Journal of the Korean Institute of Illuminating and Electrical Installation Engineers (2010) 24(4) : 25~32
DOI 10.5207/JIEIE.2010.24.4.025

논문 24-4-4

# 임베디드 리눅스 기반의 SCADA 직렬통신 구간 암호화 장치 개발

## (A Development of Cipher Device based on Embedded Linux for Serial Communication in SCADA)

이종주* · 김석주 · 강동주**
(Jong-Joo Lee · Seog-Joo Kim · Dong-Joo Kang)

## 요 약

산업 기반시설의 감시와 제어를 담당하는 SCADA 시스템은 다양한 방법과 규약으로 통신 네트워크를 구성한다. 기존의 SCADA 설비와 규약들은 구현성과 활용성 그리고 효율성들이 강조된 반면, 보안과 관련된 사항은 고려되지 못하였다. 이러한 운용상의 신뢰성과 유연성의 증가로 성능은 향상되었으나 보안성은 상대적으로 취약하다. SCADA 시스템의 보안 취약성은 고장이나 오동작뿐만 아니라 외부 침입과 사이버 공격과 같은 잠재적 위험에 노출되어 전체 시스템의 붕괴를 가져올 수 있다.

따라서 보안상 여러 가지 위험 요소들에 대응하기 위하여 암호화 장치와 같은 보안 모듈의 도입이 필요하다. 본 논문에서는 SCADA 네트워크에서 계측·제어 명령을 수행하는 RTU, IED와 같은 설비들의 보안성 향상을 위하여 직렬통신 구간에서 사용할 수 있는 암호화 장치를 개발하고 제안하였다.

## Abstract

The Supervisory Control and Data Acquisition Systems (SCADA) system provides monitoring, data gathering, analysis, and control of the equipment used to manage most infrastructure. The SCADA Network is implemented in a various manner for larger utilities, and multiple types of protocol and communication interfaces are used to network the control center to remote sites. The existing SCADA equipment and protocols were designed and implemented with availability and efficiency, and as a result security was not a consideration. So, performance, reliability, flexibility and safety of SCADA systems are robust, while the security of these systems is often weak. This makes some SCADA networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions to the infrastructure.

To reduce the risks, therefore, there is a need to have a security device such as cipher devices or cryptographic modules for security solutions. In this paper we develop an embedded cipher device for the SCADA equipment. This paper presents a cipher device designed to improve the security of its networks, especially in the serial communication.

Key Words : SCADA Security, Cipher Device, Cyber Security, Serial Communication, Key Exchange

* 주저자 : 한국전기연구원 위촉선임연구원
** 교신저자 : 한국전기연구원 선임연구원
Tel : 031-420-6188, Fax : 031-420-6189, E-mail : jongjoo@keri.re.kr
접수일자 : 2009년 11월 3일, 1차심사 : 2009년 11월 6일, 심사완료 : 2010년 1월 26일

## 1. 서 론

정보·통신 기술의 발달과 다양한 유·무선 통신 방식의 도입으로 기존의 SCADA(Supervisory Control And Data Acquisition)는 개방형 시스템으로 확장되고 있다[1-2]. 이는 시스템의 유연성과 접근성 향상으로 운용상의 효율을 가져오는 반면, 상대적으로 많은 연결과 접속지점의 허용으로 외부 노출과 침입에 대한 약점이 발생된다. SCADA 통신망 침입 그리고 정보 유출과 특정 정보에 대한 위·변조 등의 악의적 공격이 발생할 경우 이로 인한 피해와 파급효과는 매우 크다. 실제로 외국의 경우 이러한 피해 사례와 위협들이 보고되고 있다[3-6].

이처럼 SCADA 시스템의 관리 대상과 처리하는 정보의 중요성이 증가됨에 따라서 보안성 향상을 위한 취약성 분석 기법과 사이버 공격이나 침임 그리고 정보 유출과 같은 위협에 대비하기 위한 기술들이 요구된다. SCADA 상위의 고속 통신망은 안정적인 정보관리와 처리를 위하여 침입탐지 또는 방지시스템과 같은 보안 대책을 마련하고 있으나 현장에서 계측 정보를 수집하거나 원격지의 명령을 수행하는 설비들은 상대적으로 보안성이 취약하다. 즉, 출입과 같은 물리적 보안 절차를 만족할 경우 하위의 단말 장치들은 통신 구간에서 외부의 침입이나 악의적인 정보의 위·변조 공격에 대응할 수 있는 기능이 부족한 실정이다.

