韓國컴퓨터情報學會 論文誌
第16卷 第8號, 2011. 8.

2011-16-8-3-2

6LoWPAN 단편화 패킷 재전송에 따른 암호화 알고리즘 성능 분석

김 현 곤*

Performance Evaluation of Cryptographic Algorithms for the 6LoWPAN with Packet Fragmentations

HyunGon Kim*

요 약

본 논문에서는 무선 구간에서 패킷 손실을 최소화 할 수 있는 재전송 기법과 기밀성 제공을 위해 암복호화 알고리즘을 적용한 6LoWPAN 프로토콜을 MICAz 센서에 구현하고 실험적인 성능을 분석하였다. 재전송 기법에서는 재생공격을 방지하기 위한 단편화 패킷 순서번호, 타임 스템프, 난스, 체크섬을 구현하였으며, 패킷 기밀성과 무결성을 제공하기 위해 AES, 3DES, SHA2, SHA1 알고리즘을 구현하였다. 실험 결과에 의하면 전송에러가 높아질수록 즉, 패킷 손실이 높아질수록 재전송이 급격하게 증가하고, 홉 수가 증가함에 따라 재전송이 비례적으로 증가함을 알 수 있었다. 그리고 암복호화 수행 시간이 재전송 처리 시간보다 상대적으로 크다는 것을 알 수 있었다.

▸ Keyword : 6LoWPAN, 단편화, 재조립, 보안, 기밀성

Abstract

In this paper we implement a 6LoWPAN protocol on the MICAz sensor platform, which could minimize packet re-transmission, and support security primitives for packet integrity and confidentiality. And we also present a performance evaluation of the implemented protocol calculated according to the cryptographic algorithms. In the re-transmission method, time stamp, nonce, and checksum are considered to protect replay attacks. As cryptographic algorithms, AES, 3DES, SHA2, and SHA1 are implemented. If transmission errors (thus, packet losses) and the number of hops are increase then, packet re-transmissions are increase exponentially from the experimental results. Also, the result shows that cryptographic operations take more time than packet re-transmission time.

▸ Keyword : 6LoWPAN, Fragmentation, Re-assemble, Securty, Confidentiality

• 제1저자 : 김현곤 • 교신저자 : 김현곤
• 투고일 : 2011. 03. 07, 심사일 : 2011. 04. 11, 게재확정일 : 2011. 05. 09.
* 목포대학교 정보보호학과(Dept. of Information Security, Mokpo National University)
※ 본 논문은 2009학년도 목포대학교 교내연구비 지원에 의하여 연구되었음.

I. 서 론

6LoWPAN(IPv6 over Low power Wireless Personal Area Network)[1~2]은 IP를 사용함으로써 기존에 구축된 통신 및 응용서비스 인프라를 그대로 이용할 수 있어서 비용이 절감될 뿐만 아니라 잘 알려지고 검증된 IP 기술들을 사용할 수 있어서 신뢰성과 안정성을 도모할 수 있다. 그리고 LoWPAN에서는 기존 네트워크들에 비해 상당히 많은 수의 센서 노드가 배치되어야 하므로 큰 주소공간과 자동 주소설정과 같은 기능을 내장하고 있는 IPv6가 적합하다. 센서 네트워크에 IPv6 기술을 접목하기 위한 표준화는 IETF의 6LoWPAN 워킹그룹에서 추진하고 있다. 계층 2에 IEEE 802.15.4[3~4]를 기반으로 하는 센서 네트워크에 IPv6를 지원하며, 통신 환경으로서는 저전력, 20~250Kbps의 데이터 전송률, 900~2400MHz의 주파수 대역에서 최소형 메모리와 최소형 프로세서만을 장착한 센서 응용을 대상으로 한다. 따라서 열악한 통신환경을 고려하여 어떻게 하면 데이터 전송속도가 느린 IEEE 802.15.4 기술을 통해 사이즈가 큰 IPv6 패킷을 효율적으로 그리고 안전하게 전달할 것인지가 주요한 이슈 중에 하나이다. 이를 위해 6LoWPAN 적응계층에서는 단편화(fragmentation)와 재조립(re-assemble), IPv6 헤더 압축, TCP/UDP/ICMP 헤더 압축 등의 기능들을 정의하고 있다.

