USN 화재방재 시스템을 위한 보안 통신 구현 및 실험

김영혁† · 임일권† · 이재광††

요 약

USN 화재방재 시스템은 온도, 습도, 조도, 가속도, CO2 등의 다양한 센서로부터 얻는 데이터를 이용해 관리자에게 전달하고, 화재를 판별하는 화재 판별 알고리즘을 이용하여 소화설비를 동작시키는 지능적인 시스템이다. USN 화재방재 시스템은 센서의 데이터에 전적으로 의지하여 동작함으로 본 논문에서는 분산된 각각의 센서 데이터들을 임베디드 시스템 환경에서 효율적이고 안전하게 수집, 전달하기 위한 모델을 제안한다. 패킷의 구성과 패키징은 저 전력 소모를 위해 최대한 가볍고 빠른 처리 과정을 거치게 설계하였으며, 현재 나와 있는 암호화 알고리즘 중 DES, 3DES, AES, HIGHT를 각각 적용, 빠른 암복호화에 목표를 두어 최종적으로 국내에서 제안한 표준 암호화 알고리즘인 HIGHT가 잦은 센싱 시간을 요구하는 화재방재 시스템에 적합함을 확인하였다.

주제어 : USN, 화재방재, 보안통신

Security Communication Implementation and Experiments for USN Fire Prevention System

Young-Hyuk Kim† · Il-Kwon Lim† · Jae-Kwang Lee††

ABSTRACT

USN Fire Prevention System is an intelligent system that detects the fire through the value which has got from a sensor such as temperature, humidity, intensity of illumination, acceleration, carbon dioxide(CO2) and so on. And then send it to the operator also use the algorithmic fire detection to operate fire extinguish system on. It is among U-Disaster Prevention System which has prevented fire lately. Configuration of the packet was designed to make the most of lightweight and fast processing for low power consumption. Recently listed in the encryption algorithm is applied each DES, 3DES, AES and HIGHT. So objective was to faster encryption than encryption of high-performance finally domestic standard encryption algorithm HIGHT were suitable for the fire prevention system needed frequent sensing time.

Keywords : USN, FirePrevention, SecurityCommunication

† 준 회 원: 한남대학교 컴퓨터공학화 석사과정
†† 정 회 원: 한남대학교 컴퓨터공학화 교수(교신저자)
논문접수: 2010년 10월 21일, 심사완료: 2010년 11월 08일
* 본 논문은 2010년도 한남대학교 학술연구조성비 지원에 의하여 연구되었음.

1. 서 론

전 세계적으로 유비쿼터스 환경을 조성한 도시, 아파트, 학교, 직장 등이 구축 중이거나 구축되어 활성화되고 있다. 국내에서는 u-City를 국가 차세대 신 성장 동력으로 추진하기 위한 '유비쿼터스 도시건설 등에 관한 법률'을 제정하여 향후 건설되는 모든 신도시를 u-City로 추진하도록 제도적 근거를 마련하는 한편 국가 R&D 사업으로 연구하기 위해 u-Eco City 사업단을 발족하였다. u-Eco City의 제 2 핵심과제는 u-Space 구축기술로써 도시 시설물의 유지·관리 서비스의 고도화를 목표로 한 기술 개발과 지능형 도시 관리 및 제어 기술 고도화가 포함되어 있다. 그리고 이 서비스 기술 중 한 축이 u-방재 서비스이다.[1]

USN(Ubiquitous Sensor Network)이란 RFID (Radio-Frequency Identification)나 센서를 이용해 환경 정보를 획득하여 언제, 어디서나 필요한 정보를 제공하는 것을 말하며, 화재방재시스템이란 화재로부터 발생하는 열과 연기 등을 감지하여 화재 발생을 조기에 관계자에게 경보하여 주는 시스템이다.