SCADA 시스템을 대상으로 하는 잠재적 위협과 공격 가능성이 증가됨에 따라서 통신규약을 비롯한 구성 장치와 설비에 대한 보안성 향상 방안들이 연구되고 있다[6-8]. SCADA 시스템의 보안성 향상은 기존 설비를 개량·개선하는 방법과 차세대 설비로 교체하여 사이버 보안에 대비하는 것으로 구분되며, 암호화 장치나 인증 시스템을 기존 설비에 도입하는 방법과 현재 사용하고 있는 통신규약이나 운용 프로그램의 취약성을 분석하여 개선하는 방법들이 검토되고 있다[8-9].

본 논문에서는 상대적으로 보안성이 취약한 RTU(Remote Terminal Unit) 및 IED(Intelligent Electronic Device)와 같은 하위 현장 설비들에 대한 보안 대책으로 해당 설비의 통신포트에 직접 연계하거나 적용할 수 있는 암호화 장치를 제안하였다.

상위의 제어명령을 직접 수행하고 계측정보를 원격지 서버로 전송하는 현장설비들은 직렬통신 방식을 이용하여 정보를 교환한다. 하지만 공개된 통신규약과 침입탐지 또는 방지시스템이 없는 직렬통신 구간에서는 탭핑(tapping)과 같은 방법으로 현장설비들에 대한 접근이 가능하다. 따라서 악의적인 제어 명령이나 계측정보의 위·변조를 방지하기 위한 직렬통신 구간 암호화 장치와 같은 대책이 필요하다.

제안된 장치는 제어 대상의 중요도와 구성에 따라서 암호 키를 분류하고 통신 선로의 침임이나 물리적 키 유출의 대비책으로 총 6단계의 보안 절차를 구성함으로서 안전성을 확보한 효과적인 SCADA 통신을 구현할 수 있다. 암호화 장치는 임베디드 리눅스 기반으로 직렬통신 디바이스 드라이버, 키 교환 및 암·복호 처리 태스크 등의 연동으로 구성되며, SCADA 통신 규약으로 널리 사용되고 있는 Modbus와 DNP 방식을 채용한 RS232와 RS485 구간에서 기능 및 성능 평가를 수행하였다.

## 2. 암호화 장치 구성

SCADA 직렬통신 구간 암호화 장치는 기존 설비들의 통신포트에 접속되어 정보를 송·수신하고, 암호화 장치간의 암·복호 처리 기능으로 암호통신을 수행한다. 부가적으로 장치간의 인증(ID certification)과 키 교환(key exchange), 키 갱신 절차가 수행되며 외부의 물리적 침입에 대비한 탬퍼(tamper) 기능을 제공한다. 또한 통신규약과 접속 방법 및 구조(topology)를 고려하여 1 : 1(point-to-point), 1 : N 또는 다중접속(multi-drop)을 수용할 수 있도록 구성하였다.

### 2.1 암호화 장치 H/W 구조

암호화 장치 하드웨어 구성은 RTU 또는 IED와 같은 기존 설비들과 통신을 수행하는 평문 통신포트와 암호화 장치간의 암호문 통신을 위한 암호문 통신포트로 구성된다. 평문 통신포트에서 수신되는 정보는 암호화 처리 후 암호문 통신포트로 전송되며, 암호문

통신포트로 수신된 정보는 복호되어 평문 통신포트로 전달된다.

구성된 암호화 장치는 고속 암 · 복호 처리를 위하여 PowerPC 440EPx(667[MHz]) 프로세서를 사용하였으며, 임베디드 리눅스(커널 버전 2.6.24) 운영체제를 탑재하였다.

프로그램 수행과 시스템 정보의 저장을 위하여 각각 256[M](SDRAM)와 64[M](Flash RAM)의 용량을 할당하였다. 또한 암호화 장치의 키와 설정 · 변수 값들을 관리하기 위하여 물리적으로 분리된 1[Mb](SRAM) 용량의 메모리를 탬퍼 기능과 연동되도록 하였다. 그림 1은 구현된 암호화 장치를 나타낸 것이다.

그림 1. 구현된 암호화 장치
Fig. 1. SCADA Cipher Device

암호화 장치의 하드웨어 구성과 통신 구간은 그림 2에 도시한 방식으로 운용된다. [A]와 [C]는 평문 통신구간으로 각각 RTU와 서버측 통신포트와 접속되며, [B]는 암호 통신구간으로 평문 통신포트로 송 · 수신된 정보를 암호문 형식으로 재전송하는 구간이다.

