Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

# Proposal strategies of key management for data encryption in SCADA network of electric power systems

D.J. Kang [a,1], J.J. Lee [a,1], B.H. Kim [b,2], D. Hur [c,*]

[a] Korea Electrotechnology Research Institute, Fusion Technology Research Lab., 665 Naeson2-dong, Uiwang-city, Gyeonggi-province 437-808, Republic of Korea
[b] Hong-Ik University, School of Electronic and Electrical Engineering, 72-1 Sangsu-dong, Mapo-gu, Seoul 121-791, Republic of Korea
[c] Kwangwoon University, Dept. of Electrical Engineering, Kwangwoon Rd. 26, Nowon-gu, Seoul 139-701, Republic of Korea

ARTICLE INFO

*Article history:*
Received 6 November 2007
Received in revised form 10 October 2008
Accepted 13 March 2009
Available online 11 April 2009

*Keywords:*
Cyber security
Optimal key distribution period
Quality of service function
SCADA
Encryption

ABSTRACT

SCADA (Supervisory Control and Data Acquisition) systems have been used for remote measurement and control over both critical infrastructures and modern industrial facilities. The electric power system is thought of as a typical model using the SCADA network for its remote control and monitoring. Integration between many networks is one of today's global trends. In fact, the integration of the SCADA network into Information Technology (IT) networks is favorably under way in terms of automation and economics of power systems, which makes the SCADA network vulnerable to increased cyber assaults. In so far as cyber security is concerned, there exist several methods to secure the system such as encryption, firewall, authentication, and so on. In this paper, we primarily address the unique security environment and inherent problems in the radial SCADA network of electric power systems. Our approach here is informed by the symmetric encryption method. For the most part this paper will be limited to the key management for encryption and provide a solution to the optimal key distribution period as well.

## 1. Introduction

As the power industry relies increasingly on information to operate power systems, not only the power system infrastructure but also the information infrastructure cannot be effectively managed alone. First of all, the reliability of power system infrastructure is significantly affected by any problems that the information infrastructure might face [1], as automation continuously replaces manual operations, market forces necessitate more accurate and timely information, and at the same time the power system equipment becomes obsolete.

Generally, the SCADA (Supervisory Control and Data Acquisition) system is an operational twin composition of a large and strong software package and a networking infrastructure into a global supervision system. The former uses the latter to acquire data, analyze and send control actions. In recent years, IED (Intelligent Electronic Device), a control unit performing communication function with the master station, is taking the place of RTU.

So far the SCADA systems have been used for remote measurement and control of the critical infrastructures such as electric power, gas and oil as well as manufacturing facilities [2]. The general configuration of the SCADA network is sketched in Fig. 1. It is largely composed of three parts: master station, communication links, and slave stations which would be RTUs and IEDs. The communication links for connecting the SCADA server with IEDs may have different kinds of media according to the system size and circumstances.

In the beginning stage when the SCADA systems were built, they used their own private network separated from external network, but they have gradually been connected to external network, even to the Internet, for the purpose of saving the costs of building networks and installing new functions of power systems, i.e., automation and intelligent control [3].

In this sense, the SCADA network has been exposed to cyber security problems with IT advancement and network growth. Especially, the SCADA systems of energy industry are vulnerable to targeted cyber assaults and terrorism in that the attacks to these infrastructures can cause tremendous losses in the overall social systems [4]. The external attacks have increased twofold compared with internal attacks [5].

Though research efforts to overcome this problem have been spread throughout the world, the security problem in the SCADA network of Korean electric power systems has apparently been ignored. The main reason is that the SCADA system is a closed system separated from other networks such as the Internet. Thus it is probable that the private network is still being utilized in the power system communication since the control area is limited to Korea's territory and the infrastructure has been constructed by a

* Corresponding author. Tel.: +82 2 940 5473; fax: +82 2 940 5141.
*E-mail addresses:* djkang@keri.re.kr (D.J. Kang), jongjoo@keri.re.kr (J.J. Lee), bhkim@hongik.ac.kr (B.H. Kim), dhur@kw.ac.kr (D. Hur).
[1] Tel.: +82 31 420 6138; fax: +82 31 420 6029.
[2] Tel.: +82 2 320 1462; fax: +82 2 320 1110.

0142-0615/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ijepes.2009.03.004