DOI: 10.3745/KIPSTC.2009.16-C.3.407

IEEE 802.15.4 센서 네트워크에서의 신뢰성 및 보안성 향상 기법

손 태 식[†] · 박 용 석[††]

요 약

최근 무선 센서 네트워크에 적용되는 응용 서비스들은 점점 증가하며 다양화 되는 추세이고, 이에 센서 데이터에 대한 전송 신뢰성이나 보안 기능 제공이 핵심적인 이슈로 대두되고 있다. 본 논문에서는 IEEE 802.15.4 기반 센서 네트워크 환경에서 전송 신뢰성을 제공하기 위해 링크 특성과 패킷 타입을 고려하는 ALC(Adaptive Link Control)와 Hop-cache와 Hop-ack를 지원하는 EHHR(Enhanced Hop-by-Hop Reliability)이 적용된 IMHRS(IEEE 802.15.4 MAC-based Hybrid hop-by-hop Reliability Scheme) 기법을 제안하였으며, 또한 네트워크와 애플리케이션 특성을 고려하여 보안 슈트를 결정함으로써 에너지 효율성을 고려하는 HAS(Hybrid Adaptive Security) 프레임워크를 통해 보안성을 제공한다. 본 논문에서 제안된 방식들은 시뮬레이션과 실험을 통하여 검증 하였으며, 또한 H/W 프로토타입을 제작하여 실제 응용 서비스에 적용함으로써 본 방안의 효용성을 입증하였다.

키워드 : IEEE 802.15.4, 홉 간 링크 제어, 신뢰성, 보안성, 무선 센서 네트워크

Improving Reliability and Security in IEEE 802.15.4 Wireless Sensor Networks

Taeshik Shon[†] · Yongsuk Park[††]

ABSTRACT

Recently, various application services in wireless sensor networks are more considered than before, and thus reliable and secure communication of sensor network is turning out as one of essential issues. This paper studies such communication in IEEE 802.15.4 based sensor network. We present IMHRS (IEEE 802.15.4 MAC-based Hybrid hop-by-hop Reliability Scheme) employing EHHR (Enhanced Hop-by-Hop Reliability), which uses Hop-cache and Hop-ack and ALC (Adaptive Link Control), which considers link status and packet type. Also, by selecting security suite depending on network and application type, energy efficiency is considered based on HAS (Hybrid Adaptive Security) Framework. The presented schemes are evaluated by simulations and experiments. Besides, the prototype system is developed and tested to show the potential efficiency.

Keywords : IEEE 802.15.4, Hop-by-hop Link Control, Reliability, Security, Wireless Sensor Network

1. 서 론

무선 센서 네트워크는 적은 메모리, 낮은 연산 성능, 배터리 사용 등의 제약을 가지며 다양한 센싱 능력을 가진 센서 노드들로 구성된다. 보통 환경 정보나 구조물 정보 등을 수집하는 모니터링에 관련한 응용 서비스에 주로 활용 되었지만, 최근에는 U-City 등 여러 범주에서 센서 네트워크의 활용은 점점 늘어가는 추세이며 이때 센서 노드들에 수집되어 전송되는 데이터의 신뢰성은 센서 네트워크의 다양한 응용 서비스를 제공하는데 있어 가장 핵심적인 요소라고 말할 수 있다. 또한 이러한 센싱 데이터의 신뢰성은 전송 과정에서의 성공률 보장이나 지연 시간 최소화와 같은 전송 신뢰성 향상 외에도 센서 네트워크가 가지는 센싱 정보의 도청, 비정상적 패킷의 전달, 메시지 재사용, 메시지 위조 및 변조, 가장 메시지의 반복 전송을 통한 서비스 거부 공격 위협 등 보안성의 향상도 의미하고 있다. 하지만, 무선 센서 네트워크의 보안 위협의 경우 현재 관련된 많은 연구에서 보안 프로토콜 및 기능 등을 지원하지만 이러한 보안 기능의 제공은 센서 네트워크가 본질적으로 가지는 네트워크 자원의 한계로 인한 에너지 소모에 많은 영향을 미친다[1-7].

따라서 본 논문에서는 무선 센서 네트워크에서 센싱된 데

† 정 회 원 : 삼성전자 Digital Media & Communications 연구소 책임연구원
†† 정 회 원 : 삼성전자 Digital Media & Communications 연구소 수석연구원(교신저자)
논문접수 : 2009년 2월 2일
수 정 일 : 2009년 3월 2일
심사완료 : 2009년 3월 4일

이터의 전송시 신뢰성과 보안성을 제공하는 방안을 제안한다. 먼저 신뢰성 있는 통신을 위해서 제안하는 IMHRS (IEEE 802.15.4 MAC Hybrid hop-by-hop Reliable Scheme)는 전송 시 MAC 전송 파라미터를 고려하는 ALC(Adaptive Link Control)와 hop-cache 및 hop-ack를 가지는 EHHR (Enhanced Hop-by-Hop Reliability) 기법으로 구성된다. 또한 에너지 소모를 최적화하며 보안 기능을 제공하기 위한 방법으로 애플리케이션 및 네트워크 특성을 고려하여 보안 슈트를 결정하는 HAS(Hybrid Adaptive Security) 프레임워크를 제안한다. 제안 방안의 결과는 시뮬레이션을 통하여 검증을 시도하며 또한 현재 많은 센서 네트워크에서 활용되고 있는 IEEE 802.15.4 기반 센서 노드를 제작하여 실제로 그 적용 가능성을 검증 하였다.

본 논문의 나머지 부분의 구성은 다음과 같다. 2장에서는 신뢰성 및 보안성 제공에 대한 기존 연구를 설명하며, 3장에서는 본 논문의 신뢰성 및 보안성 제공 방안을 제안한다. 이후 4장에서는 제안 방식에 대한 성능 평가 및 분석이 수행되었다. 그리고 5장에서는 실제 구현 결과에 대한 분석이 이루어진다. 마지막으로 6장에서 본 논문의 결론이 내려진다.

