SCADA 통신 데이터 보호 기술

(Security Technology for SCADA Communication Data)

김학만* (인천전문대)
Hak-Man Kim (Incheon City College)

Abstract

SCADA(Supervisory Control and Data Acquisition) is popular control and monitor areas not only in critical infrastructures such as electric power, gas, oil but also industrial applications. Increasement of cyber attack technique and frequency threats secure operation of SCADA systems. Recently many researches have been studied for protecting SCADA system against cyber attacks. This paper introduces overall security technologies in SCADA systems.

1. 서 론

SCADA(Supervisory Control and Data Acquisition) 시스템은 전력, 가스, 상수도, 철도 등 국가 주요 기반 시설물뿐 아니라 산업전반의 감시 제어에 널리 이용되는 시스템이다. 특히, SCADA 시스템은 통신을 통해서 감시와 제어가 이루어지는데, 감시 및 제어 대상 시스템의 원활하고 안전한 운용을 위해서 통신 데이터의 신뢰성을 유지하는 것이 중요하다.

최근 들어 외국에서는 SCADA 시스템의 해킹 및 의도적인 공격, 웜바이러스의 침투 등으로 특히, 국가 주요 기반 시설의 SCADA 시스템에 문제가 발생하여 큰 사회적인 문제로 대두되었으며, 이를 방지하기 위한 다양한 기술들이 연구되고 있다. 특히, 이들 연구 중에서 SCADA 시스템의 통신 데이터 보호를 위한 연구들이 진행되고 있다[1]-[4]. 최근 국내에서도 SCADA 시스템의 통신 데이터 보호를 위한 연구가 일부 착수되어 현재 초보적인 단계의 연구가 진행되고 있다.

현재 국가 주요 기반 시설물의 SCADA 시스템의 통신망은 전용망을 많이 이용하고 있지만, 산업용의 경우는 범용망을 이용하는 경우가 많다. 그러나 외국의 기술 자료에 의하면 전용망의 경우에도 데이터 보호에 취약성이 있는 것으로 보고되고 있으며, 또한 장기적으로는 범용망에서 점차 전용망으로 이전될 것으로 예상되며, 이 경우 SCADA 시스템의 통신 데이터의 보호는 해결하여야 할 더욱 중요한 문제로 대두될 것이 예상된다.

본 논문에서는 SCADA 시스템의 통신 데이터 보호 기술에 대해서 SCADA 시스템 개요, 전형적인 SCADA 시스템 구성, SCADA 시스템에 적용되는 통신 프로토콜, SCADA 통신망 침입, 암호화 기술, 상호 인증 기술, 미국의 DOE에서 지원하여 개발된 암호화 장치의 시작품, 적용 개념 및 키 분배 개념에 대해서 간략하게 기술하고자 한다.

2. 본 론

2.1. SCADA 시스템

SCADA 시스템의 구성은 상위의 컨트롤 센터, 사이트의 RTU(Remote Terminal Unit) 및 IED(Intelligent Electronic Device)와 통신망으로 구성된다. 그림 1은 SCADA 시스템의 간단한 예를 간략하게 나타낸 것으로 SCADA 시스템의 컨트롤 센터와 사이트 사이에 통신망으로 연결되어 있으며, 또한 필요에 의해서 외부의 망과 연계되어 있는 경우도 있다[5].

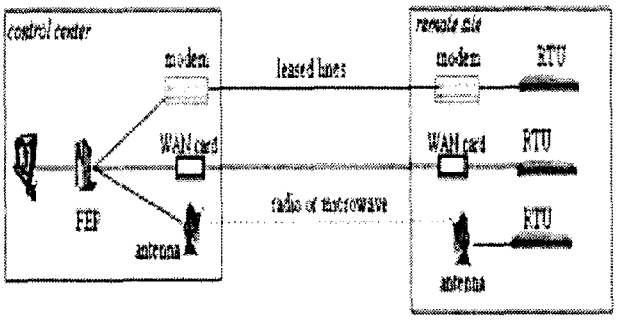

그림 1. SCADA 시스템
Fig. 1. SCADA system

그림 2는 SCADA 시스템의 전형적인 구성을 간단하게 그림으로 나타낸 것이다[5].

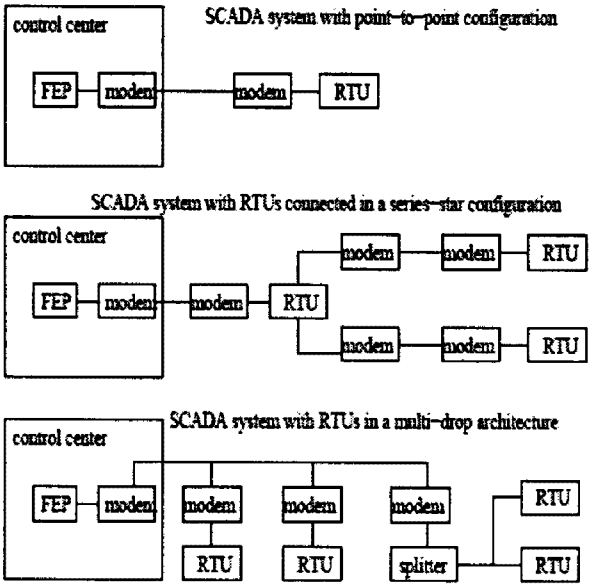

그림 2. 전형적인 SCADA 시스템 구성
Fig. 2. Typical SCADA system configurations

SCADA 시스템의 일반적인 통신 프로토콜은 표 1과 같다[6].