그러나 현재의 6LoWPAN 적응계층 표준[1]에 의하면 보안에 대한 고려가 미흡하며 센서 네트워크에서 발생할 수 있는 재밍과 같은 물리적인 공격, 웜홀 공격, 블랙홀 공격, 재생공격 등 다양한 보안 취약점들에 노출되어 있다[5~6]. 따라서 보안 위협성(security threats)들과 다양한 공격 시나리오들이 분석되어야 하고 이를 기반으로 취약점들을 제거할 수 있는 보안 기술들이 정의되어야 한다. 한편, 6LoWPAN에서의 재전송 기법[7]과 재전송 기법에서 난스(nonce), 타임 스템프(time stamp), 체크섬(checksum) 등을 이용한 재생공격 방지 기법이 제안되었다[8]. 그러나 6LoWPAN 계층에서 센서 데이터의 위변조를 막을 수 있는 무결성과 센서 데이터의 기밀성을 유지하기 위해서는 암복호화 기법 적용에 대한 연구도 이루어져야 한다.

본 논문에서는 무선 구간에서 패킷 손실을 최소화 할 수 있는 재전송 기법과 기밀성 제공을 위해 암복호화 알고리즘을 적용한 6LoWPAN 프로토콜을 MICAz 센서에 구현하고 실험적인 성능을 분석하였다. 재전송 기법에서는 재생공격을 방지하기 위한 단편화 패킷 순서번호, 타임 스템프, 난스, 체크섬을 구현하였으며, 패킷 기밀성과 무결성을 제공하기 위해 AES, 3DES, SHA2, SHA1 알고리즘을 구현하였다.

본 논문의 구성은 제 1장의 서론에 이어, 제 2장에서는 관련 연구로서 6LoWPAN에서의 단편화와 재조립 기법, 패킷 재전송 기법, 6LoWPAN과 암복화 알고리즘의 구현 예에 대해서 기술한다. 제 3장에서는 본 논문에서 구현한 구현 환경, 소프트웨어 구조, 기능 등에 대해서 기술하고, 제 4장에서는 구현한 센서를 이용하여 성능을 분석하고 마지막으로 제 5장에서 결론을 맺는다.

II. 관련 연구

1. 6LoWPAN 적응계층

6LoWPAN 적응계층은 그림 1과 같이 상위의 네트워크 계층인 IPv6와 하위의 IEEE 802.15.4 MAC/PHY 계층 사이에 위치하여 기존의 두 프로토콜을 변형시키지 않고 그대로 접목되도록 중간에 가교 역할을 수행한다. IPv6 패킷의 MTU(Maximum Transmission Unit) 크기는 1,280 바이트이고, IEEE 802.15.4의 PPDU(Physical Protocol Data Unit)는 127바이트이므로 IEEE 802.15.4 프레임은 IPv6의 MTU를 그대로 탑재할 수 없다.

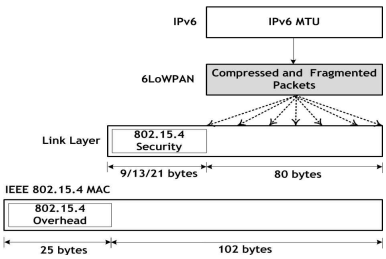

그림 1. 6LoWPAN 적응계층
Fig. 1. 6LoWPAN Adaptation Layer

또한 MAC 프레임 오버헤드가 25바이트를 차지하고, MAC 계층의 보안을 위해 최대 오버헤드를 차지하는 AES-CCM-128을 사용할 경우, 21바이트가 추가된다. 참고로 AES-CCM-32 또는 AES-CCM-64의 경우, 각각 9 또는 13 바이트가 추가된다. 이로 인해 IP 계층에서 사용할 수 있는 용량은 81바이트가 된다. 따라서 IPv6 패킷이 81바이트를 넘는 경우에는 패킷 단편화가 이루어져야만 IEEE 802.15.4 프레임에 탑재할 수 있다.

2. 패킷 재전송 기법

전송계층에서의 종단간 단편화로 인한 비효율성을 제거하

기 위해 6LoWPAN 계층에서 재전송을 하는 기법이 제안되었다[7]. 즉, TCP 등의 전송계층의 흐름제어를 최소화시켜 6LoWPAN 적응계층에 적용하는 것이다.

6LoWPAN은 저전력, 낮은 데이터 전송율 그리고 최소형 메모리와 최소형 프로세서만을 장착한 센서 환경이기 때문에 전송계층에서의 재전송을 최소화시켜 전송 효율을 높여야 할 필요가 있다. 둘째, 유선구간과 달리 무선 구간의 특성상 전파에 대한 간섭과 노이즈로 인한 성능저하와, 전송오류, 전파 간섭 등의 영향으로 비트 에러가 높기 때문에, 패킷 손실로 인한 전송계층의 재전송은 정상적인 통신을 방해하는 주요 요인이 될 수 있다.