통신 포트는 RS232규격의 DB9으로 구성되었으며, Txd, Rxd, RTS, CTS, DSR, DTR, RI, CD의 모든 신호를 제어할 수 있으며 최대 1.5[Mbps]의 전송속도를 지원한다. 동작중인 암호화 장치의 상태를 감시하거나 설정하기 위하여 별도의 제어포트에 접속하여 조작할 수 있다.

탬퍼는 휘발성 메모리(SRAM) 영역에 보관되어 있는 암호 알고리듬, 통신속도, ID와 같은 설정값과 교환된 키 정보들의 물리적 침입과 노출을 대비한 보안 기능이다. 암호화 장치 복제나 메모리 영역접근을 통한 키 정보 유출을 목적으로 하는 외부의 물리적 조작이나 분해를 방지하기 위한 것으로 탬퍼 기능이 수행되면 정보를 관리하는 메모리 영역은 제거되며, 이로 인하여 암호화 장치는 불능(function disable) 상태가 된다.

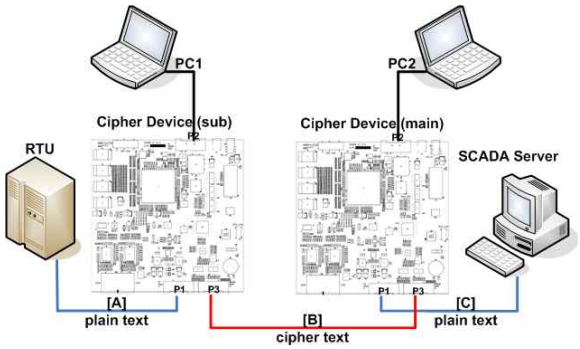


그림 2. 암호화 장치 결선 및 통신 구간
Fig. 2. Communication Interface of Cipher Device

## 2.2 암호화 장치 S/W 구조

암호화 장치의 소프트웨어는 리눅스 운영체제에서 동작하는 태스크(task) 프로그램으로 구성된다. 주요 기능과 처리 태스크는 통신포트를 관리하는 직렬통신 디바이스 드라이버(device driver)와 송 · 수신된 정보의 암 · 복호 처리, 장치들 간의 통신 세션(session)과 키 교환 절차 태스크, 키 값과 암호화 관련 설정 정보를 관리하는 램 디스크(ramdisk), 물리적 침입 감지와 램 디스크 제거를 위한 탬퍼 그리고 새로운 키 발생과 갱신을 위한 태스크들로 구성된다.

- 직렬 통신 디바이스 드라이버
  - 평문 및 암호문 통신 포트 관리 · 제어
- 세션(Session) / 키 교환 태스크
  - 장치 인증, 키 교환 및 관리 · 제어
- 암 · 복호(encryption/decryption) 태스크
  - 정보의 암 · 복호 처리
  - Plain-text(평문), AES, ARIA, SEED
- 램 디스크

- 암호화 정보 및 장치의 설정 값 관리

· 탬퍼 태스크
- 물리적 칩임이나 램 디스크 접속 감시

· 키 발생 태스크
- 새로운 키 생성 및 갱신

· 타이머 태스크
- 주기적 키 갱신 및 시스템 클럭 관리

다음의 그림 3은 상기 나열한 암호화 통신 장치를 구성하는 주요 기능들의 상관관계를 나타낸 것이다.

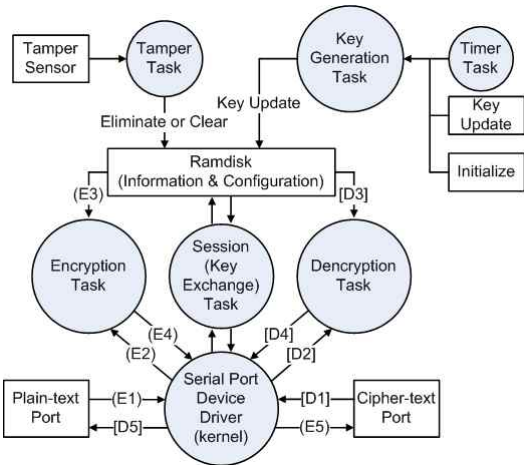


그림 3. 암호화 장치 주요 태스크 블록도
Fig. 3. Task Diagram of Cipher Device

그림 3에서 평문 통신포트로 전송되는 정보는 (E1)→(E2)→(E3)→(E4)→(E5)의 순서로 암호문 처리되어 전송된다. (E1)에서는 평문으로 전송된 정보를 수집하여 (E2)의 암호화 태스크로 평문을 전송한다. (E3)에서 암호 키를 램 디스크에서 가져온 뒤 암호문으로 처리되며, 암호화된 정보는 (E4)에서 직렬포트 디바이스 드라이버로 전달되어 (E5)의 암호문 통신포트로 출력된다. 반대로 암호화된 정보가 암호문 통신포트로 수신되면 [D1]→[D2]→[D3]→[D4]→[D5]의 순서로 복호되어 평문 통신포트로 전송된다.

