한국항행학회 논문지 제17권 제6호 2013년 12월 (JKONI 17(6): 712-719, Dec. 2013)

스마트 워터그리드 네트워크의 원격 단말기 보안을 위한 암호화 모듈에 관한 연구

A Study on Encryption Module for Remote Terminal Security of Smart Water-Grid Network

박승환*, 박형모**, 김창복***0

Seung-Hwan Park*, Hyung-Mo Park**, and Chang-Bok Kim***0

요 약

본 논문은 스마트 워터그리드의 원격단말기와 상위 서버단간의 검침 및 제어 데이터의 안정적 전송을 위한 보안모듈에 대해 연구하였다. 제안한 보안모듈은 기존에 보급되어 사용 중인 보안성 없는 원격 단말기에 부착할 수 있도록 구현되었다. 특히, 전기 분야의 스마트그리드와는 달리 스마트 워터그리드는 배터리 전원을 사용하므로 저 전력을 고려하였으며, 지하에 설치되는 계량기 위치에 의한 습하고 열악한 환경이 대단위 네트워크 시스템 구축 시 통신 장애 발생시키는 점을 고려하여 ARIA-GCM-128 대칭키 방식을 채택하였다. 본 논문의 암호화 모듈은 단말기의 검침 데이터와 상위 서버단의 제어 데이터에 대한 보안을 확보하고 임의로 위변조 되는 것을 방지하여 원격검침 시스템에 대한 안정성을 확보할 수 있도록 구현되었다.

Abstract

This paper studies the security module for the reliable transmission of the meter reading and the control data between the remote terminals and the upper server-side in smart water grid.

The proposed security module was implemented to make it attachable to the remote terminal without security function. In particular, unlike the smart grid of electric field, the low power is considered due to the use of battery power in the smart water grid, and the ARIA-GCM-128 symmetric key method is adopted taking into the account that the damp and constrictive environments by the installed meter location in the underground occur a communication obstacle on building of the large-scale network system. The encryption module of this paper was devised to ensure the safety between the reading data on the terminal and the control data from the upper server, and secure the stability of the remote meter reading system by taking protection against an arbitrary alteration or modification.

Key words : Smart Water Grid, Advanced Metering Infrastructure, Security Module, ARIA-GCM-128

I. 서 론

스마트 워터그리드(Smart Water Grid)는 기존의 수

* 을지대학교 의료공학과(Dept. of Biomedical Engineering, Eulji University)
** 패스태그(Pass Tech co., Ltd)
*** 가천대학교 IT대학 에너지 IT학과(Dept. of Energy IT, Gachon University)
· 제1저자 (First Author) : 박승환(Seung-Hwan Park)
0 교신저자 (Corresponding Author) : 김창복(Chang-Bok Kim, tel : +82-32-820-4294, email : cbkim@gachon.ac.kr)
· 접수일자 : 2013년 11월 12일 · 심사(수정)일자 : 2013년 11월 12일 (수정일자 : 2013년 12월 20일) · 게재일자 : 2013년 12월 30일
http://dx.doi.org/10.12673/jkoni.2013.17.6.712

자원 망에 ICT(Information Communication Technology) 기술을 융합하여, 분산된 수자원의 효율적인 통합관리를 통하여, 물 사용의 정보화와 지능화를 이루기 위한 기술이다[1]. 최근 국내의 스마트 그리드 연구는 대부분 전력분야의 스마트 그리드 관련 연구가 다수이며, 이를 물에 적용한 스마트 워터그리드 관련 연구는 초기적인 수준에 있다[2]. 그러나 클라우드 컴퓨팅(Cloud Computing) 확산, 지능형 검침 인프라(Advanced Metering Infrastructure) 기술 등 ICT의 기술 발전에 의해 활발한 연구가 진행될 것으로 예상된다[3].

현재 국내 수자원을 위한 네트워크 분야에서 원격 단말기, 중계기, 집중기 등을 이용한 상수도 관리시스템이나 원격 유·무선 단말기 등이 보급되고 있다. 또한, 이러한 인프라를 통해 수도설비에 센서를 설치하고 실시간으로 상수도 상태에 관련된 정보를 수집하여, 사용자의 인터넷과 모바일 디바이스에 서비스할 수 있다[4].