USN 화재방재 시스템이란 기존 유선망을 이용한 화재감지와 경보 시설의 문제점인 발화위치의 식별 장애, 유선 선로망의 망실 등을 해결하고자 제시되는 USN 기반 화재방재 시스템으로 언제, 어디서나 환경정보를 감지하고 즉각적인 정보처리를 통해 화재 진압을 할 수 있다는 측면에서 화재방재 서비스의 새로운 대안으로 제시되고 있다.[2] 그러나 이와 같은 USN 화재방재 시스템은 온도, 습도, CO2 등 여러 센서들을 통해 수집과 분류되는 자료의 양이 많고, 실시간으로 내장된 화재 패턴탐지 기술을 통해 동시 처리되기 때문에 여타의 시스템들과 달리 센싱 데이터의 의존도가 매우 높고 센싱 데이터를 정확히 처리하지 못하면 자칫 화재가 아닌 경우에도 화재로 판단하는 오류를 범할 여지와 무선 네트워크를 통해 데이터가 이동함으로 악의적인 공격에 대처하여 재산적 피해 예방 조치를 할 필요가 있다.[3] 그리하여 본 논문에서는 크게 4 단계로 나누어 연구를 수행하였다.

첫째, USN 화재방재 시스템의 전반적인 이론과 배경 및 연구 수행 목적에 대하여 서론을 통해 밝힌다.

둘째, 목표로 하는 USN 화재방재 시스템과 각각 분산된 센서들의 데이터를 처리하기 위한 효율적인 패킷을 설계한다.

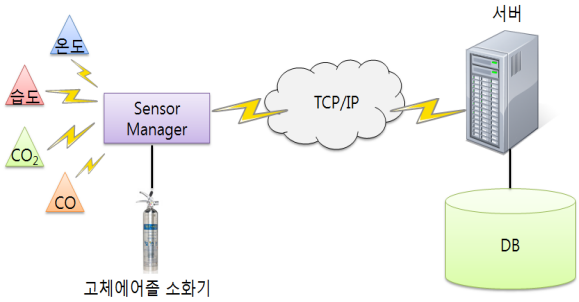
셋째, 악의적인 외부 공격에 의해 쉽게 조작되어 잘못된 소화설비 동작으로 인한 재산적 피해를 줄이기 위하여 암호화 기술을 선별하여 실험한다.

마지막으로 실험 결과를 토대로 결론을 맺는다.

2. USN 화재방재 시스템 통신 프로토콜 설계

2.1 USN 화재방재 시스템

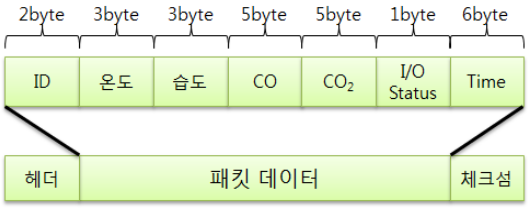
USN 화재방재 시스템은 여러 센서들을 관리하고 센싱 데이터를 수집 및 처리, 가공하는 역할을 하는 장치인 SM(SensorManager)과 가공된 센싱 데이터를 수신 받는 서버와 DBMS가 필요하다.



<그림 1> USN 화재방재 시스템 구성도

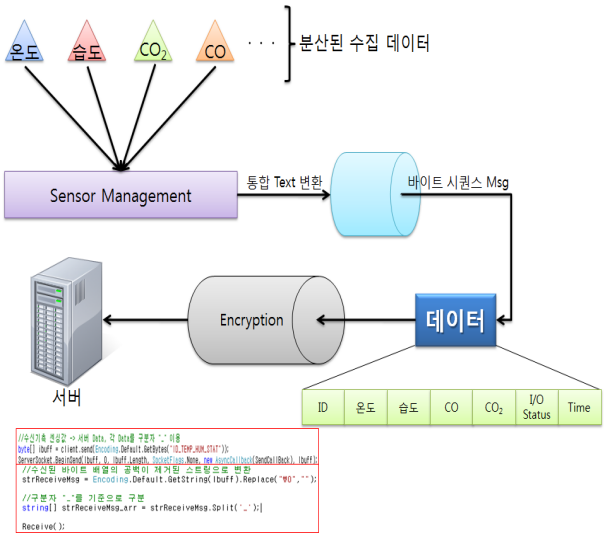
<그림 1>과 같이 USN 화재방재 시스템의 구성에서 가장 핵심적인 요소는 각 단대단에서 전달되는 데이터이다. 그러므로 시스템에 정의되어 있는 주기에 맞춰 센싱하여 획득한 데이터를 SM에 전송, SM에서 다시 서버로 전송되어 DBMS에 저장되는 One-Cycle 안에서 분산된 각각의 센싱 데이터의 패킷 구성 및 전송 메커니즘을 어떻게 구성하느냐에 따라 신뢰 및 안전성이 결정된다.