2. 관련 연구

2.1 기존 신뢰성 전송 기법에 관한 연구

Hop-by-Hop Reliability 기법[8]은 단일 패킷 전송 기법에 적용한 신뢰성 전송 방식의 한 예이다. 이 연구에서는 HHR에 관련하여 Ack 및 broadcast 특성 파라미터를 시뮬레이션 하였지만, 구체적인 실험 환경이나 센서 노드들의 특성에 대한 언급은 없었다. 블록 패킷 전송 방식은 무선 센서 네트워크의 노드들에게 새로운 코드나 쿼리를 전송하기 위한 방법으로서 필요한 경우이며 이때 PSPQ(Pump Slowly, Fetch Quickly)[9], RMST(Reliable Multi-Segment Transport)[10]와 같은 방식이 연구되었다. 먼저 PSPQ 프로토콜은 단일 소스 노드로부터 수신자 노드들의 그룹에 세그먼트 단위의 패킷을 전송하거나 네트워크의 모든 노드들에게 이벤트를 알리는 경우에 적용된다. [9]의 연구에서 PSPQ를 시뮬레이션하기 위해 TinyOS기반 Berkeley 모트를 사용한 테스트베드를 구성하였다. 하지만, PSPQ는 TinyOS의 MAC 수준에서 신뢰성 있는 전송 스킴을 제공하는 것이 아니라 부가적인 전송 계층 프로토콜로서 동작함으로써 노드간 링크 특성을 반영하지 못하며 계층간 오버헤드를 초래한다. 또한 RMST 프로토콜은 여러 세그먼트 데이터 블록을 신뢰성 있는 방법을 통해 전송하기 위한 기법이며, direct diffusion과 MAC 재전송 스킴 등을 제공한다. 하지만, PSPQ와 마찬가지로 부가적인 전송 계층에서 블록 전송시 신뢰성을 제공하기 위한 스킴이며 MAC 계층에서는 단순 재전송 기법을 지원한다. 마지막으로 ESRT(Event to Sink Reliable Transport)[11]라 불리는 스트림 패킷 전송 방식은 일종의 주기적 데이터 리포팅 프로토콜 방식으로 알려져 있다. ESRT는 혼잡 발생의 문제를 해결하기 위하여 응용 서비스 수준의 신뢰성 보장을 목표로 한다. 따라서 각 노드들로부터 보고되는 패킷 전송 빈도수 리포팅에 의해 네트워크의 혼잡비를 조절하게 되지만, 각 노드들로부터 빈도수 리포팅을 받아야하므로 성능에 큰 문제점을 가질 수도 있다. [17]의 연구에서는 기존 WSN환경에서 고려되지 않고 있던 실시간 애플리케이션에 대한 신뢰성 전송을 제안하고 있으며 특정 애플리케이션을 사용할 때 전송 지연시간을 줄이기 위한 혼잡 제어를 적용하였다.

2.2 기존 보안 구조에 관한 연구

현재 WSN 분야에서 에너지 소모나 라우팅 외에도 보안에 관한 다양한 연구들이 시도되고 있다. TinySA[12]라 불리는 보안구조는 TinyOS 기반의 스마트 더스트 기반으로 구현되었으며 WSN을 위한 경량화된 보안 기능을 제공하는 것이 목적이다. TinySA는 ECC(Elliptic Curve Cryptography) 알고리즘을 사용하여 기밀성, 무결성 등을 제공하기 위한 보안 프로토콜들로 구성된다. TinySA의 주된 기여는 ECC 기반의 경량화 된 공개키 기반 보안 구조 및 에너지 절감 효과를 가져온 것이다. 하지만, ECC 기반 구조를 WSN 환경에 널리 적용하기에는 표준에서의 지원문제나 부가적인 키관리가 필요하는 등의 문제가 발생한다. Neeli[13]의 연구에서는 응용 서비스에 따른 차별화된 보안 구조 개념을 제안하였다. 이 구조에서는 응용 서비스에 따른 보안 수준을 low, medium, high로 분류하여 적용하였으며, Slijepcevic [14]의 연구 역시 앞선 연구와 유사한 개념을 사용하여 센서 네트워크의 데이터 타입에 따른 분류를 하고 거기에 적합한 보안 기능을 제공하였다. [14]의 연구에서는 보안 레벨을 구분하고 각 레벨은 네트워크를 통해 전송되는 모바일 코드, 위치 정보, 응용서비스에 특화된 정보 등으로 분류하였다. 하지만 이 연구들은 센서 네트워크에 보안 레벨이나 기능을 적용하는 개념을 제공하고는 있지만, 실제 그 영향이나 적용 가능성에 대해서는 구체적인 분석이나 결과를 제공하지 못하고 있다. 또한 [18]의 연구에서는 양단간 전송시 보안을 위한 다중계층 키관리 스킴을 제공한다. 하지만 이러한 키분배 기반 보안구조는 계층간 키관리 등에 오버헤드를 가진다.

3. IEEE 802.15.4기반 WSN을 위한 신뢰성 있고 안전한 보안 구조

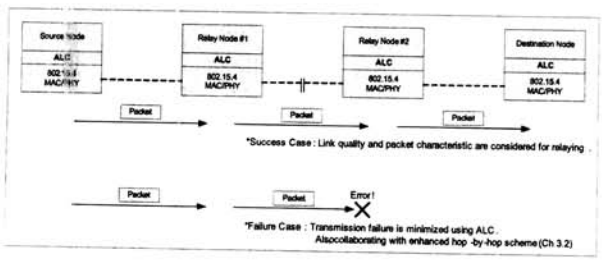
3.1 제안하는 신뢰성 향상 기법

3.1.1. IMHRS - 적응적 링크 제어 기법(ALC)

IEEE 802.15.4 표준에서 규정하고 있는 MAC 계층 링크 재전송 기법은 링크 전송이 실패하는 경우에 보통 3회의 단순한 재전송 명령을 지시한다. 이러한 재전송 관련 값들은 MAC 파라미터에 의해 설정되어 있다. 재전송 횟수의 경우 "aMaxFrameRetries" 파라미터를 사용하여 보통 3회의 재전송 값을 지정하고 있으며 time-out 시간은 "maxAckWaitDuration" 파라미터를 사용하여 54 심볼값이 지정되어 있다. 따라서 IEEE 802.15.4에서 패킷 전송이 실패하게 되면 MAC 계층

은 MAC 파라미터에 정해진 재전송 회수만큼 재전송을 시도하고 상대 노드로부터 응답 패킷이 오기를 기대한다. 만약 응답 패킷을 수신하지 못한다면 MAC 계층은 상위 계층에 전송 실패를 통보하고, 해당 패킷은 더 이상 전송 되지 못한다. 이처럼 표준에서 정의한 기법은 MAC 계층에서 패킷의 전송 신뢰성을 단지 정해진 횟수만큼의 재전송에 의존하고 있기 때문에 충분한 전송 신뢰성을 보장하기 어렵다.