현재 스마트 워터그리드의 검침시스템은 측정된 검침정보가 그대로 송·수신되고 있어, 정보보안 문제가 발생하게 된다. 이러한 검침정보는 각 사용 가구에 대한 요금 책정의 기준이 되기 때문에, 위변조(Forgery)가 발생될 경우에 정확한 요금부과가 어렵게 되어 원격검침에 대한 신뢰성 저하를 일으키게 된다. 또한, 상위단 서버에서 원격지의 수량관리를 위한 밸브 제어장치 등에 제어 명령어 전달시에도 해킹 조작에 의한 큰 피해가 발생할 수 있다. 따라서, 원격으로 검침되어 전송되는 검침정보 및 서버의 제어 정보 등에 대한 안정성과 신뢰성을 확보할 수 있는 보안기술에 대한 필요성이 대두되고 있다.

본 연구는 기존에 설치된 보안성 없는 원격단말기에 보안 기능을 추가하기 위해 하드웨어 모듈을 구현하였다. 제안된 하드웨어 모듈은 국내의 해시 알고리즘 보안강도에 의거하여 SHA256(Secure Hash Algorithm 256), HMAC(Hash-based Message Authentication Code) SHA256을 사용하였다. 또한, 전기 분야의 스마트그리드와는 달리 스마트 워터그리드는 배터리 전원을 사용하므로 저 전력동작을 고려하였으며, 단말기의 설치 위치가 지하에 위치하고 습한 환경 등으로 통신 환경이 열악하여 대단위 네트워크 시스템 구축 시 발생되는 통신 장애를 고려하여, 블록 암호화 알고리즘으로 전력계량기의 국내 KS(Korean Industrial Standards) 스펙인 ARIA(Academy Research Institute Agency) - GCM(Galois Counter Mode)-128을 사용하였다.

본 논문은 2장에서는 관련연구로서 원격단말기의 보안에 대해서 서술하였으며, 3장에서 제안한 원격단말기의 보안모듈에 대해서 나타냈다. 또한, 4장에서 제안 원격검침 시스템의 구현결과와 검토를 하였으며, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 스마트 워터그리드의 원격단말기 보안

현재 스마트 워터그리드의 원격시스템은 보안처리 없이 그대로 송·수신되고 있어, 서비스 거부 공격, 개인정보 노출, 장치의 오작동 유도, 검침 및 제어정보의 위변조 등 다양한 보안 문제가 발생할 수 있다. 표 1은 스마트 워터그리드에서 발생할 수 있는 보안문제에 대해서 나타냈다.

스마트 그리드의 서비스 거부 공격은 DDoS 공격에 대한 효율적 탐지와 차단을 위해 기업의 전사적 보안상황판 같은 솔루션 구축이 필요하고, 차단하는

표 1. 스마트 워터그리드의 보안문제
Table 1. Security issues of smart water grid

공격유형	공격 내용
서비스 거부 공격	AMI의 대부분의 장치들은 한정된 컴퓨팅 자원을 가지고 있어, 약간의 트래픽으로도 서비스 거부 공격을 받을 수 있다.
개인 정보 노출	개인식별정보, 과금정보, 물사용정보, 개인행태 정보 등 다양한 정보의 노출은 프라이버시(privacy)에 관련되어 사회적인 파장을 미칠 수 있음
장치 오작동 유도	- 장치 설정, 동작 메시지 위변조 - 악성 코드 - 펌웨어(firmware) - 물리적 조작(physical tampering)
검침정보 변조	물 사용 정보를 변조하여 수용가에 책정된 과금 변조
제어신호 변조	스마트워터그리드 네트워크상에서 요구되는 각종 제어 시스템에 대하여 밸브, 수문제어등의 제어 명령 변조로 인한 대형사고 발생

방법으로 DNS 싱크홀, L7 스위치, 블랙홀 라우팅과 같은 방법이 요구된다. 또한, 개인정보 노출을 방지하기 위해, 각종 검색엔진에 대한 분석에 따른 인증 알고리즘을 강화할 필요가 있다.