한편, 6LoWPAN에서 재생공격으로 인한 패킷 단편화 패킷 재전송을 최소화할 수 있는 경량의 보안 기법이 제안되었다[8]. LoWPAN 적응계층에 보안 기능을 탑재하게 되면 보안강도는 높아지지만 단말의 성능저하와 비용이 증가된다. 보안이 요구되는 센서 네트워크 환경을 고려하면 6LoWPAN 적응계층의 특성상 초경량이고 추가적인 컴퓨팅 자원, 메모리, 센서 노드의 가격을 최소화할 수 있는 보안 메커니즘이 필요하다. 이를 위해 추가적으로 탑재되는 패킷의 양과 신호 메시지의 수를 최소화시켜야 한다. 이 기법에서는 단편화 패킷 재전송을 최소화시켜 저전력 통신을 이루고, 패킷의 신선도 유지 및 재생공격을 방지하고 있다. 패킷손실이 발생했을 때, 6LoWPAN 적응계층에서 재전송이 이루어지며, 통신 선로상에서의 데이터 손실을 검증할 수 있는 체크섬을 도입하여 데이터 무결성을 체크한다. 그리고 재생 공격으로 인한 재전송을 막기 위해 타임 스템프와 난스를 도입하였다.

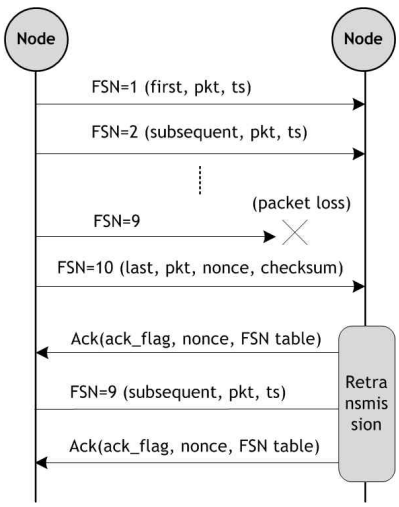

그림 2. 6LoWPAN 재전송 절차
Fig. 2. 6LoWPAN Re-transmission Procedure

하나의 IPv6 데이터그램이 다수의 단편화된 패킷들로 조각되어 전송되는 경우에, 그리고 중간의 단편화 패킷의 일부가 손실되었다고 가정했을 때, 참고문헌 [8]의 재전송 절차를 그림 3에 도시하였다. 예를 들어, 6LoWPAN 계층에서 전송해야 할 하나의 데이터그램 사이즈가 800바이트이고, 6LoWPAN 적응계층에서는 80바이트로 단편화 되어 전송되어진다고 가정하자. 우선 송신측 노드에서 단편화된 패킷 각각에 대해 순서번호 FSN(Fragmented Sequence Numb er)를 부여한다. 이 경우에는 단편화된 패킷 단위로 FSN이 10번까지 부여된다. 그림 2의 절차는 FSN 10번까지의 단편화된 패킷이 송신측 노드에서 수신측 노드로 전송되는 도중에 FSN 9번의 단편화 패킷이 손실되어 재전송되는 흐름을 보여주고 있다. 이 기법에서는 단편화 무결성과 재생공격을 방지하기 위하여 단편화 순서 번호, 타임 스템프, 난스, 체크섬을 도입하였다.

6LoWPAN 적응계층에서 단편화가 발생했을 때, 하위 계층인 IEEE 802.15.4 MAC/PHY에서의 에러 확률에 따른 6LoWPAN MTU의 전송시간과 홉 수에 따른 전송시간은 아래의 수식 (1)과 같다. 여기서 다중 홉 일 경우에는 다양한 네트워크 토폴로지가 아닌 단일경로를 가정하였으며, 재전송 타임아웃, 재조립 버퍼에 의한 지연은 고려하지 않는다 그리고 6LoWPAN MTU는 6LoWPAN 헤더, 재전송을 위해 추가된 단편화 헤더, 상위의 IP, TCP, 그리고 응용계층이 포함된 데이터를 의미한다. 하나의 MTU가 송신측 노드에서 수신측 노드로 전달되는 전체 전송시간은 아래와 같이 표현된다[8].

$$Trns_{tot} = (1 + N_{retrns}) \times \frac{(T_{frg} \times M_{nfrag}) + (N_{hop} \times D_{pro})}{(1-p_e)^{N_{hop}}} \quad \cdots\cdots (1)$$