(그림 1)과 같은 본 논문의 제안 방안은 MAC에 정의된 LQI(Link Quality Indicator)를 이용하여 전송하려는 링크의 상태를 파악하고, 전송하려는 패킷이 속하는 애플리케이션의 분류에 따른 특성을 고려한다. 이때 패킷이 속한 애플리케이션 특성이란 사전에 정의된 값이며 패킷 헤더에 포함된 것으로 가정한다. 이러한 패킷 특성을 고려하는 이유는, 일반적으로 패킷을 전송하는 경우 패킷 전송의 성공 또는 실패는 주로 전송하려는 링크의 상태가 큰 영향을 미치기는 하지만, 이러한 링크 품질이 좋은 상태를 유지하는 경우 일지라도, 그 당시 패킷 전송이 항상 성공적으로 전송될 것이라는 것을 보장하는 것은 아니기 때문이다. 그러므로 본 논문에서는 적응적 링크 제어 기법을 통해 패킷 전송시 링크의 특성을 고려함은 물론이거니와 각 패킷들이 가지는 응용 서비스 수준의 특성을 반영한다. 다시 말해서, 패킷을 전송하려고 할 때 그 패킷이 보내지는 링크에 대한 LQI 값을 가져온다. 이 LQI 값은 해당 목적지로부터 수신된 패킷으로부터 알 수 있으며, 실제로 패킷이 수신을 알리는 "PD-DATA.indication" 명령이 오면 해당 패킷의 "ppduLinkQuality" 파라미터로부터 구할 수 있다. 만약 사전에 해당 목적지로부터 수신된 LQI 값이 없다면 패킷 전송전 LQI 값을 얻기 위한 LQI 요청 패킷을 먼저 발송하게 된다. 만약 LQI 요청 패킷이 유실되는 경우에는 이전에 수신된 LQI 값을 사용하거나 또는 default LQI 값을 사용한다. LQI 값이 결정되고 난 후에는 해당 패킷의 서비스 특성을 패킷 헤더로부터 구하게 되는데 이러한 특성은 주기적 서비스(periodic), 이벤트 발생 서비스(event-driven), 요구기반 서비스(on-demand) 그리고 제어 메시지(control-message)의 네 가지로 분류하여 적용하였다. 이러한 방안은 링크 전송 품질 및 패킷이 속한 응용 서비스를 고려하여 재전송 횟수, 타임 아웃 기간 등 MAC 재전송에 관련한 파라미터들을 조절한다. 이때 실제 링크 품질과 패킷의 애플리케이션 특성에 의한 MAC 전송 파라미터에 대한 적용 예시는 IV 장의 성능평가에서 자세히 다룬다.



(그림 1) 적응적 링크 제어 방안

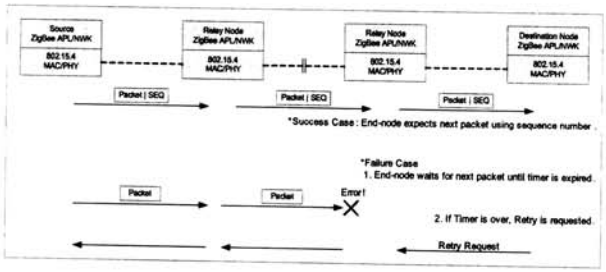
3.1.2. IMHRS - 향상된 홉 간 신뢰성 제공 기법(EHHR)

앞서 제안한 ALC 기법은 홉 간 신뢰성을 제공하기 위한 방법이었다. 그러나 홉 간 신뢰성 제공만으로는 사용자의 요청이나 센싱 된 데이터의 싱크로까지의 전송등 양단간 통신에서 해당 정보가 확실히 전송 될 수 있다는 보장이 어렵다. 따라서 센서 네트워크에서 양단간 신뢰성을 확보하기 위한 방안이 여전히 필요하다.

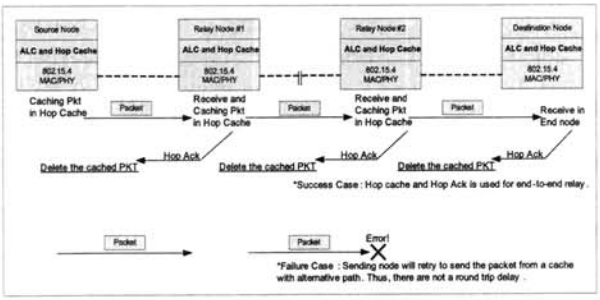
(그림 2)와 같이 ZigBee를 사용하는 센서 네트워크의 경우에는 네트워크 계층에서 순차번호를 적용하여 양단간 신뢰성을 제공하고 있다. 이 방법은 일반적인 TCP/IP 네트워크와 유사한 방법으로서 양단의 노드들은 자신이 수신할 패킷의 순차번호를 알고 있고 다음에 현재 수신한 이후의 순차번호를 가진 패킷이 들어오기를 기다리게 된다. 하지만, 에러 발생이나 원인을 알 수 없는 비정상적 상황이 발생한다면 양단의 노드들은 해당 패킷을 time-out 시간까지 기다리게 되고 실패하는 경우 다시 수신되기를 기대하는 순차번호를 가진 패킷의 재전송을 요청하는 패킷을 보내게 된다. 센서 네트워크의 경우 멀티 홉으로 구성되어 있고 라우팅 경로가 일정치 않을 수 있음을 고려할 때 반복적인 전송 실패로 인한 양단간 재전송 요청이 빈번히 발생한다면 그 전송 지연은 센서 네트워크 서비스 자체에 큰 영향을 미칠 수 있을 것이다. 즉, 기존 방식은 양단간 통신에서 중간 홉들은 신뢰성 전송에 영향을 주지 못하며 단순히 홉간 경유에 따른 오버헤드만을 가지게 된다.

그러므로 본 논문에서는 hop-cache와 hop-ack를 사용하는 EHHR을 제안한다. EHHR은 홉 사이에서 ALC 기법을 적용한 전송 신뢰성을 제공하며, 이렇게 홉 간에 적용되는 ALC를 바탕으로 노드와 노드간 통신을 양단 노드들 사이에서 신뢰성이 제공되는 통신으로 확장한다. 이때 홉 간에 적용되는 EHHR 기법은 기존의 ALC 기법에 더불어 노드간에 패킷 전송 실패를 대비하는 hop-cache를 가지고 있으며, 또한 노드간 통신 성공을 확인하는 수단으로서 hop-ack를 사용한다.

(그림 3)에서 패킷을 전송하려고 할 때 각각의 패킷들은 먼저 hop-cache에 저장된다. 이후 패킷이 다음 노드로 전송되고 만약 전송이 성공한다면 성공의 결과로서 그 패킷을 수신한 노드는 전송한 노드에게 hop-ack를 전송한다. Hop-ack를 수신한 노드는 전송한 패킷의 전송 성공을 확인하고 해당 전송 패킷의 목적지까지 전송 책임을 그 패킷을 수신한 노드에게 위임하며, 자신은 자신의 hop-cache에서 전송



(그림 2) ZigBee에서 양단간 신뢰성 제공



(그림 3) 향상된 홉간 신뢰성 전송 기법

한 패킷을 삭제하게 된다. 따라서 패킷의 전송의 책임은 멀티 홉의 노드들을 거쳐 가며 hop-ack를 수신함과 함께 다음 노드로 계속 위임되어 양단간 패킷 전송 시에도 패킷이 재전송이 발생하는 경우 부과되는 지연 시간을 최소화 할 수 있다. 이러한 과정은 최종 목적지 노드에 도착하기 전까지 반복적으로 발생한다. 하지만 패킷 전송이 실패하는 경우에는 패킷 전송을 시도한 노드가 실패한 패킷을 그대로 hop-cache에 보관하며 상위 계층에게 전송 실패를 통보하고 새로운 경로를 요청하게 된다. 이때 상위 계층에게 새로운 경로 요청에 대한 사항은 본 논문에서 다루지 않는다. 즉, 양단간 패킷 전송은 처음 소스 노드의 전송 책임하에 시작되어 hop-ack를 수신하며 계속 다으므이 멀티홉 노드로 위임되어가므로 전송 성공률과 지연시간들을 줄일 수 있다.