특히, 스마트 워터그리드는 유·무선으로 검침 및 제어정보를 송·수신하기 때문에, 원격단말기에 직접 침입을 하거나 통신 데이터에 위변조 공격을 시도할 수 있다. 원격단말기는 상위 시스템과 주기적으로 정보를 송·수신하며, 이 과정이 정상적으로 수행되지 않을 경우, 물 수급 및 과금 등 다양한 문제를 발생할 수 있다. 따라서 스마트 워터그리드의 원격단말기는 도청 및 위변조 등의 공격으로부터 안전하게 보호받기 위해서 기밀성(Confidentiality), 무결성(Integrity), 부인방지(Non-Repudiation), 상호인증(Mutual Authentication) 등을 만족해야 한다. 또한, 원격단말기의 데이터 보호를 위해 서비스 제공에 필요한 최소 정보만 단말기에 저장하며, 원격단말기에 저장되는 중요 정보는 암호화하여 저장해야 한다.

원격단말기는 보안을 위해 다양한 암호 알고리즘을 적용할 수 있으며, 암호화를 통해 기밀성, 무결성, 부인방지, 상호인증 등의 다양한 보안 서비스가 가능하다. 원격단말기는 암호 알고리즘과 암호학적 강도 선정을 위해서 시스템 예상 수명과 보호되는 정보를 고려해야 한다. 일반적으로 암호 알고리즘이 n-비트 안전성을 가진다고 하는 것은 공격자가 2^n번의 계산을 해야만 올바른 키를 발견할 수 있음을 의미한다. 표 2는 미국 표준기술연구소 NIST(National Institute of Standards and Technology)의 시스템 수명에 따른 안정성에 대한 예측이다.

스마트 워터그리드에서 요구되는 시스템의 보급은 향후 10년 이내, 그리고 운용은 최소 20년 이상을 예상하고 있다. 이에 따라 원격단말기에 요구되는 암호학적 강도는 128-비트 안전성을 권고하고 있다.

표 2. 보안수명
Table 2. Security lifetime

보안수명	암호학적 최소 강도(비트)
<=2010	80
<=2029	112
> 2030	128

표 3. 암호 알고리즘
Table 3. Encryption algorithm

분류	암호 알고리즘
블록암호	ARIA-128[KS X 1213-1][RFC 5794] AES[FIPS 197]
블록암호 운용모드	GCM[SP 800-38D] CCM[SP 800-38C] ECB, CBC, CTR[SP 800-38A]
해시함수/ HMAC	SHA256[FIPS 180-3]/ HMAC-SHA256[FIPS 198-1]
난수발생기	CTR_DRBG[SP 800-90] Hash_DRBG[SP 800-90]
타원곡선	secp256r1(P-256), sect283k1(K-283)[SEC2][FIPS 186-3]
디지털 서명	ECDSA[ANS X9.62][SEC1] EC-KCDSA[TTAS.KO-12.0015] RSASSA-PSS[ANS X9.31]
키 설정	ECDH[ANS X9.63][SP 800-56A] ECMQV[SEC1][SP 800-56A] RSAES-OAEP[ANS X9.44]

표 4. 보안 슈트
Table 4. Security suite

Security Suite Id	Authentication algorithm	Encryption algorithm	Key transport method
0	AES-GCM-128	AES-GCM-128	Key wrapping using AES-128 key wrap
10	ARIA-GCM-128	ARIA-GCM-128	

따라서 원격단말기는 128-비트 암호학적 강도 및 표준 암호적용을 고려하여, 표 3과 같은 암호 알고리즘을 사용할 수 있다.

원격단말기는 네트워크 통신을 통한 안전한 데이터 전송을 위해 통신 데이터 보호에 명시된 요구사항을 만족해야 한다. 표 4에 이를 위한 보안 슈트(Security Suite)에 대해서 나타냈다.