여기서 p_e는 전송 에러 확률, $Trns_{tot}$는 하나의 MTU 전체 전송시간, M_{nfrag}는 하나의 MTU에 대한 단편화 개수, T_{frag}는 단편화 패킷 전송시간, D_{pro}는 홉과 홉 사이의 전파지연, N_{hops}는 홉 수, N_{retrns}는 재전송 횟수의 평균값이며 아래와 같이 계산된다.

$$N_{retrns} = \frac{1}{(1-p_e)} \qquad 0 \le p_e < 1 \quad \cdots\cdots (2)$$

3. 6LoWPAN과 암복호화 알고리즘 구현 예

6LoWPAN은 다양한 형태의 센서 하드웨어에 구현되고 있다. 대표적인 6LoWPAN의 구현으로 6lowpancli[9], b6lowpan [10], sicslowpan[11] 등을 들 수 있다[12~14].

6lowpancli은 TinyOS-2.x에서 구현되었으며 헤더 압축, 단편화, 어드레싱, IPv6 비상태형 주소 자동 설정 기능을 지원한다. 그러나 노드 발견 메커니즘, 메시 네트워킹, 이동성 프로토콜은 지원하지 않는다. b6lowpan은 동일하게 Tiny OS-2.x에서 구현되었으며 헤더 압축, 단편화, 어드레싱, 노드 발견, 링크 로컬 주소 설정, 라우터 광고 등을 지원한다. sicslowpan은 Contik OS에서 구현되었으며 기본적으로 MAC 계층에서 RIME이라 불리우는 non-IP 프로토콜을 적용한다. 기본적인 기능은 헤더 압축, 단편화, 어드레싱, 이웃 노드 발견을 지원하며, 메시 네트워킹, 이동성 프로토콜은 지원하지 않는다.

표 1. UDP 패킷 전송 시간(ms)
Table 1. Time Needed to send an UDP packet(ms)

바이트	32	64	128	256	512	1024
6lowpancli	26	40	52	104	182	334
b6lowpan	25	29	34	34	42	45
SICSlowpan	7	8	15	19	20	24

구현된 소프트웨어의 전송시간은 다음과 같다. UDP 패킷을 대상으로 패킷 사이즈에 따른 전송 시간을 측정하고 비교하여 표 1에 나타내었다[15]. b6lowpan을 기준으로 하였을 때, 1512 바이트를 전송하기 위해서는 약 42ms의 전송시간이 소요된다.

센서 환경에서 일반적인 보안 요구사항인 기밀성, 무결성, 인증, 부인방지가 구현되어야 하며, 이를 위한 암호학적 연산에 대한 성능이 분석되어야 한다. 참고 문헌 [16]에 의하면 MICAz 센서, ATMega128L, 클럭 속도 16MHz, 내부 SRAM 4KB, EEPROM 128KB 환경에서 128바이트의 평문을 암호화(encryption)화하는데 소요되는 시간은 표 2와 같다. 센서의 자원 한계로 인하여 알고리즘 수행시간이 많이 소요되는 것을 알 수 있다.

표 2. 알고리즘에 따른 128바이트 암호화 소요시간
Table 2. Encryption Time per Algorithms for 128bytes

알고리즘	키/해시	블록사이즈	측정된 처리시간
AES	192비트	128비트	800ms
3DES	192비트	64비트	890ms
SHA2	160비트	512비트	360ms
SHA1	512비트	512비트	26ms

III. 6LoWPAN 프로토콜 구현

6LoWPAN에서 재전송 기법과 암복호화 알고리즘이 결합되었을 때, 성능에 미치는 영향을 분석하기 위하여 MICAz 센서에 6LoWPAN 프로토콜을 구현하였다. 센서 운영체계는 Tiny OS 2.1을 기반으로 하였으며 그 외의 구현 환경은 표 2에 나타내었다. 재전송 기법은 참고문헌 [8]에서 제시한 알고리즘을 적용하였으며, 이 기법에서 제시한 단편화 패킷 순서 번호(sequence number), 타임 스템프, 난스, 체크섬 등을 구현하였다. 구현한 소프트웨어는 오픈 소스 b6lowpan[10]를 참조하였다.

