only one master station. Indexing the number of RTU or IED as 'N-1' which is similar to the number of hosts excluding the master station, the number of communication combinations becomes just 'N-1'. It seems reasonable, therefore, to apply symmetric encryption to SCADA communication when considering the number of keys to be shared.

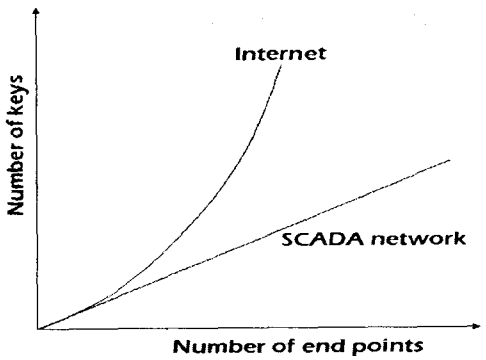

Fig. 5. Number of keys required in the SCADA network and Internet for symmetric encryption

The second reason that symmetric encryption is proposed is the process speed required in SCADA communication. SCADA deals with massive amounts of data in a very short period. When there is a system failure, the possibility of a traffic jam on the network arises which could be worsened by the encryption process. It is recommended therefore to reduce the time taken in the encryption process to as little as possible. Considering the time needed simply for encryption itself, the symmetric encryption is the better method for SCADA communication. However, symmetric encryption is more vulnerable to attack compared to asymmetric encryption. Complementary measures are therefore needed when using the symmetric encryption. This

method which is also the thesis of this paper, is detailed later.

A symmetric encryption algorithm can be characterized by the fact that the decryption key is identical to the encryption key. Symmetric encryption, also referred to as conventional encryption or single-key encryption, was the only type of encryption in use prior to the development of public key encryption in the 1970s [9].

The key must be exchanged in advance between sender and receiver in a secure manner and must be kept secret [10]. Fig. 6 illustrates the basic process of symmetric encryption.

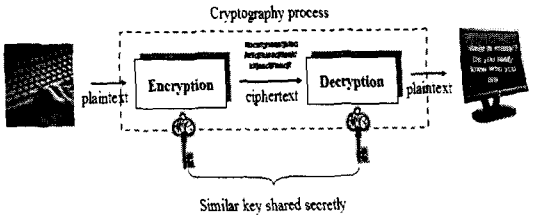

Fig. 6. Symmetric encryption

Fig. 7 illustrates the process of the key distribution process in the SCADA network the symmetric encryption is applied to the network. 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. Finally, A confirms the key distribution process at ③.

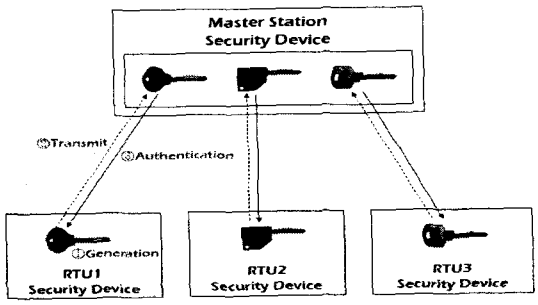

Fig. 7. Key distribution process in SCADA

There are two options here. The first is that the entire SCADA system uses one common secret key, and the second one is that each RTU shares its own secret key with the master station. This could be determined by network status or the security policy of the system. The key distribution period could be also considered as one of the variables in deciding which to use. This is an issue for further research.

5. Conclusion

The cyber security problems of the SCADA network for critical infrastructures such as electric power, gas and oil delivery systems are very important in guarding against cyber attack and terrorism. Recently, research efforts to resolve the problem have been accelerating and have been yielding visible improvement. This study focuses on the SCADA network of electric power systems, specifically, the power system in Korea. The Korean power system has used its own exclusive network for SCADA communication, which is not connected to the Internet. Considering its simplicity of network topology, a symmetric encryption method was applied to the SCADA network for the encryption of information. The beginning stage of the system security problem in the Korea SCADA network was only considered. Therefore, the focus of this paper is symmetric encryption only. The application of asymmetric encryption is an area for future study. More studies will be performed on the mathematical formulation for the security function of the key distribution period or economic investment.

References

[1] Stuart A. Boyer, "SCADA: Supervisory Control and Data Acquisition", 2nd Edition, Instrument Society of America, 1999.

[2] Rolf Carlson, "Sandia SCADA Program: High-Security SCADA LDRD Final Report", Sandia Report, SAND 2002-0729, April, 2002.

[3] J. Eisenhauer, P. Donnelly, M. Ellis and M. O'Brien, "Roadmap to Secure Control Systems in the Energy Sector", January, 2006.

[4] C.L. Beaver, D.R. Gallup, W.D. NeuMann, and M.D. Torgerson, "Key Management for SCADA", SAND Report SAND2001-3252, March, 2002.

[5] Dacfey Dzung, Mario Crevatin, "Security for Industrial Communication Systems", Proceedings of the IEEE, 2005.

[6] Thomas Kropp, "System Threats and Vulnerabilities - An EMS and SCADA Security System Overview", IEEE Power and Energy Magazine, March, pp.46-50, 2006.

[7] GAO-04-628T, "Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems. Testimony before the Subcommittee on Technology Information Policy", Intergovernmental Relations and the Census, House Committee on Government Reform, March, 2004.

[8] Yongge Wang and Bei-Tseng Chu: sSCADA, "Securing SCADA Infrastructure Communications", August, 2004.

[9] William Stallings, "Cryptography and Network Security - Principles and Practices", Pearson International Edition, 2006.

[10] Dacfey Dzung, Mario Crevatin, Security for Industrial Communication Systems, 2005 Proceedings of the IEEE, 2005.

Biography

Hak-Man Kim

Received a B.S., M.S and Ph.D degree in Electrical Engineering from Sungkyunkwan University, Korea in 1991, 1993 and 1998, respectively. Dr. Kim has been with KERI since 1996. His interests include cyber security, optimization, artificial intelligence application, control of power facilities and systems. He is a member of the KIIEE and KIEE.

Dong-Joo Kang

Received a B.S. and M.S degree in Electrical Engineering from Hongik University, Korea in 1999 and 2001, respectively. Mr. Kang has been with KERI since 2001. His interests include cyber security in SCADA systems, application of game theory to cyber security and power transactions, and the development of an electricity market simulator. He is a member of the KIIEE and KIEE.