램 디스크에서 관리되는 키 값과 선정된 알고리듬 및 기타 설정 값들은 각각의 태스크 처리 과정에서 해당 정보의 갱신여부를 상시 확인한다.

## 2.3 키 교환 절차

구현된 암호화 장치는 키를 생성하고 배분하는 주(Main) 장치와 키를 요청하고 할당 받는 보조(Sub) 장치로 구분되어 키 교환 절차가 수행된다.

보안성 향상과 안전성 확보 그리고 키 교환 과정의 정보 유출을 대비하여 키 교환은 여러 단계의 절차와 과정을 통하여 암호 키를 공유한다.

구현된 키 교환 절차는 마스터 키(Master key, 이하 Mkey), 세션 키(Session key 또는 Uni-cast [1 : 1] key, 이하 Skey), 브로드캐스트 키(Broadcast; [1 : N] key, 이하 Bkey) 그리고 암호 키(Encryption key, 이하 Ekey) 들로 구분되어 각 단계별로 교환된다. 그림 4는 암호화 장치의 키 교환 절차를 나타낸 것이다.

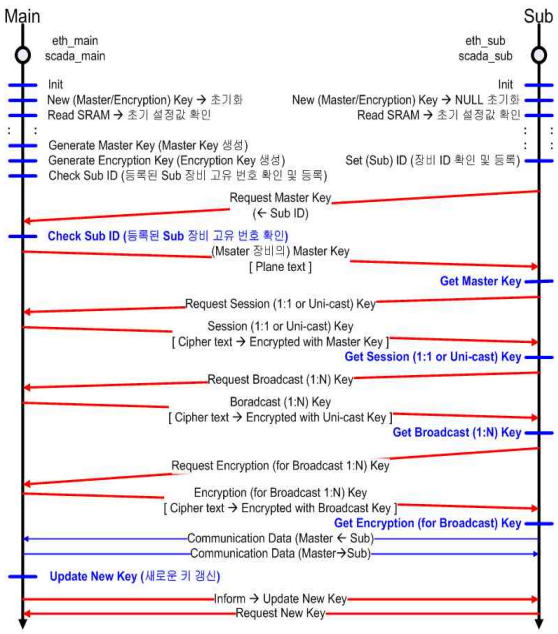


그림 4. 암호화 장치 키 교환 절차
Fig. 4. Key Exchang Procedure of Cipher Device

암호화 장치의 최초 접속은 보조 장치가 주 장치에게 Mkey를 요청하는 절차로 시작된다. 이때 각 장치들 갖는 16[byte] 크기의 고유한 인식번호(ID)가 전달되며, 접속 요청 허가를 위하여 주 장치에는 보조 장치의 ID가 사전에 등록되어야 한다. 만일 등록되지 않은

ID로 접속하거나, Mkey를 요청하는 경우 해당 장치는 거부된다. 최초 접속시 사전에 교환된 키 값의 부재로 Mkey 요청과 응답 프레임은 평문 형식으로 전송된다.

Mkey 교환 후에는 Skey 분배가 이루어지며, 키 교환 이후의 과정은 앞서 교환된 키 값으로 처리된 암호문이 전달된다. Skey는 1 : 1 통신을 위한 유니케스트(Uni-cast) 키로도 활용할 수 있다. Skey는 보조 장치가 Mkey로 처리된 암호문 형식으로 주 장치에게 요청한다. 주 장치는 수신된 Skey 요청을 Mkey로 복호하여 확인하고 합당한 요청인 경우 Skey를 Mkey로 암호화 하여 요청한 장치에게 전송한다.

1 : N 통신을 위한 Bkey 교환은 앞서 수행된 Skey로 암 · 복호 처리된다. Bkey는 주 장치와 연결되어 있는 모든 보조 장치들과의 통신에 사용되나, 실제 암 · 복호 키(Ekey)를 교환하기 위한 목적으로도 사용된다. Skey 교환 후 보조 장치는 Skey로 암호화된 Bkey 요청을 전송하고, 주 장치는 수신된 요청을 Skey로 복호하여 합당한 Bkey 요청인 경우 Skey로 처리된 암호문으로 Bkey를 전송한다.