표 1. SCADA 시스템의 통신 프로토콜
Table 1. Communication protocols of SCACA system

Protocol	Organization/standard
Ethernet/IP (Industrial Protocol)	Open DeviceNet Vendors Association (ODVA) (www.odva.org)
DeviceNet	Open DeviceNet Vendors Association (ODVA) (www.odva.org)
ControlNet	ControlNet International (www.controlnet.org)
PROFIBUS	Type 3 protocol of IEC Standard 11674 and 61158 (www.profibus.org)
MODBUS TCP/IP	MODBUS-IDA (www.modbus.org)
DNP3	(IEC) Technical Committee 57, Working Group 03 Standard
Foundation Fieldbus	The Fieldbus Foundation/open Standard protocol (www.fieldbus.org)

2.2. SCADA 통신 데이터 보호

SCADA 통신에서의 외부 침입은 그림 3에 나타낸 탭핑을 통한 방법이 가장 일반적인 방법이며, 이에 대한 일반적인 데이터 보호 방법은 그림 4의 암호화 장치를 이용한 것이다[7].

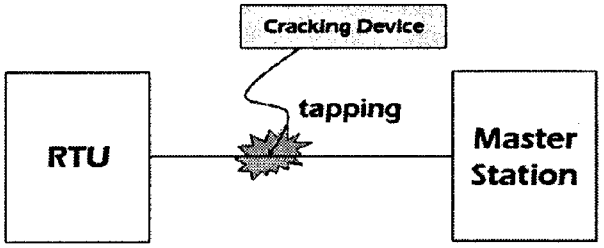

그림 3. SCADA 통신망의 침입
Fig. 3. Intrusion into communication line of SCADA

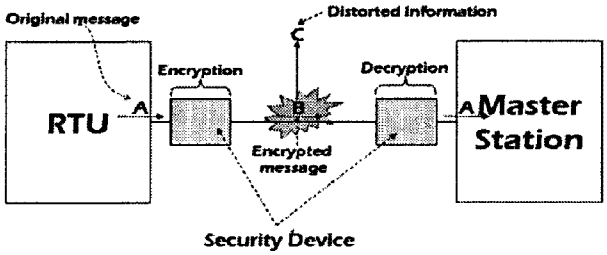

그림 4. SCADA 통신망의 암호화 기술 적용
Fig. 4. Cryptography application to communication line of SCADA

SCADA 네트워크에 암호화 기술 적용을 위해서는 암호화 기술, 상호 인증 기술, 키 공유 기술의 개발 및 적용이 요구된다. 그림 5는 대칭키에서의 암호화 기술을 개념적으로 나타낸 것이고 그림 6은 상호 인증 기술을 개념적으로 나타낸 것이다.

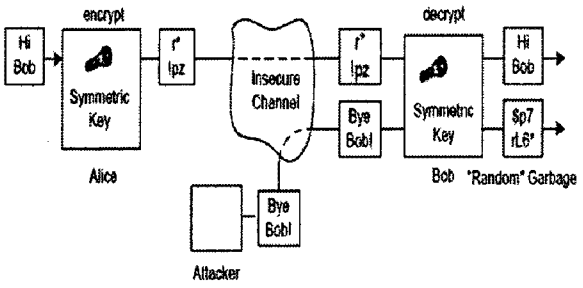

그림 5. 암호화 기술
Fig. 5. Cryptographic technique

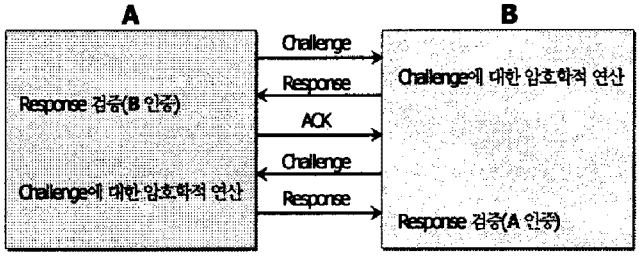

그림 6. 인증 기술
Fig. 6. Authentication

그림 7은 미국의 DOE에서 지원하여 개발된 암호화 장치의 시작품을 나타낸 것이고 그림 8은 MODBUS SCADA 네트워크에 암호화 장치의 설치의 예를 개념적

으로 나타낸 것으로 그림에서 SCM은 암호화 장치를 나타낸 것이다[8].