2.2 USN 화재방재 시스템 통신 프로토콜



<그림 2> 패킷 구조

<그림 2>는 USN 화재방재 시스템을 위해 구성한 데이터 패킷 구조이다. 통신 거리에 대한 제약과 단일 공간이 아닌 복합 공간에서 각 구역마다 온도 및 습도의 환경차이가 발생함으로 오류율을 낮추기 위해서는 구분된 공간마다 센서들과 SM을 구성해야 한다. 그러므로 서버는 여러 SM으로부터 전달되는 데이터를 구분하기 위하여 ID 값을 이용하고, SM에서 송신하는 시간과 서버에서 수신 받는 시간을 검사하여 네트워크상의 딜레이 차에 따라 데이터 유효성 여부를 판단하게 된다. 또한 SM에는 화재 진압을 위한 소화설비가 연결되어 있어 패킷 데이터에 포함되어 있는 I/O Status 값을 이용하여 소화기의 동작 여부를 판단, 추후 소화설비 작동시 DBMS에 기록된 로그를 토대로 어느 시점에 화재가 발생하고 언제 소화설비가 동작하고 중지되었는지 등의 정보를 알 수 있게 한다.



<그림 3> 데이터 처리 과정

그리하여 최종적으로 SM에서는 <그림 3>과 같이 분산된 수집 센서 데이터를 구분자 토큰을 삽입하여 통합 Text로 변환하게 된다. 그러면 통합 Text를 네트워크 전송을 위한 바이트 시퀀스 데이터로 변환하는 작업을 한 뒤 변환된 데이터를 암호화하여 서버로 전송한다.

2.3 USN 화재방재 시스템 적용 후보 암호화 기술

USN 화재방재 시스템은 각 센서가 1초마다 데이터를 수집하여 SM에 전송하고, SM에서는 수집된 데이터를 3초 간격으로 서버로 전송하게 된다. 3초의 간격을 정의한 이유는 복수의 센서로부터 데이터를 수집하기 때문에 전체 데이터를 모두 수집하여 가공해야하는 시간과 암호화를 위한 시간을 위함이며, 이와 같은 특성을 유지할 수 있는 암호화 기술을 확인하기 위해 다음과 같은 후보 기술을 선택하여 실험하였다.

2.3.1 DES(Data Encryption Standard)

가장 대표적인 블록 암호화 알고리즘으로 알려진 DES는 64비트의 데이터와 56비트 길이의 키를 사용하여 64비트의 암호화 결과를 생성한다. DES는 암호화, 복호화 알고리즘이 대칭적이며 치환(Permutation)과 대치(Substitution) 그리고 S_box로 구성된 블록 암호화 시스템이다.[4][5]

2.3.2 3-DES(Triple-Data Encryption Standard)

3-DES는 Triple DES 또는 DES 암호화 알고리즘을 다른 키에 3번 적용, 암호화-복호화-암호화 하여 DES-EDE(Encryption-Decryption-Encryption)라고도 불리는 기술로써, 현재의 컴퓨터 환경에 취약한 DES의 취약점을 보완하기 위하여 사용하기 시작하였으며 64비트의 키를 두 개 또는 세 개를 사용한다.[6][7]