3.2 제안하는 보안성 향상 기법

3.2.1. HAS의 보안 슈트 및 결정 매트릭스

IEEE 802.15.4의 보안 슈트는 프레임에 대한 보안 기능을 제공하기 위한 정보를 담고 있으며 기밀성, 메시지 인증, 무결성 등의 기능을 제공하는 8가지 종류의 슈트를 가지고 있다. 하지만, 표준에서 정의한 슈트는 실제로 상위 계층이나 응용 프로그램 수준에서 특정 슈트를 지정해주는 방식을 사용하거나 또는 별도의 규정을 가지고 있지 않다. 따라서 본 논문에서는 표준안에서 제안하는 보안 슈트 중 보안 기능이 없는 슈트를 제외한 후 <표 1>과 같은 7개의 보안 슈트를 구성하고, <표 2> 에서는 네트워크 특성과 데이터 특성에 맞게 보안 슈트를 선택적으로 적용하는 방안을 제시한다. 이러한 보안 슈트는 기존 IEEE 802.15.4 보안 슈트 테이블을 기반으로 하여 작성되었으며 IEEE 802.15.4 표준안과 달리 별도의 No Security Suite 없이 보안 기능이 필요하지 않을때는 원천적으로 suite가 적용되지 않는 방식을 사용하였다. 또한 보안 슈트 결정 테이블은 기존 보안 구조들의 카테고리와 ZigBee 표준안에서의 보안 구조등을 참고하였다.

기본적으로 제안 방식은 프레임을 송수신 할 때 해당 네

〈표 1〉 HAS의 보안 슈트

	Security Suite in HAS						
	#1	#2	#3	#4	#5	#6	#7
인증/무결성		O	O	O	O	O	O
기밀성	O				O	O	O
MAC 크기	0	32	64	128	32	64	128

〈표 2〉 보안 슈트 결정 테이블

			Security Suite in HAS						
			#1	#2	#3	#4	#5	#6	#7
Pub	App	Periodic	0	0					
		Periodic(URG)	0	0					
		On-Demand	0	0					
		Event-Driven	0	0					
	Ctrl	OTA:Mobile	0				0		
		Location	0				0		
		Routing	0				0		
		Security	0				0		
Com	App	Periodic			0		0		
		Periodic(URG)			0		0		
		On-Demand			0		0		
		Event-Driven			0		0		
	Ctrl	OTA:Mobile	0					0	
		Location	0					0	
		Routing	0					0	
		Security	0					0	
Priv	App	Periodic				0		0	
		Periodic(URG)				0		0	
		On-Demand				0		0	
		Event-Driven				0		0	
	Ctrl	OTA:Mobile	0						0
		Location	0						0
		Routing	0						0
		Security	0						0

트워크의 특성과 프레임들이 속한 응용 프로그램의 특성에 따라 상이한 보안 슈트를 적용하는 것을 목적으로 한다. 이러한 목적을 위해 <표 2>에서와 같이 HAS 보안 슈트 판정 테이블은 먼저 네트워크 특성을 "Pub" (Public), "Com" (Commercial), "Priv"(Private)로 구분한다. "Pub"은 일종의 개방 네트워크를 의미하며 특별한 제한 없이 네트워크의 일원으로 접속하여 서비스를 제공받을 수 있는 특성을 가진다. "Priv"은 "Pub"과는 상반된 특성을 가진 네트워크 환경으로서 매우 개인적이며 민감한 정보를 다루는 네트워크의 특성으로서 규정한다. 또한 "Com" 특성의 경우는 앞서의 두 특성의 경계에 속한 중립적인 네트워크 특성을 나타낸다. 각 네트워크 특성은 메시지 인증 코드에 있어서 4/8/12bytes의 크기를 가진다.

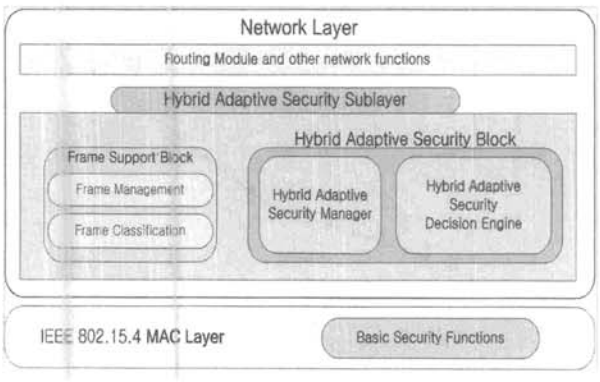
다음으로 데이터 특성의 경우 일반 응용 프로그램에 적용되는 "App" (Application) 데이터와 센서 네트워크 경로 설정 등 제어에 관련된 "Ctrl" (Control) 데이터의 두 가지로 구분한다. "App" 특성은 다시 주기적 데이터(Periodic), 긴급한 주기적 데이터(Urgent-Periodic), 사용자 요청 데이터(On-Demand), 그리고 이벤트 발생(Event-driven)으로 구분된다. "Ctrl" 특성은 원격 모바일 코드 전송(Over-The-Air Mobile Code), 위치 정보 데이터(Location), 라우팅 정보 데이터(Routing), 그리고 보안 관련 정보 (Security)로 구성된다. 이렇게 전송할 프레임을 두 가지 대분류로 구분하여 각 특성을 파악한 후 그 특성에 맞는 보안 슈트를 <표 2>에 따라 결정하고 적용하는 것이다. <표 2>의 적용 값들은 실제 적용 센서 네트워크의 환경이나 응용 서비스의 특성에 따라 달리 최적화 될 수 있다.

3.2.2. HAS 프레임워크

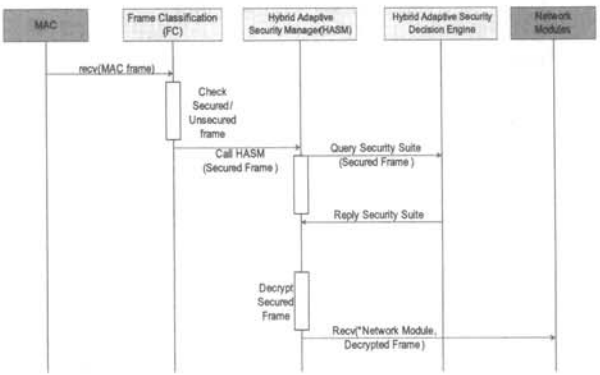
HAS 프레임워크는 기존 IEEE 802.15.4 MAC과 PHY의 통신 기능을 바탕으로 하며 보안성 향상을 위해 수정된 보안 슈트와 매 통신 과정에서 그 상황에 적합한 보안 슈트를 적용하기 위한 보안 슈트 결정 테이블을 가지고 있다. (그림 4)는 IEEE 802.15.4 MAC 기반의 네트워크 스택에 HAS 프레임워크를 적용하기 위한 새로운 보안 부계층을 포함한 네트워크 스택을 보여 주고 있다. HAS 프레임워크는 다음의 하이브리드 맞춤형 보안 블럭(HASB: Hybrid Adaptive Security Block)과 프레임 지원 블럭(FSB: Frame Support Block)로 구성된다. 먼저 HASB는 암복호화 오퍼레이션들을 효율적으로 적용하기 위한 보안 슈트를 결정하기 위한 기능을 제공하며 HASM(Hybrid Adaptive Security Manager)모듈과 HASDE(Hybrid Adaptive Security Decision Engine) 모듈로 구성된다. HASM은 어떤 프레임이나 패킷이 HASM에 도착할 때 수신한 프레임이나 패킷이 가지고 있는 보안 정보를 분석하는 기능을 제공한다. 만약 상위 계층으로부터의 패킷인 경우 보안 슈트를 결정하기 위한 정보들을 수집하며, 하위 계층으로부터의 프레임인 경우 적용되어 있는 보안 슈트 정보를 분석한다. 이후 HASDE 모듈에게 수집된 보안 정보를 전달하며 HASDE에서는 필요한 보안 슈트를 결정하거나 또는 수신된 프레임을 복호화하기 위한 보안 슈트 정보를 제공한다. 또한 FSB는 수신되는 프레임을 분류하고 적합한 상위 계층 모듈로 분배하는 FC(Frame Classification) 및 FM(Frame Management) 모듈로 구성되어 있다. 실제 HAS 프레임워크의 블록간 암복화 프레임 및 패킷 처리는 다음의 (그림 5, 6)과 같다.