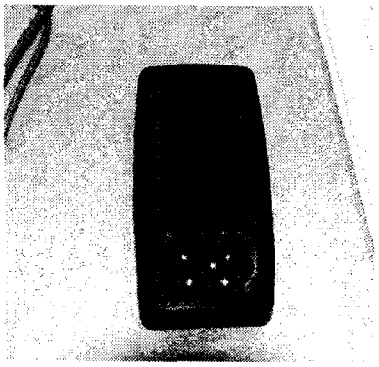

그림 7. 암호화 장치
Fig. 7. Cryptographic device

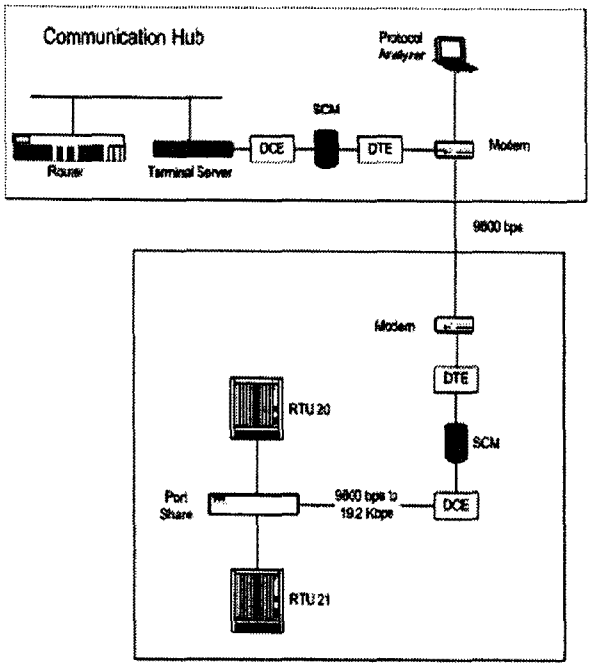

그림 8. SCADA 통신망의 암호화 장치 설치
Fig. 8. Installation of communication line of SCADA

SCADA 시스템의 키 분배는 다양한 방법으로 적용 가능한데, 그림 9는 SCADA 시스템의 키 분배의 한 구성 예를 간단하게 나타낸 것이다[7].

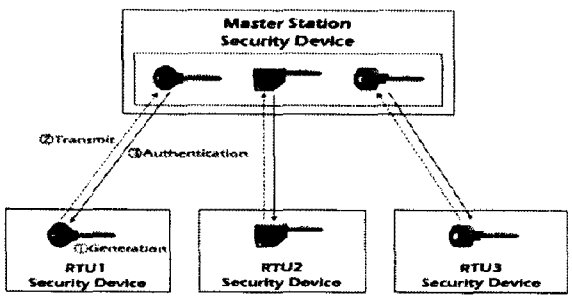

그림 9. SCADA에서 키 분배 과정
Fig. 9. Key distribution process in SCADA

3. 결 론

국가 주요 기반 시설물뿐 아니라 산업전반의 감시 제어에 널리 이용되는 SCADA 시스템의 통신 데이터의 보호는 안전한 SCADA 시스템의 운용 측면에서 중요한 문제다.

본 논문에서는 SCADA 시스템의 통신 데이터 보호 기술에 대해서 SCADA 시스템 개요, 전형적인 SCADA 시스템 구성, SCADA 시스템에 적용되는 통신 프로토콜, SCADA 통신망 침입, 암호화 기술, 상호 인증 기술, 미국의 DOE에서 지원하여 개발된 암호화 장치의 시작품, 적용 개념 및 키 분배 개념에 대해서 전반적으로 간략하게 기술하였다.

국내에서도 현재 이 분야의 연구가 시작되어 현재 초기적인 연구가 진행되고 있는데, 특히 이 분야는 전력, 통신, 시스템 등 다양한 요소기술이 필요한 융·복합적인 기술 분야로 추후 많은 공동 연구가 수행될 것으로 판단된다.

참 고 문 헌

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

[2] Hank Kenchington, "Securing Control Systems in the Energy Sector", Presentation Material, DOE

[3] Rolf Carlson: Sandia SCADA Program: High-Security SCADA LDRD Final Report, Sandia Report, SAND2002-0729, April 2002

[4] NERC, Security Guidelines for the Electricity Sector, June 2002

[5] Yongge Wang and Bei-Tseng Chu, "sSCADA:Securing SCADA Infrastrure Communications", http://eprint.iacr.org/2004/265.pdf, 2005

[6] V.M. Igure, S.A. Laughter, R.D. Williams: "Security issues in SCADA networks", Computer&Society, Vol.25, pp. 498-506, 2006

[7] H.M. Kim and D.J. Kang, "Security issues in SCADA networks", Computer&Society, Vol.25, pp. 498-506, 2006 "Security Issues & Application in Korea SCADA",Journal of the Korean Institute of Illuminating and Electrical Installation Engineers, Vol.21, No.9, pp.76-80, Nov. 2007

[8] D. Holstein, J. Tengdin, J. Wack, R. Bulter, T. Draelos and P. Blomgren, Cyber Security for Utility Operations, Final Report of NETL Project M63SNL34, 2005