표 1. 암호화 장치의 키 종류와 등급
Table 1. Features and Specification of Cipher Keys

| 명 칭 | 용 도 | 단계 |
|---|---|---|
| 장치 ID 등록/인증 | 접속 장치의 인증/식별 | 1차 보안 |
| 마스터 키 (Master key) | 최초 접속 수행 시 배분하는 (초기) 암호 키 → 세션 키 암호화 | 2차 보안 |
| 세션 키 (Session key) | 1 : 1 (Uni-cast) 통신 키 → 브로드 케스트키 암호화 | 3차 보안 |
| 브로드 케스트 키 (Broadcast key) | 1 : N 통신 키 → 암호 키 암호화 | 4차 보안 |
| 암호 키 (Encryption key) | 암 · 복호 키 → 평문 정보의 암호화 | 5차 보안 |
| 키 갱신 | 주기적/요청에 따른 갱신 → 장시간 키 사용 방지 | 6차 보안 |

Bkey 전송후 SCADA 통신시 서버 및 RTU와 접속된 장치들에게 Bkey로 처리된 암호문으로 암 · 복호 처리를 위한 Ekey 분배가 수행된다. Ekey을 끝으로 모든 키 교환 절차가 완료되면, Ekey를 이용한 암호문 통신을 수행한다. 다음의 표 1은 구현된 암호화 장치에서 교환되는 키 종류와 용도를 나타낸 것이다.

모든 키 정보들이 공유되면, 암호화 장치는 통신 구조와 목적에 따라서 키를 선택적으로 사용할 수 있다.

Skey와 Ekey는 사용자의 요청이나 필요에 따라 주 장치에서 갱신할 수 있으며, 특히 Ekey는 설정된 타이머의 주기에 따라서 자동 갱신된다. 키 값이 갱신되는 경우 주 장치는 보조 장치들에게 해당 키 정보가 갱신되었음을 통보하고 보조 장치들은 주 장치에 접속하여 갱신된 새로운 키를 할당 받는다.

## 3. 암호화 장치 구현 및 성능 평가

RTU와 IED 그리고 FEP(Front End Processor)로 구성된 장비들은 직렬통신(RS232 또는 RS485)으로 연결되며, DNP와 Modbus 규약을 이용하여 통신을 수행한다. 구현된 암호화 장치의 성능 평가를 위하여 그림 5에 나타난 구조의 SCADA 테스트베드를 활용하였다. 암호화 장치는 직렬통신 구간에 설치되며, 평문 통신포트는 SCADA 장비 그리고 암호문 통신포트는 상대측 암호화 장치와 연결된다.

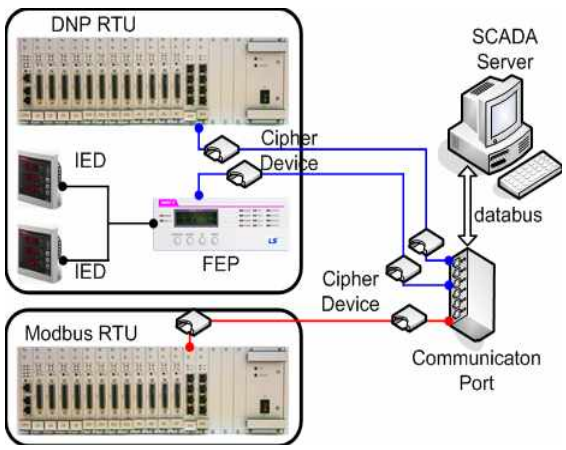


그림 5. 암호화 장치 시험 환경 테스트베드
Fig. 5. Testbed for Cipher Device

구현된 암호화 장치의 성능은 통신규약에 따라서 입력 정보에 대한 암·복호 및 통신 속도에 따른 처리 시간으로 평가할 수 있다.

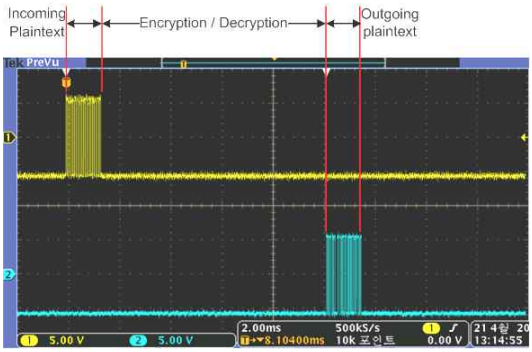


그림 6. 암·복호 처리 후 평문 신호 파형
Fig. 6. Plaintext Waveform after De/Encryption Processing

그림 6은 통신 속도는 9600bps에서 RTU와 연계된 암호화 장치의 평문 입력과 암·복호 처리 및 직렬통신 수행 후 SCADA 서버와 연계된 장치의 평문 출력을 측정한 것이다.