(그림 5)는 수신된 암호화 프레임의 처리 과정을 나타낸다. MAC 계층으로부터 프레임이 수신되면 먼저 FC 모듈이 수신 프레임의 암호화 여부를 판단하여 일반 프레임인 경우는 상위 계층 모듈로 전달하며, 암호화 프레임인 경우에는 HASM으로 전달한다. HASM은 프레임에 적용되어 있는 보안 슈트 정보를 분석하여 HASDE 모듈에 복호화에 필요한 보안 슈트 및 정보를 요청하여 처리한다. 이후 복호화 된 프레임은 상위 계층으로 전달된다.

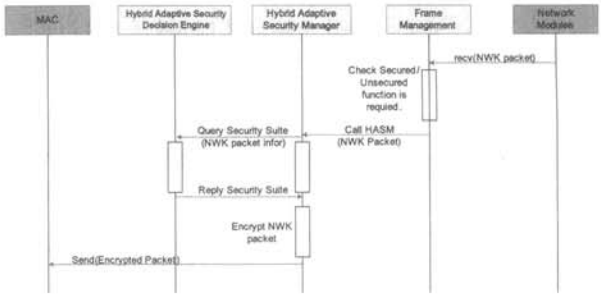
또한 (그림 6)과 같이 상위 네트워크 계층에서 생성된 패킷을 FM 모듈이 수신한 경우에는 FM 모듈에서 해당 패킷



(그림 4) 하이브리드 맞춤형 보안 구조



(그림 5) 수신된 암호화 프레임 처리 과정



(그림 6) 송신할 패킷의 암호화 처리 과정

이 암호화가 필요한지 판단하여 필요한 경우에는 HASM 모듈로 전송한다. HASM에서는 암호화에 필요한 보안 슈트를 결정하기 위한 정보를 분석하여 HASDE에 전달하고 HASDE는 적당한 보안 슈트를 결정하여 HASM에 알려주고 암호화 처리된 패킷은 하위 계층으로 전달된다.

4. 성능 평가

4.1 신뢰성 향상 방안에 대한 시뮬레이션 및 결과

IMHRS 방식에 대한 신뢰성 전송 방식에 대한 성능 평가를 수행하였다. 성능 평가 실험의 시뮬레이션은 IEEE 802.15.4 MAC과 본 제안 방식을 NS-2와 C 코드로 작성하여 수행하였다.

<표 3>에서는 시뮬레이션에 적용된 파라미터들이 나타나 있다. 본 실험에서는 시뮬레이션 시간을 3600초로 설정하였고, 기본 라운드 트립 시간(Round Trip Time)을 약 0.192ms, 최대 센서 노드의 개수는 100개, MAC PDU의 크기는 127bytes, 전송률은 최대 250kbps, 그리고 IEEE 802.15.4에서 기본적으로 제공하는 MAC 파라미터로서 time-out은 기본54 symbol(최소 27~최대120), 그리고 시스템 프로세싱 지연시간은 0.05ms등으로 설정하였다. IMHRS 방식을 실험하기 위해서는 ALC 스킴에서 사용될 LQI 값과 응용 서비스 레벨에 따른 분류가 필요하다. 따라서 본 실험을 위해서 <표 4, 5>와 같은 적응적 링크 테이블 및 전송 테이블을 설정하였다. 물론 이러한 테이블의 값들은 실제

〈표 3〉 시뮬레이션 파라미터

파라미터	값	파라미터	값
Simulation Time	3600sec	IEEE 802.15.4 Timeout	54 (symbol)
RTT	0.192ms	Processing Delay	0.05ms
No. of Nodes	100	Packet Size	127bytes
Throughput	Max 250Kbps	Retries	2~5
Multiple Copies	None/Use	Timeout	27~120 (symbol)
App(Pkt) Type	Periodic/On-Demand Event-Driven/Control	Cache Size	127bytes* 10

〈표 4〉 적응적 링크 레벨 테이블

LQI value / Packet Type	LQI (0x00~0x63)	LQI (0x64~0xC7)	LQI (0xC8~0xFF)
Periodic	Level 2	Level 1	Level 1
On-Demand	Level 3	Level 2	Level 2
Event-Driven	Level 3	Level 3	Level 2
Control	Level 3	Level 3	Level 3

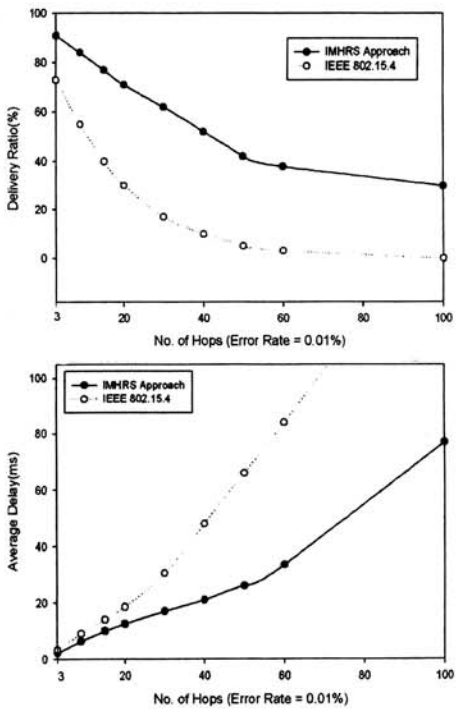
〈표 5〉 적응적 링크 전송 테이블

Actions / Adaptive Link Level	Timeout Period (symbol)	No. of Retries	Copies	Alternative Path
Level 1	27	2	None	None
Level 2	54	3	None	None
Level 3	120	5	Use	Use