표 3. 구현 환경
Table 3. Implementation Environments

Mode	MICAz
Microprocessor	ATMega128L(8bit)
Clock Speed	16MHz
Internal SRAM	4KB
EEPROM	128KB
Radio Frequency	2.4GHZ
Radio Chip	CC2420
Operating System	TinyOS 2.1
Program Language	NesC

구현한 전체 소프트웨어 구조를 그림 3에 OSI 계층별로 나타내었다. 본 논문의 주요 관심사인 6LoWPAN 블록에는 패킷 압축, 단편화와 재조립 등 RFC4944에서 정의한 기능들과 참고문헌 [8]의 재전송 기법과 암복호화 알고리즘들이 구현되었다.

암복호화가 성능에 미치는 영향을 분석하기 위하여 AES, 3DES, SHA2, SHA1 알고리즘을 NesC 응용 형태로 구현하였으며 알고리즘들의 키 사이즈와 블록 사이즈를 표 4에 나타내었다. 여기서 AES 알고리즘은 AES-CCM-128 모드만을 구현하였다.

표 4. 구현한 암복호화 알고리즘
Table 4. Implemented Cryptographic Algorithms

알고리즘	타입	키/해시	블록 사이즈
AES	블록	192비트	128비트
3DES	블록	192비트	64비트
SHA2	해시	512비트	512비트
SHA1	해시	160비트	512비트

6LoWPAN 소프트웨어 블록의 구조를 그림 3에 나타내었다. 블록은 단편화 유닛(Fragmentation Unit), 재조립 유닛(Re-assembly Unit), 암호 프리미티브 유닛(Cryptogra phic

Primitives Unit)으로 구성된다. 상위 응용 계층의 MTU는 암호 프리미티브를 통해 암호화 된 후, 단편화 유닛으로 전달된다. 반대로 하위 계층으로부터 수신한 패킷은 재조립 유닛을 거치고 복호화 된 후, 상위 응용 계층으로 전달된다.

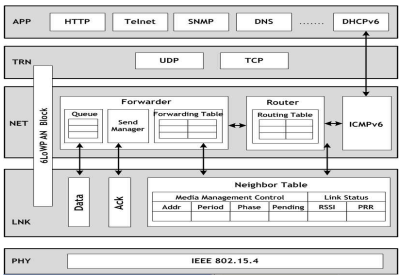

그림 3. 구현한 전체 소프트웨어 구조
Fig. 3. Overall Software Architecture

단편화 유닛의 주요 기능은 하나의 MTU를 다수의 단편화된 패킷들로 단편화 하는 것이다. 단편화된 패킷은 헤더 압축 과정을 거치며 최종적으로 6LoWPAN 포맷에 따른 패킷이 생성된다. 재전송을 위해 매 패킷마다 순서번호를 부여하며, 전체 패킷의 재전송을 감안하여 단편화된 패킷들은 버퍼링된다. 그리고 재전송 공격을 막기 위해 난스와 타임 스템프를 무결성을 제공하기 위해 체크섬을 포함시킨다.

재조립 유닛의 주요 기능은 다수의 단편화된 패킷들을 하나의 MTU로 재조립하는 것이다. 수신된 패킷은 압축을 해제한 후, 패킷 헤더를 추출하고 수신된 패킷들을 재정렬(re-ordering)해서 최종적으로 원래의 패킷으로 재조립 한다. 수신된 단편화 패킷들은 순서 번호를 가지므로 순서 번호 테이블을 운영한다. 만약 특정 단편화 패킷이 누락될 경우 송신측에 재전송을 요청한다.

암호 프리미티브 유닛은 다른 유닛에 암복호화 프리미티브를 제공한다. 즉, AES, 3DES, SHA2, SHA1 알고리즘을 사용할 수 있도록 API를 제공하며, 난수생성기 (PRNG; Pseudo Random Number Generator)를 제공하여 타 유닛이 난스를 사용할 수 있도록 해준다.

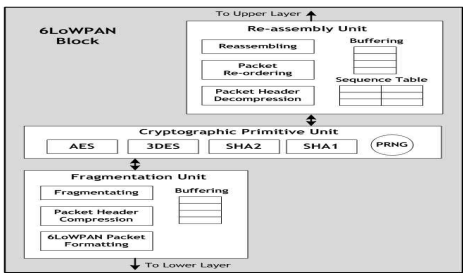

그림 4. 구현한 6LoWPAN 블록의 소프트웨어 구조
Fig. 4. Software Architecture of 6LoWPAN Block

IV. 실험에 의한 성능 고찰

재전송 기법과 암복호화 알고리즘을 구현한 6LoWPAN 센서를 대상으로 성능 분석 실험을 하였다. 센서 노드 사이에 하나 이상의 홉이 존재할 경우에는 네트워크 토폴로지에 대한 고려가 있어야 한다. 본 실험에서는 참고문헌 [16]과 동일한 성능 평가 방법을 따랐다. 단일 경로와 재전송 타임아웃은 고정하였으며, 재조립 버퍼에 의한 지연은 고려하지 않았다. 그리고 어드레스는 링크 헤더로부터 추출한 인터페이스 ID를 사용하였으며, 라우팅은 링크 로컬 유니캐스트를 사용하였다.