ARIA는 2004년에 국가 표준 기본법에 의거, 국가표준(KS)으로 지정된 범용 블록 암호 알고리즘이다. ARIA의 블록 크기는 128비트이며, 키 크기는 128/192/256비트로 AES와 동일 규격이다. 또한, 전체 구조는 Involutional Substitution-Permutation Network로서 라운드 수는 키의 크기에 따라 12, 14, 16이다. ARIA는 경량 환경 및 하드웨어에서의 효율성 향상을 위해 개발되었으며, ARIA가 사용하는 대부분의

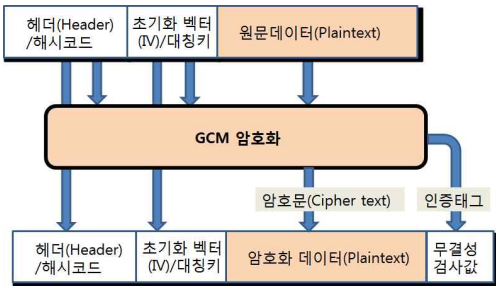

그림 1. GCM 암호화 및 캡슐화 과정
Fig. 1. GCM encryption and capsulation process

연산은 XOR과 같은 단순한 바이트 단위 연산으로 구성되어 있다[5][6]. ARIA는 1개의 블록을 암호화하는 기술이며, GCM은 몇개의 블록을 암호화하는 기술이다. 그림 1에 GCM의 암호화와 캡슐화 과정에 대해서 나타냈다[7].

GCM의 암호화 및 캡슐화 과정은 헤더와 초기화 벡터(Initialization Vector)가 전달되면서 수행된다. 헤더필드는 해시함수의 다이제스트를 HMAC에 의해 생성된 인증 데이터를 사용한다. 초기화 벡터와 대칭키는, 헤더필드 뒤에 포함시켜 원문 데이터와 함께 GCM 암호화의 입력으로 전달된다. GCM 암호화 알고리즘의 수행 후 캡슐화 과정에서 인증 데이터, 초기화 백터, 암호화 데이터와 함께 무결성 검사 값의 인증 태그가 추가된다. 복호화 과정은 암호화과정의 역순으로 처리된다.

Ⅲ. 제안 암호화 모듈

본 연구는 기존에 보급되어 설치된 보안성 없는 원격단말기를 교체하지 않고, 보안 기능을 추가하기 위해 하드웨어 보안모듈을 구현하였다. 제안된 하드웨어 보안모듈은 국내의 해시 알고리즘 보안강도에 의거하여 SHA256, HMAC-SHA256을 사용하였다. 또한, 전기 분야의 스마트그리드와는 달리 스마트 워터그리드는 배터리 전원을 사용하므로 저 전력 고려하였으며, 단말기의 설치 위치가 지하에 위치하고, 습한 환경 등으로 통신 환경이 열악하여 대단위 네트워크 시스템 구축 시 통신 장애를 고려하여, 블록 암호화 알고리즘으로 ARIA-GCM-128을 사용하였다. 그림 2에 스마트 워터그리드의 구성에 대해서 나타냈다.

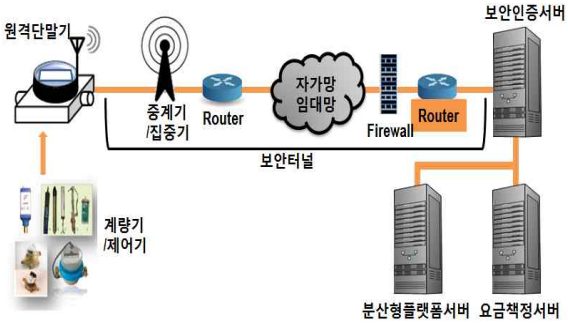

그림 2. 스마트 워터그리드 구성
Fig. 2. Construction of smart water grid

그림 2에서 계량기는 물 사용량을 검침하는 검침부, 검침정보를 저장하는 메모리, 메모리에 저장된 정보를 전송하는 통신부, 계량기를 제어하는 제어부로 구성된다. 계량기의 검침방식은 리드스위치 센서와 리드스위치를 사용하여, 전자식으로 검침하는 방식을 사용하였다. 원격단말기와 통신은 지그비(Zigbee), RF(Radio Frequency), 블루투스(Bluetooth) 등을 사용할 수 있다.