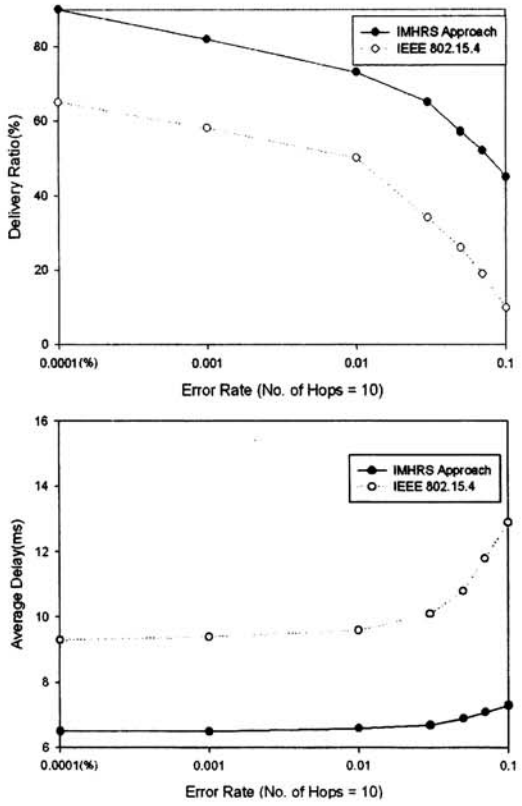
사이트에 적용하는 경우 해당 사이트의 특성에 따라 보다 적합한 값으로 대체될 수 있다. 본 논문의 실험에서 <표 4>는 전송하려는 패킷이 보내어질 노드까지 경로의 링크에 대한 LQI와 해당 패킷이 속한 응용 서비스 분류의 패킷 타입을 바탕으로 링크 레벨을 결정하는 기준이 되는 파라미터이며, 이렇게 결정된 링크 레벨은 다시 <표 5>와 같은 적응적 링크 전송 테이블에서 해당하는 링크 레벨이 필요로 하는 전송 신뢰성을 보장하기 위한 MAC 파라미터들을 결정하게 된다. 시뮬레이션에서 사용된 MAC 전송 파라미터 중 Timeout periods는 전송 실패까지 수신측에서 패킷이 도달하기를 대기하는 시간이며, No. of retries는 재전송 횟수, copies는 반복적으로 같은 패킷을 전송하는 횟수, 그리고 alternative path는 상위 계층에 전송 실패시 새로운 경로를 요청하는 것을 의미한다. 이때 <표 4>에서의 control 특성은 LQI 요청 패킷등과 같은 네트워크 제어에 사용되는 패킷들에 적용된다.

실험의 결과 본 논문에서 제안한 방법을 사용할 경우 IEEE 802.15.4를 사용하는 경우에 비해 전송 지연시간 및 전송 효율이 향상되는 결과를 얻을 수 있었다. 단, 본 성능 분석실험의 IEEE 802.15.4는 기본적으로 양단간 신뢰성 기능을 가지고 있지 않지만 실험에 사용된 IEEE 802.15.4에서는 ZigBee와 처럼 순차번호를 적용한 양단간 통신기능이 적용되어 있음을 미리 언급한다. (그림 8)의 실험은 홉 수의 증가에 따른 전송 성공률과 전송 지연 시간에 관한 실험 결과로서 이 실험에서 전송 에러율은 0.01%로 유지되었으며 제안한 방식은 홉 수의 증가에 따라 전송 성공률과 평균 지연시간에 있어서 IEEE 802.15.4에 비해 훨씬 높은 성능을 보임을 알 수 있었다. 실제로 홉의 수가 약 30일 경우, 제안 방식의 전송 성공률은 60%이상이었지만, IEEE 802.15.4에서는 20%이하였다. 따라서 제안 방식은 멀티 홉으로 구성된 센서 네트워크 환경에서 기존 IEEE 802.15.4 방식을 순수하게 적용하던 네트워크 환경에 비해 전송 실패를 훨씬 줄일 수 있음을 알 수 있다. 반면에 IEEE 802.15.4 방식은 홉 수의 증가에 따라 급격하게 전송 성공률이 낮아지고 평균 지연시간도 급속하게 증가함을 알 수 있었다.

또한 (그림 9)의 에러율 증가에 따른 전송 성공률과 평균 지연시간에 관한 실험 결과에서는 평균 10 홉을 가진 센서 네트워크 환경을 고려하였으며, 그 결과 제안한 방식은 에러가 빈번히 발생하는 환경에서도 평균 지연 시간이나 전송 성공률에 있어 급격한 변화를 보이지 않는 강건성을 보여주었다. 반면에 IEEE 802.15.4의 경우 홉의 수에 매우 민감한 결과를 보여준 것처럼 에러율의 증가에도 매우 급격한 성능 저하를 보여주었다. 실제로 에러율이 0.01%에서 0.1%로 증



(그림 8) 홉 수 증가에 따른 평균 지연시간 및 전송 성공률에 대한 시뮬레이션 결과 그래프



(그림 9) 에러율 증가에 따른 평균 지연시간 및 전송 성공률에 대한 시뮬레이션 결과 그래프

가할 때 본 논문의 제안 방식은 약 7ms정도의 평균 지연시간을 일정하게 유지했지만, IEEE 802.15.4는 약 9ms에서 13ms 이상으로 급격히 증가하는 것을 알 수 있었다. 즉, 에러율 0.01%이하에서 본 제안 방식은 최적의 성능을 보여주었다.

4.2 보안성 향상 방안에 대한 시뮬레이션 및 결과

HAS 프레임워크의 성능 평가를 위하여 HAS가 적용된 시스템에서의 보안 헤더 크기를 계산하기 위하여 Expected Overhead Size(EOS)를 적용하였다. EOS는 보안 슈트를 사용 할 때 발생 할 수 있는 헤더 크기의 조합과 그 사용되는 헤더 조합 비율의 사용빈도를 가중치로 가지는 다항식으로서 (1)과 같이 유도되어 계산 될 수 있다. 보안 헤더의 기본 크기는 1바이트 키 카운터와 4 바이트 프레임 카운터의 총 5바이트로 구성되며 만약 4, 8, 16 바이트의 크기를 가지는 메시지 인증 코드가 적용된다면 누적되는 헤더 크기는 0, 5, 9, 13, 21바이트 크기 조합을 가질 수 있다. 그러므로 식 (1)에 EOS의 크기 조합에 대한 각 사용 빈도를 적용하여 HAS 프레임워크에서의 소모되는 헤더 크기 값을 식 (2)와 같이 계산할 수 있다. 이때 식 (2)에서 적용된 EOS의 적용 비율에 대한 가중치 W는 실제 적용 사이트 환경에 따라 변경 될 수 있다. 본 논문의 제안 방안 평가에서 적용한 가중치(W) 적용 비율은 다음의 5장과 같은 실제 구현 환경에 적용하여 도출된 결과 값을 바탕으로 하였다.