2.3.3 AES(Advanced Encryption Standard)

AES는 Feistel 구조를 채택하지 않으며, 4개의 독립된 역변환 가능한 라운드 변환으로 구성된다. AES는 블록 길이를 128비트로 고정하고, 3가지

키 길이 128, 192, 256 비트를 사용한다. 암호에 필요한 라운드 수는 키 길이(Nk)에 따라 라운드 수(Nr)는 10, 12, 14로 다른 값을 갖게 된다. 일반적으로 AES는 강한 보안성과 적절한 암호화 속도를 가져 콘텐츠 암호화에 사용되고 있으나 많은 전력소모의 단점이 있다.[8][9]

2.3.4 HIGHT(HIGh security and light weigHT)

HIGHT는 RFID, USN 등과 같이 저전력·경량화를 요구하는 컴퓨팅 환경에서 기밀성을 제공하기 위해 2005년 KISA, 구)국가보안연구소 및 고려대가 공동으로 개발한 64비트 블록암호 알고리즘으로 128비트 마스터키, 64비트 평문으로부터 64비트 암호문을 출력하고, SEED, AES 등 기타 알고리즘보다 간단한 구조로 설계되었다.[10]

<표 1> Symmetric Cipher Block and Key Sizes

Cipher	Block Size	Key Length		
		Default	Minimum	Maximum
AES	16	16	16	32
Blowfish	8	16	0	56
DES	8	8	8	8
DES-EDE2	8	16	16	16
DES-EDE3	8	24	24	24
DES-XEX3	8	24	24	24
IDEA	8	16	16	16
RC2	8	16	1	128
RC5	8	16	0	255
RC6	16	16	0	255
Twofish	16	16	0	32

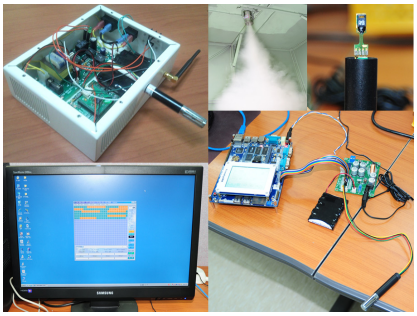
표 2 Plain Text Size(12 bytes) versus Cipher Text Size

Cipher	Block Size	Cipher Text Size					
		ECB	CBC	OFB	CTR	CFB	CTS
AES	16	16	16	12	12	12	-
Blowfish	8	16	16	12	12	12	12
DES	8	16	16	12	12	12	12
DES-EDE2	8	16	16	12	12	12	12
DES-EDE3	8	16	16	12	12	12	12
DES-XEX3	8	16	16	12	12	12	12
IDEA	8	16	16	12	12	12	12
RC2	8	16	16	12	12	12	12
RC5	8	16	16	12	12	12	12
RC6	16	16	16	12	12	12	-
Twofish	16	16	16	12	12	12	-

3. 실험 환경

3.1 실험 장비

<그림 4>는 <표 3> 장비들의 모습이며, 실험은 <표 3>과 같이 구성하여 실험하였다.