그림 2에서 원격단말기는 본 논문에서 구현한 하드웨어 보안모듈이 장착된다. 또한, 원격단말기와 상위 보안인증 서버간 보안터널은 암·복호화 모듈에 의해 안정적으로 데이터가 송·수신되는 공간이다. 원격단말기는 물 사용량, 현지의 수량, 수질 등의 데이터를 센서들을 통해 획득하고, 획득된 검침정보들을 보안모듈에서 암호화하여, 원격지에 위치한 보안인증서버에서 복호화된다. 또한, 관리서버에서 암호화되어 전송되는 제어정보는 원격단말기에서 복호화하여 단말기와 계량기를 제어함으로서 스마트 워터그리드 네트워크의 보안을 유지할 수 있다.

기존의 원격단말기는 수량 및 수질 검출센서, MCU(Micro Controller Unit), 메모리, 유·무선통신부, RTC(Real Time Clock), 전원부로 구성된다. 수량 및 수질 센서의 물리적 변화량은 검출부를 통해 신호증폭 또는 계측과정을 거쳐 디지털정보로 변환되어 메모리에 RTC에서 출력되는 실시간정보와 함께 메모리에 저장되고, 계측된 유효데이터는 유·무선 통신부를 통해 중계기 및 네트워크로 전송된다. 본 논문은 이러한 기존의 원격단말기에 보안을 위해 하드웨어 보안모듈을 구현하였다. 그림 3에 본 연구에서 제안한 하드웨어 보안모듈을 장착한 원격단말기를 나타냈다.

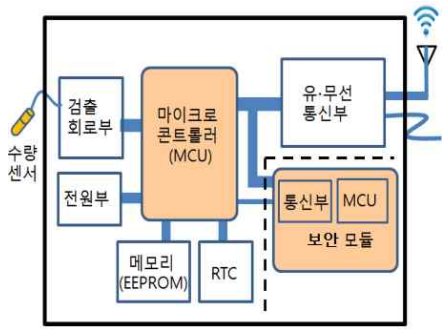

그림 3. 제안 원격단말기 구성
Fig. 3. Construction of proposed remote terminal

표 5. 전송 데이터
Table 5. Transmission data

항 목		타입	길이
Data	데이터길이	HEX	1
	계량기 번호	HEX	4
	제조일자	HEX	4
	검침값	HEX	4
	배터리	HEX	1
	상태	HEX	1

본 연구의 제안 보안모듈은 암·복호화를 위한 알고리즘을 내장시킨 MCU와 통신부로 구성된다. 여기서 보안모듈은 계량기의 검침데이터를 암호화하고, 관리서버의 제어데이터를 복호화하는 암·복호화 기능을 지닌다. 또한, 보안모듈의 통신부는 기존 단말기의 MCU로 부터 데이터를 입출력하는 기능을 지닌다. 표 5에 원격단말기의 보안모듈에서 암호화되어 전송되는 데이터에 대하여 나타냈다.

표 4에서 데이터 길이는 단말기에서 전송되는 데이터의 길이를 나타내며, 계량기 번호는 계량기 ID를 나타낸다. 또한, 제조일자는 YYMMDD으로 표시하며, 검침값은 사용자 검침정보로서 하위 3자리는 리터, 그 이상은 톤으로 표시한다. 배터리는 4단계로 표시하며, 3.6V는 3단계, 3.3V는 2단계, 3.0V는 1단계, 2.7V는 0단계이며, 배터리를 교체해야 하는 시점을 인식하는 기능으로 사용한다. 상태는 동파, 순간유량(대유량 누수), 누수(소유량 누수, 역류등 수자원에 대한 상태정보를 나타낸다.