$$\textit{Expected Overhead of HASS} = W_0 * EOS_0 + W_1 * EOS_1 + W_2 * EOS_2 + W_3 * EOS_3 + W_4 * EOS_4 \quad -(1)$$

where,

$EOS_{\#}$: *Expected Overhead Size,*

$W_{\#}$: *Weighted Value of HASS*

$$\textit{Expected Overhead Calculation} = 0.45*0 + 0.20*5 + 0.15*9 + 0.1*13 + 0.05*21 = 0 + 1.0 + 1.35 + 1.3 + 1.05 = 4.7 \quad -(2)$$

where,

$EOS_{\#} = 0, 5, 9, 13$ *and* 21,

$W_{\#} = 45\%, 20\%, 15\%, 10\%,$ *and* 5%

식 (2)를 통해서 HAS 프레임워크에 EOS 가중치를 45%, 20%, 15%, 10%, 5%의 비율로 적용하였을 때 계산된 EOS 값은 4.7바이트였다. 이 값을 사용하여 본 논문에서는 보안 헤더를 가지는 패킷당 소모되는 에너지를 계산함으로써 기존 IEEE 802.15.4 MAC을 사용하는 시스템에서의 에너지 소모율과 본 HAS 프레임워크를 가지는 시스템에서의 에너지 소모율을 평가하였다. 단, 본 실험에서 도출된 값은 실험 대상 네트워크 특성과 환경을 고려하여 적합한 가중치를 근거로 도출된 결과이다. 따라서 상이한 네트워크 환경에 적용할 경우 추후 고려가 필요하다. 실제 에너지 계산을 위해 적용된 H/W 플랫폼의 스펙은 TI CC2420 RF 칩을 사용하며 전류 소모량은 18.8mA 이며 공급 전압은 3v 이다. 소모되는 에너지의 계산은 식 (3)에 의하여 계산될 수 있으며, 이때 본 논문의 제안 방식과의 평가를 위해서 보안 기능을 사용하지 않는 IEEE 802.15.4, 보안 기능을 가지는 IEEE 802.15.4와 비교 검증하였다.

$$Energy(j) = \frac{Supply\ Power * Current\ Consumption * Header}{Transfer\ Rate} \quad -(3)$$

에너지 효율 테스트의 결과는 <표 6>과 같으며, 이 결과로부터는 제안하는 HAS 프레임워크를 적용한 결과 보안 기능을 사용하지 않는 기본 IEEE 802.15.4 시스템에 비교할 때 IEEE 802.15.4 보안 기능을 사용하는 경우 16%이상의 에너지 소비량이 증가하지만, 제안 시스템에서는 단지 4%정도의 에너지 소비량 증가가 있음을 알 수 있다.

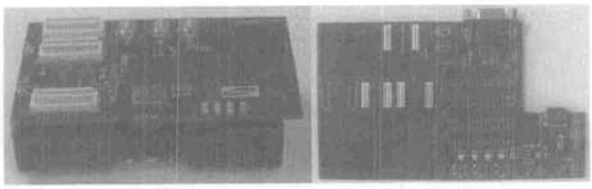
〈표 6〉 패킷당 에너지 효율

	Energy Consumption(mJ)	Increasing Rate(%)
IEEE 802.15.4 (No Security)	0.24mJ	-
IEEE 802.15.4 (Security)	0.28mJ	16.7%
Proposed Approach(HASS)	0.25mJ	4.2%

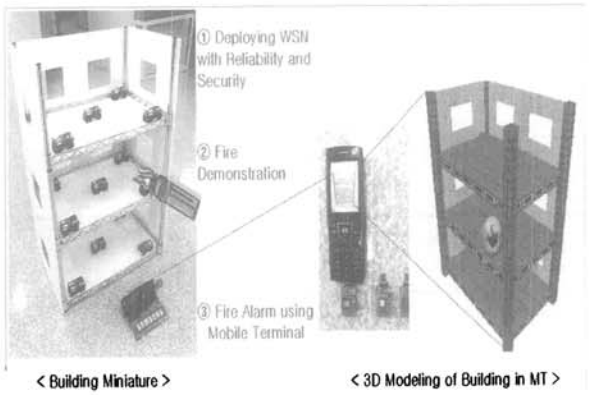
5. 구현 결과를 통한 검증

제안 방안들의 실제 검증을 위하여 (그림 10)과 같은 센서 노드 프로토타입을 제작하였다. 제작한 노드들은 Chipcon의 CC2420 RF[15] 칩과 TI의 MSP430 MCU[16]로 구성되었다. CC2420은 최대 250Kbps의 전송률을 가지며 2.4Ghz 주파수와 -95 dbm의 수신감도로 동작한다. MSP430은 16비트 RISC구조로서 12비트 AD(Analog-to-Digital) 컨버터를 가지고 있다. 또한 116KB의 플래쉬 메모리와 8Kb램을 가지며 센서 보드는 60x32mm의 크기를 가진다. 운영체제는 NesC를 기반으로 하는 TinyOS 2.0을 사용하였다. 이렇게 제작된 노드는 다음의 (그림 11)과 같은 건물에서의 화재 모니터링 응용 서비스를 구축하여 실제 적용 실험을 수행하였다. (그림 11)의 응용서비스는 건물의 미니어쳐를 제작하고 센서 보드를 설치한 후 화재와 같은 상황이 발생함을 고려해서 센서 네트워크가 얼마나 신뢰성을 가지고 안전하게 동작하는지 검증하는데 활용 되었다. 이 적용 실험에서는 패킷 전송 성공률과 HAS 프레임워크에서의 에너지 소모를 고려한 보안 슈트 적용이 실제 수행되었으며 그 결과는 <표 7, 8>에 나타나 있는 것과 같다.

실제 H/W 플랫폼을 사용한 적용 결과는 <표 7>과 같으며 거의 99%가 넘는 패킷 전송 성공률을 보이며 실제로 신뢰성 있는 전송이 가능함을 알 수 있었다. 또한 HAS 프레임워크를 적용하여 <표 8>과 같이 다양한 네트워크 및 응용애플리케이션 타입에 각각 적당한 보안 슈트가 선택되어 보안 서비스를 제공할 수 있음을 또한 확인하였다. <표 8>의 테스트 결과에서는 세 가지 경우에 대하여 각각 Suite 1, 2, 7번이 선택되어 적용됨을 알 수 있었다.



(그림 10) IEEE 802.15.4기반 센서 노드 프로토타입



(그림 11) IMHRS 기법과 HAS 프레임워크가 적용된 데모

〈표 7〉 실제 H/W 플랫폼에 IMHRS 적용 결과

Test Cases / Approaches	1st (1200)	2nd (1200)	3rd (1200)	Total (3600)	Success Ratio
Proposed approach	1198	1199	1194	3591	99.75%
IEEE 802.15.4 with default settings	923	967	985	2875	79.86%

〈표 8〉 HAS 프레임워크 적용 사례

	네트워크타입	App타입		보안 슈트	보안 서비스		
		일반	제어		인증	기밀성	인증/기밀성
Case #1	Pub	Per	-	Suite#1	X	O	X
Case#2	Com	Eve	-	Suite#2	O	X	X
Case#3	Priv	-	OTA	Suite#7	X	X	O

* Pub: Public, Com: Commercial, Priv: Private, Per: Periodic, Eve: Event-driven, OTA: Over-the-Air-