그림 5에 MTU 사이즈에 따른 전송 시간을 나타내었으며 각 전송 시간은 10회 평균의 결과 값이다. 여기서 MTU는 6LoWPAN 헤더, 재전송 기법의 단편화 헤더, 상위의 IP, TCP, 응용 등이 포함된 데이터를 의미한다. 그리고 MTU 전송 시간이란 하나의 노드에서 다음 노드로 전송되는 전체 시간을 말한다. 따라서 단편화된 패킷 재전송과 암호화 및 복호화 시간이 포함된다. 그림 5에서는 통신 에러가 없다고 가정하므로 재전송이 이루어지지 않는다.

실험에서 비교적 가벼운 SHA1의 경우에는 실행에 문제가 없으나, 나머지 3개의 알고리즘은 4KB의 SRAM 사이즈로 인해 문제가 발생하였다. AES와 SHA2는 4KB로 실행이 가능하나 남는 메모리 공간이 작아 실행이 어렵고, 3DES의 경우는 실행에만 4KB 이상의 메모리 공간이 필요하여 실행을 할 수 없었다. 본 논문에서는 이를 감안하여 알고리즘 수행시간을 별도로 측정하고, 재전송 시간 측정 후에 합산하는 방식을 취하였다. 실험 결과에 의하면 2,048 바이트의 MTU를 네 가지 알고리즘으로 각각 암복호화하고 송수신하는데 각각 6.1초, 5.3초, 2.3초, 0.18초가 소요되었다.

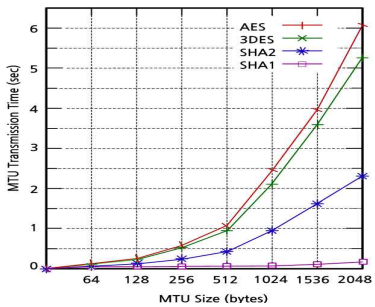

그림 5. 암복호화 알고리즘에 따른 MTU 전송 시간
Fig. 5. MTU Transmission Time Per Cryptographic Algorithms

512 바이트의 MTU를 재전송하는데 있어서 통신 에러 환경을 고려한 성능 실험 결과를 그림 6과 그림 7에 나타내었다. 그림 6의 경우는 송신과 수신이 1홉으로 이루어지며 그림 7의 경우는 2홉으로 이루어진다. 하나의 MTU를 보내는데 재전송율은 10%를 고려하였으며 Pe는 0에서 0.6까지 고려하였다.

실험 결과, Pe가 0.5이고 1홉일 경우, MTU를 네 가지 알고리즘으로 각각 암복호화하고 송수신하는데 각각 1.6초, 1.4초, 0.6초, 0.1초가 그리고 Pe가 0.5이고 2홉일 경우, 512 바이트의 MTU를 네 가지 알고리즘으로 각각 암복호화하고 송수신하는데 각각 3.8초, 3.3초, 1.5초, 0.3초가 소요된다.

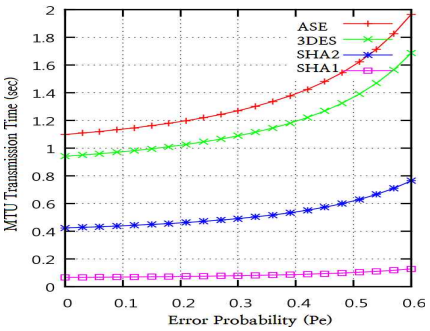

그림 6. MTU 512 바이트 전송 시간(1홉)
Fig. 6. MTU 512 bytes Transmission Time(1hop)

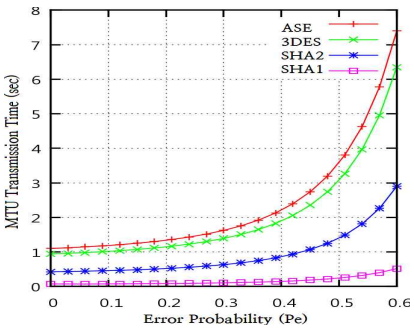

그림 7. MTU 512 바이트 전송 시간(2홉)
Fig. 7. MTU 512 bytes Transmission Time(2hop)

1,024 바이트의 MTU를 재전송하는데 있어서 통신 에러 환경을 고려한 성능 실험 결과를 그림 8과 그림 9에 나타내었다. 그림 8의 경우는 송신과 수신이 1홉으로 이루어지며 그림 9의 경우는 2홉으로 이루어진다. 전체 하나의 MTU를 보내는데 재전송율은 10%를 고려하였으며 Pe는 0에서 0.6까지 고려하였다.