본 논문은 국내의 해시 알고리즘 보안강도에 의거하여 SHA256, HMAC-SHA256을 사용하였다. 또한, 단말기의 설치 위치가 지하에 위치하고 습한 환경 등

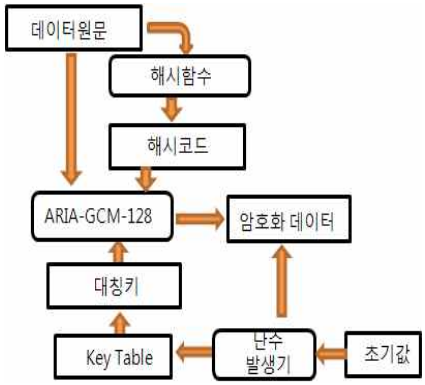

그림 4. 원격단말기의 암호화
Fig. 4. Encryption of a remote terminal

으로 통신 환경이 열악하여 대단위 네트워크 시스템 구축 시 통신 장애를 고려하여 블록 암호화 알고리즘으로 ARIA-GCM-128을 사용하였다. 그림 4에 원격단말기의 보안모듈에서 수행하는 암호화 과정의 흐름도를 나타냈다.

본 논문은 암호화를 위해 HMAC알고리즘을 사용하여 메시지 인증코드를 생성하고, 원문 데이터와 함께 블록 암호화 알고리즘에 전달한다. 또한, 난수발생기의 초기값을 이용하여 대칭키를 생성하여, 원문 데이터와 인증코드를 암호화 한다. 최종적으로 암호화된 데이터를 전송 포맷에 맞추어 데이터를 구성하여 전송하게 된다.

특히, 본 논문의 난수발생기 알고리즘은 의사 난수를 생성하는 PRNG(Pseudo Random Number Generator)를 이용하여 랜덤키(Random Key) 값을 선정하는 방법을 사용하였다. 또한, 난수를 발생하기 위해 종자(Seed) 값으로 계량기 ID, 검침 값, 단말기 ID, 전원 노이즈, RSSI, 계량값의 측정 및 전송 시간(RTC) 등을 사용할 수 있다.

Ⅳ. 보안 모듈 구현 및 검토

본 논문에서 제안한 보안모듈은 저전력 기반의 ST Microelectronics사의 STM8L151을 사용하여 하드웨어를 구현하였으며, 보안 암호화 프로그래밍은 C로 작성하였다. STM8L151은 ARM7 Cortex-M3 프로세서 설계구조의 MCU이다[8]. STM8L151 동작특성은 클록 16MHz, 동작온도 -40℃~125℃, 최저전력(Lowest Power) 0.4uA/MHz, 동작전력(Operating Power) 200

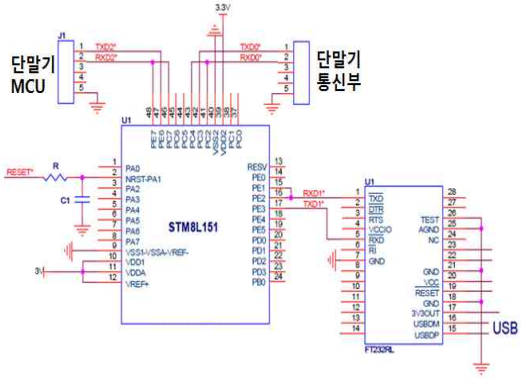

그림 5. 보안모듈 회로
Fig. 5. Security module circuit

uA/MHz 등의 특성을 보인다. 또한, STM8L151은 플래시메모리 64KB, SRAM 4KB, EEPROM 2KB의 메모리용량이 내장되어 있어 프로그램 코드와 데이터 저장용으로 사용된다[9]. 그림 5에 보안모듈 회로도를 보였다.

본 논문에서 제안한 보안모듈은 STM8L151에 내장된 3개의 직렬통신을 이용하며, 기존 단말기의 MCU와 유·무선 통신부를 직렬통신으로 데이터를 송·수신하고, 1개는 프로그램을 위한 통신용으로 사용하였다. 또한, 본 논문은 보안모듈의 시뮬레이션을 위해 직렬-USB 변환기인 FT232L를 사용하여 암호화 알고리즘을 실행시켰다.