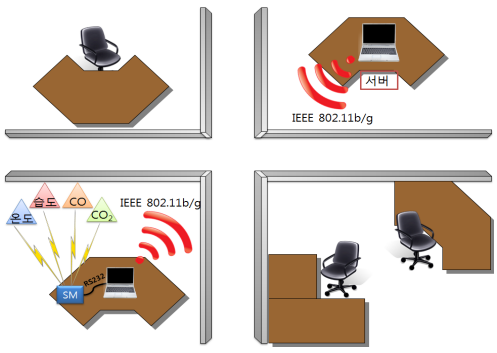


<그림 4> 실험 장비

<표 3> 실험 구성

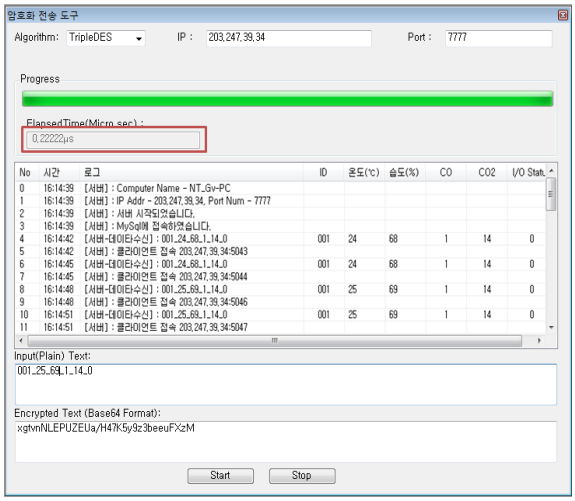
장비	구성
SM(Board)	ARM9 S3C2440 CPU : 533MHz RAM : 64MB SDRAM
Server	Intel Server
PC	CPU : 850MHz RAM : 64MB SDRAM
OS	Board : Linux Server : Windows Server 2008
DB	MySQL 5.1.39
S/W (자체개발)	SM-Server 통신 전용 소프트웨어 3-DES, AES, RSA, String Encryption, IDEA 암호화 소프트웨어

3.2 실험 시나리오



<그림 5> 실험 환경

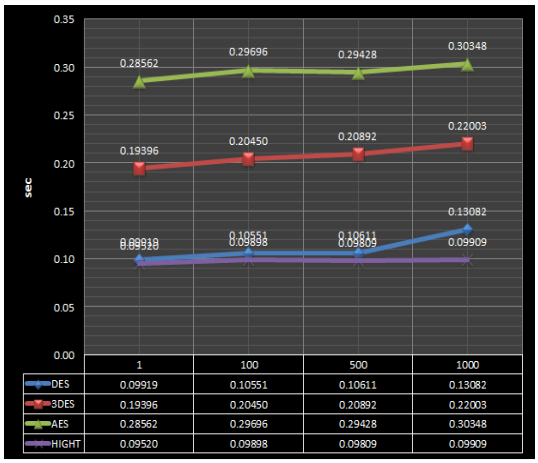
<그림 5>와 같이 SM에 PC를 시리얼 통신으로 연결하여 센서로부터 수집된 데이터를 가져오고, 가져온 시간과 암호화하여 전송하기까지의 시간을 <그림 6>과 같이 측정한다. 낮은 성능의 PC를 실험에 사용한 이유는 최대한 SM과 비슷한 환경을 위함이며, 총 1000회의 통신 과정에서 1, 100, 500, 1000회로 구분하여 소요되는 평균 시간을 측정하였다.



<그림 6> 실험 소프트웨어

4. 실험 결과

총 1000회에 걸친 실험 결과 <그림 7>, <표 4>와 같은 결과가 발생하였다.



<그림 7> DES·3DES·AES·HIGHT 비교 그래프

<표 4> DES·3DES·AES·HIGHT 결과표

	1	100	500	1000
DES	0.09919	0.11579	0.10314	0.13549
		0.19917	0.11160	0.10284
		0.11072	0.12038	0.10319
		.	.	.
		.	.	.
Average	0.09919	0.10551	0.10611	0.13082
3DES	0.19396	0.27848	0.29914	0.29914
		0.20873	0.19608	0.29608
		0.19797	0.20801	0.19483
		.	.	.
		.	.	.
Average	0.19396	0.20450	0.20892	0.22003
AES	0.28562	0.34319	0.29008	0.37417
		0.29531	0.30133	0.30556
		0.30366	0.30142	0.31018
		.	.	.
		.	.	.
Average	0.28562	0.29696	0.29428	0.30348
HIGHT	0.09520	0.09894	0.09769	0.09011
		0.09943	0.10020	0.09760
		0.09898	0.09006	0.10053
		.	.	.
		.	.	.
Average	0.09520	0.09898	0.09809	0.09909