그림 7은 평문 입력포트 정보와 암호 처리된 암호문 통신포트의 출력, 그림 8은 암호화 장치의 암호문 입력신호와 복호된 평문 출력신호를 측정한 것이다.

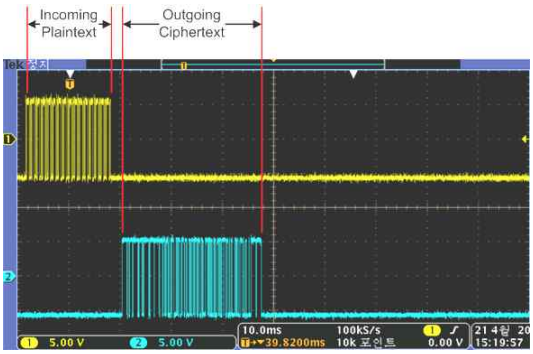


그림 7. 암호 처리 후 암호문 신호 파형
Fig. 7. Plaintext & Ciphertext Waveform after Encryption Processing

각 입·출력 신호의 지연 구간은 암·복호 처리 및 송·수신에 따른 통신 지연시간을 나타내며, 암·복호 처리 과정에 결과 그림 7의 입력신호와 그림 8의 복호된 출력신호가 일치함을 확인할 수 있다.

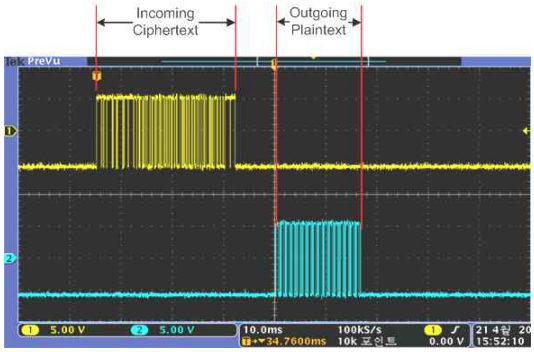


그림 8. 복호 처리 후 평문 신호 파형
Fig. 8. Ciphertext & Plaintext Waveform after Decryption Processing

암호화 장치에 구현된 암·복호와 통신관련 프로그램은 임베디드 운영체제에서 동작하는 태스크로 운영체제의 우선순위(time shared priority)와 스케줄링(queue scheduling)에 따라서 처리 속도의 변화가 발생한다. 다음의 표 2는 16[byte] 크기의 정보를 처리하는 암호화 장치의 성능을 실험적으로 측정한 것이다.

표 2. 암호화 장치의 평균 처리속도
Table 2. Latency of Cipher Device

| 처리방법 | 통신 속도 및 시간 | |
|---|---|---|
| | 9,600[bps] | 115,200[bps] |
| 암호처리 통신 | 1.0~3.0[msec] | 1.0~2.4[msec] |
| 복호화 통신 | 6.0~8.0[msec] | 2.0~3.0[msec] |
| 암·복호 처리 통신 | 10~40[msec] | 5.0~10[msec] |

표 3은 암호화 장치에서 선택 가능한 알고리듬의 암·복호 처리 속도를 나타낸 것으로 상대적인 처리 속도 비교를 위하여 3.9[Mbyte] 크기의 파일 처리 시간을 측정하였다.

암호화 장치를 사용하지 않는 직렬통신 구간에서는 설정된 통신규약에 따라서 평문 형식의 정보가 전달된다. 평문 형식의 정보는 탭핑과 SCADA 표준 통신규약을 지원하는 프로토콜 분석 툴을 이용하여 해석할 수 있다[10-11].

표 3. 암호화 알고리듬에 따른 처리 속도
Table 3. Latency of Encryption Algorithms

| 알고리듬 | aes 128-cfb | aria 128-cfb | seed 128-cfb |
|---|---|---|---|
| 암호화 | 0.348[sec] | 2.030[sec] | 0.479[sec] |
| 복호화 | 0.322[sec] | 2.003[sec] | 0.461[sec] |
| 조건 | 3974250 [3.9 M] 크기 파일의 암 · 복호 | | |

탭핑을 이용한 스니핑(sniffing)은 통신 네트워크에 송 · 수신되는 정보(traffic)을 감시하고 장시간 수집된 정보와 전송되는 정보들의 패턴을 분석하여 필요한 정보를 획득하는 기법이다. 또한 재생공격(replay attack)은 정보 프레임을 수집한 뒤 해당 메시지를 재전송함으로서 갱신되지 않은 정보의 전달이나, 대상 설비에게 정당한 정보 전송으로 인식시켜 오류를 유도하는 기법으로 평문 형식의 정보가 전송되는 통신 구간에서 발생할 수 있는 사이버 공격의 유형이다.