제안 보안모듈의 암호화는 기존 단말기로부터 전송되는 검침데이터를 직렬통신으로 전송받아 암호화하여 유·무선 통신부를 통해 상위 서버단으로 전송된다. 또한, 제안 보안모듈의 복호화는 상위 서버단으로부터 단말기 제어정보를 수신하여, 보안모듈의 직렬통신장치를 통해 보안모듈로 전송되고, 복호화가 완료된 제어정보는 기존 단말기 MCU에 보내져서 단말기의 제어를 실행할 수 있도록 하였다. 그림 6에 본 연구에 사용된 암호화 모듈을 나타냈다.

그림 6에서 STM8L151의 보안모듈은 기존 단말기의 MCU, 유·무선 통신부, 프로그램 통신을 위해 3개의 직렬 포트를 사용함을 보였다. 또한, 암호화 알고리즘을 시뮬레이션 하기 위해 직렬-USB 변환기를 보였다. 그림 7에 본 논문에서 제안한 보안 모듈에서 구현된 암호화 결과에 대해서 나타냈다.

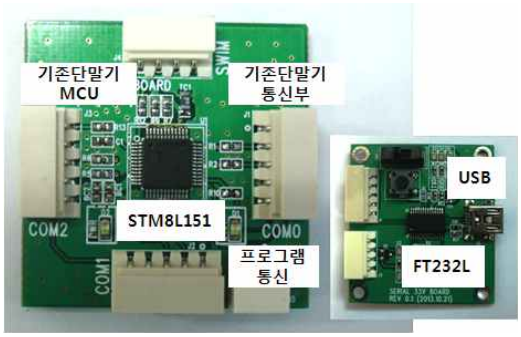

그림 6. 보안 모듈
Fig. 6. Security module

그림 7. 암호화 결과
Fig. 7. Encrypted result

PlainText는 보안이 필요한 원문 데이터로서 16바이트로 구성되어 있다. 이것은 수도계량기의 데이터가 16-32바이트 정도이기 때문에 16바이트로 시뮬레이션을 하였다. 전송데이터는 표 1에 나타낸 바와 같이 계량기 번호, 제조일자, 검침값, 배터리 사용량 등이다. HMACOut은 HMAC Key에 의해 생성된 인증데이터이다. PlainText + HMAC은 원문데이터와 인증데이터를 연접한 결과이다. 또한, Key는 사용된 대칭키이고, IV는 초기화 벡터이며, Encrypted는 최종적으로 암호화된 결과이다. 여기서 Tag는 암호문 뒤에 연접하여 전송할 무결성 검사 값의 인증 태그이다. 그림 8에 제안 암호화 모듈에서 구현한 복호화 결과에 대해서 나타냈다.

그림 8에서 복호화 결과는 암호화 과정의 역순이며, 최종적으로 전송된 암호화 문에 복호화 결과 평문이 동일함을 알 수 있다.

본 논문에서 제안한 원격단말기의 보안모듈의 특장점은 다음과 같다.

그림 8. 복호화 결과
Fig. 8. Decrypted result

1. 제안 보안모듈은 기존에 스마트 워터그리드에서 보급되어 사용 중인 보안성 없는 원격단말기를 그대로 사용하면서 보안모듈만을 추가하여 보안기능을 제공할 수 있도록 구현하였다.

2. 제안 보안모듈은 보다 암호화 강도를 높이기 위해 난수발생기의 종자값으로 시스템에서 발생하는 계량기 ID, 계량 값, 단말기 ID, 전원 노이즈, RSSI, 계량값의 측정 및 전송 시간(RTC) 등의 랜덤값을 사용할 수 있다.

3. 전기 분야의 스마트그리드와는 달리 스마트 워터그리드는 배터리 전원을 사용하므로 저 전력을 고려하여 설계하였다.

4. 계량기의 설치 위치가 지하에 위치하고 습한 환경 등으로 통신 환경이 열악하여 대단위 네트워크 시스템 구축 시 통신 장애를 고려하여 보다 간소화된 ARIA-GCM-128 대칭키 방식을 이용하였다.