5. 결 론

USN 화재방재 시스템은 다양한 센서들의 데이터를 통합적으로 수집·가공하여 화재를 판단하는 시스템으로써 개인적인 공간, 화장실, 탈의실 등의 Vision 시스템이 감시할 수 없는 공간까지도 대체할 수 있는 장점을 가지고 있는 반면, 화재를 판단하는 근거를 전적으로 데이터에 의존하게 되므로 외부의 악의적 공격 혹은 오류, 변형 등에 의해 보호하는 대상에 피해를 입힐 수 있다는 점에서 보안의 중요성은 매우 높다. 그리하여 본 논문에서는 블록 암호 알고리즘인 DES, 3DES, AES, HIGHT를 USN 화재방재 시스템 환경에서 실험하였다. HIGHT는 USN과 같은 저전력·경량화 환경을 위한 암호화 알고리즘인 만큼 속도면에서 가장 빠른 결과를 보였으며, AES가 가장 느렸으나 이는 HIGHT의 구조가 AES보다 간단한 구조로 동작함으로 인한 결과로 보인다. 그러나 1초 이상을 기준으로 센싱 하는 환경에서 AES의 속도는 문제가 되지 않는 수준으로 보이며, 이러한 여타 시스템에서도 요구되는 보안 수준과 환경 및 목적을 판단하여 암호화 알고리즘을 선택

하는 것이 필요하다.

향후에는 센서와 Vision 시스템이 결합된 복합 시스템으로의 전환이 발생하고 있으므로 센서 데이터와 영상 데이터가 혼재한 상황에서의 환경적 특성 분석과 프로토콜 설계, 화재판별 영상 데이터 암호화에 대한 연구가 필요하다.

참 고 문 헌

[1] 문창엽 (2010). U-Eco City 사업단. **한국지반환경공학회 지반환경, 11**(1), 67-72.

[2] 최갑용・엄정섭 (2009). USN기반의 화재 온도 데이터의 시·공간 분포특성 분석. **한국화재소방학회논문지, 23**(2), 41-48.

[3] 한국전산원 (2006). 2005년 USN 현장시험 결과보고서. NCA V-RER-05148

[4] 이완복・김정태 (2006). 파이프라인 구조의 3DES 암호알고리즘의 설계 및 구현. **한국해양정보통신학회논문지, 10**(2), 55-64.

[5] Raymond G. Kammer (1999). DATA ENCRYPTION STANDARD (DES). **FIPS PUB(FEDARAL INFORMATION PROCESSING STANDARDS PUBLICATION)**, 46-2.

[6] 김용희・정용진 (2008). 스마트카드 적용을 위한 저전력 통합 암호화 엔진의 설계. **전자공학회논문지-SD, 45**(6), 80-88.

[7] William C. Barker (2008). Recommendation for the Triple Data Encryption Algorithm(TDEA) Block Cipher. **NIST Special Publication**, 800-67.

[8] 유경인・김민재・이진영・조성제・김준모 (2008). 모바일 콘텐츠의 안전한 부분암호화 방법에 대한 연구. **한국정보과학회 종합학술대회논문집, 35**(1), 92-96.

[9] ADVANCED ENCRYPTION STANDARD(AES). **FIPS PUB(FEDARAL INFORMATION PROCESSING STANDARDS PUBLICATION)**, 197.

[10] 한국인터넷진흥원 (2009). HIGHT 블록암호 알고리즘 사양 및 세부 명세서.

김 영 혁

2009 한남대학교 컴퓨터공학과(공학학사)
2009~2010 한남대학교 컴퓨터공학과(석사과정)
관심분야: 네트워크, 정보보호
E-Mail: yhkim@netwk.hannam.ac.kr

임 일 권

2009 한남대학교 컴퓨터공학과(공학학사)
2009~2010 한남대학교 컴퓨터공학과(석사과정)
관심분야: 네트워크, 정보보호
E-Mail: iklim@netwk.hannam.ac.kr

이 재 광

1986 광운대학교 전자계산학(이학석사)
1993 광운대학교 전자계산학(이학박사)
1993~현재 한남대학교 컴퓨터공학과 교수
관심분야: 네트워크, 정보보호
E-Mail: jklee@hnu.kr