실험 결과, Pe가 0.5이고 1홉일 경우, MTU를 네 가지 알고리즘으로 각각 암복호화하고 송수신하는데 각각 4.4초, 3.8초, 1.7초, 0.2초가 소요된다. Pe가 0.5이고 2홉일 경우, 1,024 바이트의 MTU를 네 가지 알고리즘으로 각각 암복호화하고 송수신하는데 각각 12.3초, 10.7초, 4.9초, 0.5초가 소요된다.

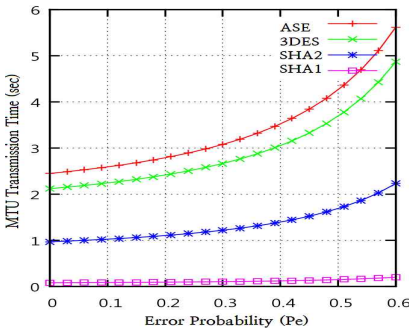

그림 8. MTU 1024 바이트 전송 시간(1홉)
Fig. 8. MTU 1024 bytes Transmission Time(1hop)

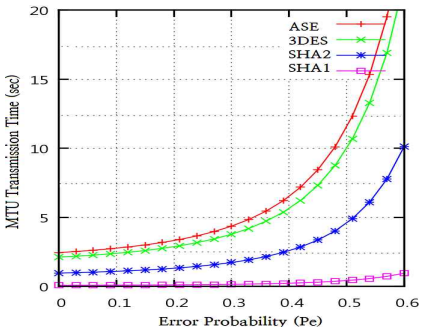

그림 9. MTU 1024 바이트 전송 시간(2홉)
Fig. 9. MTU 1024 bytes Transmission Time(2hop)

표 5. 512바이트 재전송 시간(msec)
Table 5. 512bytes Re-transmission Time(msec)

	Pe	0	0.1	0.2	0.3	0.4	0.5
512 (1홉)	AES	1,099	1,139	1,191	1,271	1,392	1,612
	3DES	942	974	1,023	1,090	1,375	1,687
	SHA2	425	440	462	492	541	625
	SHA1	68	70	74	80	88	104
512 (2홉)	AES	1,099	1,186	1,342	1,623	2,450	3,695
	3DES	942	1,013	1,145	1,391	1,897	3,256
	SHA2	425	464	524	631	987	1,410
	SHA1	68	75	85	105	144	259

전체적으로 실험 결과를 고찰해보기 위해 재전송과 암복호화 알고리즘이 동시에 수행될 때, 512바이트를 전송하기 위해 필요한 시간을 표 5에 나타내었다. 1홉을 기준으로 하였을 때, 암복호화 수행 시간이 재전송에 따른 처리 시간보다 영향이 비교적 크다는 것을 알 수 있다. 그리고 전송에러가 높아질수록 즉, 패킷 손실이 높아질수록 재전송이 급격하게 증가하고 또한, 홉 수가 증가함에 따라 재전송이 비례적으로 증가함을 알 수 있었다.

기본적으로 WPAN은 저속의 데이터를 전송하는 것을 전제로 하여 만든 프로토콜이다. 여기에 특정 응용을 위해 6LoWPAN을 이용한 IPv6 패킷을 전송하게 되면 전송 시간이 길어지는 것이 당연한 결과이다. 게다가 본 논문에서처럼 센서 데이터의 무결성과 기밀성을 제공하기 위해 다소 무거운 암복호화 알고리즘을 적용하고 재전송기법을 적용한 결과, 더욱 긴 전송시간이 소요된다. 예를 들면 AES 알고리즘, MTU 크기는 1,024 바이트, 재전송율이 10%, 에러 확률이 0.5일 때, MTU 전송 시간은 약 4.4초가 소요됨을 알 수 있다.