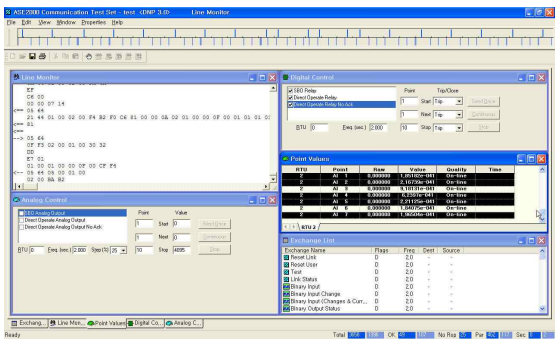

그림 9. 평문 전송시 통신 프레임 분석
Fig. 9. Data Frame Analysis of Plaintext

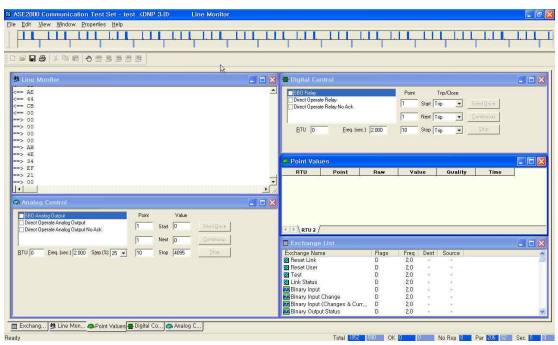

그림 10. 암호문 전송시 통신 프레임 분석
Fig. 10. Data Frame Analysis of Ciphertext

그림 9와 그림 10은 SCADA 직렬통신 구간에서 DNP 규약 프레임의 평문 형식과 암호화 장치에서 처리된 암호문 분석 결과를 나타낸 것이다.

평문 전송은 그림 9에 나타난 바와 같이 각 프레임의 종류와 규격에 따라서 해당 정보와 제어값이 구분되어 표시된다. 반면, 암호화 장치에서 처리된 암호문 전송은 표준 규약에 따른 프레임을 형성하지 못하여 그림 10에 나타난 바와 같이 프레임 부분(fragment) 오류로 표시된다.

암호문 통신 구간에서 수행되는 스니핑 기법은 암호화 장치에서 처리된 정보의 프레임 구조가 표준 통신 규약과 다름으로 정보를 바로 해석할 수 없다. 만일 통신 프레임이 분석되어도 실제 암호 키와 알고리듬을 모를 경우 스니핑이 불가능하다.

수집된 정보 프레임을 재전송하는 재생공격은 암호화 장치의 (주기적 또는 요청에 따른) 키 갱신으로 이전에 수집된 정보 프레임은 키 갱신 이후의 프레임과 다른 구조임으로 원하는 공격을 수행할 수 없다. 표 4는 직렬통신 구간에서 발생 가능한 사이버 공격과 암호화 장치의 대응 방식을 나타낸 것이다.

표 4. 사이버 공격에 대한 암호화 장치 대응
Table 4. Cipher Device Against to Cyber Attack

| 공격 | 공격 및 대응 방안 |
|---|---|
| 위장하기 (spoofing) | · 암호화 장치의 ID 도용<br>→ ID 인증 및 재접속 요청 관리 |
| 스니핑 (sniffing) | · 통신 데이터 프레임 수집 · 분석<br>→ 암호문 전송 : 통신규약 불일치 |
| 재생공격 (replay attack) | · 수집된 데이터 프레임 재전송<br>→ 주기적인 키 갱신 : 전송 프레임 무효화 |

또한 암호화 장치는 AES, ARIA, SEED의 암호 알고리듬을 채용하고 있으므로 알고리듬의 선택적 변경으로 암호 키를 변경하는 것과 같은 효과를 얻을 수 있다.

## 4. 결 론

다양한 통신 기술의 도입으로 SCADA 시스템의 유

연성과 접근성이 향상되고 있으며, 적용 분야와 대상도 증가하고 있다. 이러한 시스템의 확장은 운용상 효율이 증가하지만 상대적으로 많은 연결과 접속지점의 허용으로 외부 노출과 침입에 대한 보안 취약성이 발생된다. 특히, 계측·제어 명령을 직접 수행하는 하위 장치들의 직렬통신 구간은 중요성과 규모에 비하여 상대적으로 보안 대책이 취약하다. 따라서, 이에 대한 보안 대책과 취약성 대비가 필요하다.