V. 결 론

본 연구는 기존에 설치된 보안성 없는 원격단말기에, 보안모듈을 추가 삽입하여 인터페이스함으로써, 보안기능을 제공하기 위해 하드웨어 모듈을 구현하였다.

제안된 하드웨어 모듈은 국내의 해시 알고리즘 보안강도에 의거하여 SHA256, HMAC-SHA256을 사용하였다. 또한, 단말기의 설치 위치가 지하에 위치하고 습한 환경 등으로 통신 환경이 열악하여 대단위 네트워크 시스템 구축 시 통신 장애를 고려하여 블록 암호화 알고리즘으로 전력계량기의 국내 KS 스펙인 ARIA-GCM-128을 사용하였다. 특히, 또한, 전기 분야의 스마트그리드와는 달리 스마트 워터그리드는 배터리 전원을 사용하므로 저 전력 설계를 고려하였다.

본 논문에서 제안한 암호화 모듈은 검침단말기의 검침정보와 상위 서버 단에서 현지 단말기로 보내지는 각종 제어정보들에 대하여 도청 및 위변조를 방지함으로써, 스마트 워터그리드 시스템에 대한 안정성을 확보할 수 있다.

Reference

[1] S. K. Hong, "Future Active Water Resources Secure ment Technology", *Magazine of Korea water resourc es association,* Vol. 44, No. 8, pp. 14-18. 2011.

[2] S. H. Kim, H. J. Oh, J. H. Jung, W. J. Kim, and Y. H. Yoon, "A Study on the Development of Smart Water Grid Service", *Journal of the Korea Academia-Industrial cooperation Society,* Vol. 13, No. 12, pp. 6143-6150, 2012.

[3] M. G. Kang and S. J. Park, "Methodologies for Incorp orating Smart Water Grid into Water Resources Mana gement Considering the Outlook for Future Water Re sources", *2012 year Conference of Korea water resou rces association,* pp. 785-789, May 2012.

[4] Y. H. Hong, S. J. Song, and K. R. KO, "Service Technologies of Smart Home and Smart Water Grid", *Magazine of Korea water resources association*, Vol. 43, No.12, pp. 79-91, 2010.

[5] J. S. Hand and J. K. Choi, "Implementation of ARIA Block Encryption Algorithm", *The 35th Conference of Korea Information Processing Society*, Vol. 18, No. 1, pp. 64-67, May 2011.

[6] http://seed.kisa.or.kr/iwt/ko/sup/EgovAriaInfo.do

[7] D. McGrew, J. Viega, The Galois/Counter Mode of Operation (GCM), Natl. Inst. Stand. Technol., http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/prop

osedmodes/gcm/gcm-spec.pdf, May 31, 2005.
[8] Joseph Yiu, "ARM CORtex-M3 Complete Guide", pp.5-9. 2009.
[9]http://www.digchip.com/datasheets/parts/datasheet/456/ STM8L151.php

박 승 환 (Seung-Hwan Park)

1984년 2월 : 인하대학교 전자공학과 (공학사)
1990년 2월 : 인하대학교 전자공학과 (공학석사)
1995년 8월 : 인하대학교 전자공학과 (공학박사)
1995년 ~ 현재 : 을지대학교 의료공학과 교수
관심분야 : 임베디드MCU 응용, 신호처리, 의료기기 시스템

박 형 모 (Hyung-Mo Park)

1985년 8월 : 인하대학교 전자공학과 (공학사)
2000년 2월 : 모토롤라 스마트사업부 연구원
2002년 6월: 디지털패스(주) 대표이사
2005년 ~현재: 패스테크(주) 대표이사
관심분야 : RFID 시스템, 원격제어 및 모니터링

김 창 복 (Chang-Bok Kim)

1986년 2월 : 단국대학교 전자공학과 (공학사)
1989년 2월 : 단국대학교 전자공학과 (공학석사)
2008년 2월 : 인천대학교 컴퓨터 공학과(공학박사)
1994년 ~ 현재 : 가천대학교 IT대학 에너지 IT학과 교수
관심분야 : 인터넷보안, 클라우드 컴퓨팅, 모바일, 임베디드 시스템