V. 결 론

본 논문에서는 무선 구간에서 패킷 손실에 의한 재전송 기법과 센서 데이터의 기밀성과 무결성을 제공하기 위해 암복호화 알고리즘을 적용한 6LoWPAN 프로토콜을 MICAz 센서에 구현하고, 실험적인 성능을 분석하였다. 재전송 기법에서는 재생공격을 방지하기 위한 단편화 패킷 순서번호, 타임스템프, 난스, 체크섬을 구현하였으며, 암복호화 알고리즘으로는 AES, 3DES, SHA2, SHA1을 구현하였다. 실험 결과에 의하면 전송에러가 높아질수록 즉, 패킷 손실이 높아질수록 재전송이 급격하게 증가하고, 홉 수가 증가함에 따라 재전송이 비례적으로 증가함을 알 수 있었다. 그리고 암복호화 수행 시간이 재전송 처리 시간보다 상재적으로 크다는 것을 알 수 있었다. 추후 연구 내용으로서, 성능향상을 위해 IETF 6LoWPAN WG에서 진행하고 있는 새로운 헤더 압축 기법을 적용을 적용해서 성능을 분석 할 예정이다.

참고문헌

[1] G G. Montenegro, N. Kushalnager, etc,. "Transmis sion of IPv6 Packets over IEEE 802.15.4 Networks, "IETF RFC4944, Sept. 2007.

[2] IETF, "IPv6 over Low power WPAN(6LowPAN), " http://www.ietf.org

[3] IEEE, "IEEE std. 802.15.4-2003, "IEEE Computer Society, Oct. 2003.

[4] IEEE, "802.15.4 Wireless Medium Access Control (MAC) and Physical Layer(PHY) Specifications for Low-Rate Wireless Personal Area Networks (LRWPANs), "IEEE Computer Society, September 2003.

[5] S. Diniel Park, K. Kim, E. Seo, S. Charkrabarti, "IPv6 over Low Power WPAN Security Analysis, "IETF draft-danie-6lowpan-security- analysis-02 .txt, June 2006.

[6] G. P. Chandranmenon and G. Varghese, "Reconsid ering fragmentation and reassembly, "17th ACM SIGACT -SIG OPS Symposium on Priciples of Distrubuted Computing, 1998.

[7] HyunGon Kim, "A Secure 6LoWPAN Re-transmission Mec hanism for Packet Fragmentation against Replay Attacks, "Korea Society of Computer Information, Vol. 14, pp.101-110, Oct. 2009.

[8] P. Thubert, J. Hui, "LoWPAN Fragment Fowarding and Recovery, "IETF draft draft-thubert-6lowpa n-simple-frag ment-recovery-07.txt, June 2010.

[9] Wiki page of 6LoWPAN, http://smote.cs.berkeley.edu:8000/tracenw/wiki/6loWPAN, the wiki-site of 6LoWPAN

[10] Hui, J. W. and Culler, D. E., "IP is dead, long live IP for wireless sensor networks, "In Proceeding of the 6th ACM Conference on Embedded Network Sensor Systems, pp.15-28, Nov. 2008.

[11] http://sics.se/projects/sicslowpan

[12] Wei Liu, Rong Luo, Huazhong Yang, "Cryptography Overhead Evaluation and Analysis for Wireless Sensor Networks, " WRI International Conference on Communicati ons and Mobile Computing, vol. 3, pp.496-501, 2009.

[13] P. Ganesan, R. Venugopalan etc., "Analyzing and Modeling Encryption Overhead for Sensor Network Nodes, "WSNA 03, Sept. 2003.

[14] R. Venugopalan, P. Ganesan etc., "Encryption Ove rhead in Embedded Systems and Sensor Network Nodes: Modeling and Analysis, "CASES, pp.188-197, Oct. 2003.

[15] R. Silva, J. S. Silva, F. Boavida, "Evaluating 6Lo WPAN Implementations in WSNs, "In Proceeding of the 9th Conference on Computer Networks, pp.15-16, Oct. 2009.

[16] J. Granjal, R. Silva, E. Monteiro, J. Silva, F. Boav ida, "Why is IPSec a viable option for Wireless Sensor Networks, "Proceedings of WSNS 2008, pp.802-807, Sept. 2008.

저 자 소 개

김 현 곤

1992 : 금오공과대학교 전자공학과 공학사
1994 : 금오공과대학교 전자공학과 공학석사
2003 : 충남대학교 전자공학과 공학석사
1994~2005 : 한국전자통신연구원 정보보호연구단 팀장
현 재 : 목포대학교 정보보호학과 부교수
관심분야 : RFID/USN 보안, 이동통신 보안, 차량통신 보안
Email : hyungon@mokpo.ac.kr