본 논문에서는 직렬통신 구간의 보안성 향상을 위하여 임베디드 리눅스 기반의 암호화 장치를 구현하고, SCADA 테스트베드에서 성능 시험 및 사이버 공격에 대한 암호화 장치의 대응을 모의하였다.

특히 구현된 장치는 국내 표준 암호화 알고리듬인 aria, seed 뿐만 아니라 북미 표준으로 사용되는 aes 알고리듬을 병용함으로서 다양한 국가 표준의 직렬통신망에 적용될 수 있을 것으로 기대된다.

개발된 암호화 장치는 다음의 기능들을 추가적으로 개선하여 Smart Grid 기술 도입에 따른 다양한 통신 방식과 규약에 효과적으로 대비할 수 있을 것이다.

- 통신 속도 자동 검출
- 암호 통신 구간의 고속화
- 소형화 또는 모듈화
- 암호화 알고리듬의 공유 태스크 처리
- 암호화 장치의 핫 스왑(hot swap) 또는 핫 플러그인(hot plug-in) 지원

제안된 암호화 장치의 부가적인 기능 개선과 현장 실증을 통하여 향후 SCADA 시스템의 주요설비 보호와 악의적인 침입 및 해킹공격에 대한 대응 과 운영상의 보안성 향상에 기여할 수 있을 것으로 기대한다.

## References


[1] Gordon Clarke, Deon Reynders, "PRACTICAL MODERN SCADA PROTOCOLS", Newnes, 1 edition, September 2004.

[2] Krutz, R., "Securing SCADA Systems", Wiley Publishing, Indianapolis, Indiana, 2006.

[3] National Infrastructure Security Coordination Centre, "The electronic Attack (eA) Threat to Supervisory Control and Data Acquisition(SCADA) Control & Automation Systems", "NISCC Briefing 02/04, 2004.

[4] Hugh Njemanze, "SCADA Security Protections Are On The Increase", Pipeline & Gas Journal, February 2007.

[5] 이철원, "주요 제어시설의 사이버 보안 동향", 국가보안기술연구소, 2007년 4월.

[6] 이철수, "원방감시제어자료수집(SCADA) 시스템 보안성 강화 방안", 국가사이버안전센터, 사이버 시큐리티, pp. 8-17, 2005년 12월호.

[7] Erik Johansson, Teodor Sommestad, Mathias Ekstedt, "SECURITY ISSUES FOR SCADA SYSTEMS. WITHIN POWER DISTRIBUTION",.

[8] Dennis Holstein, John Tengdin, Jay Wack, Roger Butler, Timothy Draelos, Paul Blomgren, "Cyber Security for Utility Operations, Final Report - NETL Project M63SNL34", April 18, 2005.

[9] WRIGHT Andrew K, KINAST John A, MCCARTY Joe, "Low-latency cryptographic protection for SCADA communications", Applied cryptography and network security. International conference vol. 3089, pp. 263-277, June 2004.

[10] Applied Systems Engineering, SUBNET Solutions, Inc., "ASE2000 Communication Test Set User Guide - Document Version 2.2".

[11] TRIANGLE MICROWORKS, INC., "Communication Protocol Test Harness Product Documentation - Version 3.06", April 7, 2009.


## ◇ 저자소개 ◇


**이종주**(李種柱)
1975년 11월 27일생. 1999년 수원대학교 전기공학 졸업. 2001년 성균관대학교 정보통신공학부 대학원 졸업(석사). 2008년 동대학원 정보통신공학부(박사). 2001~2004년 새턴정보통신(주) 개발팀장. 2005~2007년 성균관대학교 정보통신용신기능성소재및공정연구소 연구원. 2008년~현재 한국전기연구원 전력시스템 연구본부 Smart Grid 연구센터 위촉선임연구원.

**김석주**(金碩柱)
1961년 12월 8일생. 1984년 연세대학교 전기공학과 졸업. 1986년 동대학원 전기공학과(석사). 2007년 동대학원 전기전자공학과(박사). 1987년~현재 한국전기연구원 전력시스템 연구본부 Smart Grid 연구센터 책임연구원.

**강동주**(姜東周)
1975년 9월 9일생. 1999년 홍익대학교 전자전기제어공학과 졸업. 2001년 동대학원 전기정보제어공학과 졸업(석사). 2001년~현재 한국전기연구원 전력시스템 연구본부 Smart Grid 연구센터 선임연구원.