6. 결 론

본 논문에서는 IEEE 802.15.4 표준을 기반으로 하는 센서 네트워크 환경에서 신뢰성 있는 전송과 보안성을 제공하기 위한 IMHRS(IEEE 802.15.4 MAC-based Hybrid hop-by-hop Reliability Scheme) 전송 기법과 HAS(Hybrid Adaptive Security) 프레임워크를 제안하였다. 본 논문의 신뢰성 향상을 위한 주된 기여 요소는 IMHRS 방식에 있어 홉 간의 링크 제어를 위해 LQI와 같은 링크 상태 값과 각 전송하려는 패킷이 속한 애플리케이션의 특성을 바탕으로 MAC 전송 파라미터를 선택하는 ALC기법을 사용한 것이다. 또한 ALC를 바탕으로 hop-cache와 hop-ack를 사용하는 EHHR 기법을 적용하여 단순히 두 노드간의 전송 신뢰성 제공뿐만이 아니라 양단간에서 발생할 수 있었던 전송 지연 문제를 해결하였다. 또한 보안성 향상을 위해서 네트워크의 특성과 애플리케이션의 특성을 반영하여 보안 슈트를 결정하는 HAS(Hybrid Adaptive Security) 프레임워크를 사용함으로써 기존 정적인 보안 슈트 적용 방식에서의 에너지 비효율성을 개선하여 맞춤형 보안 기능을 제공하며 에너지 소비율 개선에 기여하였다.

이러한 제안 방식들은 먼저 시뮬레이션 및 실험을 통하여 검증되었다. IMHRS의 경우 전송 성공률에 있어 0.01% 에러율을 가지는 10개의 홉으로 구성된 네트워크 환경에서의 성능 평가 실험을 통하여 제안 방식은 60%, IEEE 802.15.4는 20%정도의 성능을 보였으며, HAS 프레임워크가 적용된 경우 보안 기능을 사용하지 않는 IEEE 802.15.4 시스템에 비하여 제안 방안은 4%의 에너지 소모율, 기존 IEEE 802.15.4에서의 보안 기능을 그대로 적용하는 방안은 약

16%의 에너지 소모율을 보였다. 따라서 제안 방안들은 기존 방안 대비 높은 전송 성공률과 낮은 에너지 소모량을 가지며 보안 기능을 제공 할 수 있음을 알 수 있었다. 또한 본 제안방안에 대한 시뮬레이션과 실험을 통한 검증 외에도 실제 센서 노드 H/W를 제작하여 건물 화재 발생 감지와 같은 응용 서비스 운용 환경에서 제안 방안들이 효과적으로 동작함을 검증하였다.

향후에는 IMHRS 방안에 적용되는 MAC 전송 파라미터 등의 선택과 적용 및 HAS 프레임워크에서의 보안 슈트 결정 테이블에 있어 최적화 시킬 수 있는 범용화 된 방법과 상위 네트워크 계층 등에서 alternative path 설정 지원 등에 대한 보다 세부적인 방안에 대한 연구가 필요하다.

참 고 문 헌

[1] Institute of Electrical and Electronics Engineers, Inc., IEEE Std. 802.15.4-2003, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), NewYork, IEEE Press. October, 1, 2003.

[2] ZigBee Alliance, ZigBee Specifications, version 1.1, November, 3, 2006.

[3] Paolo Baronti, Prashant Pillai, Vince W.C. Chook, Stefano Chessa, Alberto Gotta and Y. Fun Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards", Computer Communications, Vol.30, Issue7, 26 May, 2007, pp.1655-1695.

[4] Guoliang Xue and Hossam Hassanein, "On current areas of interest in wireless sensor networks designs", Computer Communications, Vol.29, Issue4, 20 Feb., 2006, pp.409-412.

[5] Andreas Willig, Holger Karl, "Data Transport Reliability in Wireless Sensor Networks - A Survey of Issues and Solutions", Praxis der Informations verarbeitung und Kommunikation, Vol.28, April, 2005, pp.86-92.

[6] Yong Wang Attebury, G. Ramamurthy, B., "A survey of security issues in wireless sensor networks", Communications Surveys & Tutorials, Vol.8, Issue2, 2006, pp.2-23.

[7] N. Sastry, D. Wagner, "Security Consideration for IEEE 802.15.4 Networks", WiSe'04 Proceeding, pp.32-42, 2004.

[8] B. Deb, S. Bhatnagar, and B.Nath, "Information assurance in sensor networks", in Proc. 2nd ACM Workshop on Wireless Sensor Networks and Applications, San Diego, CA, Sept., 2003.

[9] C.-Y. Wan, A. T. Campbell, and L. Krishnamurthy, "PSFQ: A reliable transport protocol for wireless sensor networks," in Proc. First ACM Intl. Workshop on Wireless Sensor Networks and Applications, Atlanta, GA, 2002.

[10] F. Stann and J. Heidemann, "RMST: Reliable data transport in sensor networks," in Proc. 1st IEEE Intl. Workshop on Sensor Network Protocols and Applications, Anchorage, Alaska, May, 2003.

[11] Y. Sankarasubramaniam, O. Akan, and I. Akyildiz, "ESRT: Event-to-sink reliable transport in wireless sensor networks," in Proc. ACM MOBIHOC 2003, Association of Computing Machinery, Maryland: ACM Press, June, 2003.

[12] Johann Großschädl, "TinySA: a security architecture for wireless sensor networks", International Conference On Emerging Networking Experiments And Technologies archive, Proc of the 2006 ACM CoNEXT Lisboa, Portugal 2006.

[13] N. R. Prasad and M. Alam, "Security Framework for Wireless Sensor Networks", Wireless Personal Communications, Vol.37, No.3-4, pp.455-469, 2006.

[14] Slijepcevic S., et al,. "On communication security in wireless ad-hoc sensor networks", 19th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE 2002. Proc. 139-144, 2002.

[15] Chipcon, Chipcon Products from Texas Instruments, http://www.chipcon.com

[16] MSP430, Texas Instruments, http://www.ti.com

[17] Vehbi C. Gungor, Özgür B. Akan, "Delay aware reliable transport in wireless sensor networks: Research Articles", International Journal of Communication Systems archive, Vol.20 , Issue10, Oct., 2007, pp.1155-1177.

[18] Kui Ren, Wenjing Lou, Yanchao Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks", IEEE Transactions on Mobile Computing, Vol.7, Issue5, May, 2008, pp.585-598.

손 태 식

e-mail : ts.shon@samsung.com

2000년 아주대학교 정보 및 컴퓨터공학부 (학사)

2002년 아주대학교 정보통신 정보통신공학과 (공학석사)

2005년 고려대학교 정보보호학과(공학박사)

2004년~2005년 2월 Research Scholar, Univ. of Minnesota

2005년~현 재 삼성전자 Digital Media & Communications 연구소 책임연구원

관심분야 : Wireless/Mobile Network Security, WSN/WPAN, Anomaly Detection/Machine Learning

박 용 석

e-mail : dryspark@gmail.com

1988년 서강대학교 컴퓨터학과(학사)

1992년 뉴욕 폴리테크닉 컴퓨터학과(공학석사)

1998년 뉴욕 폴리테크닉 컴퓨터학과(공학박사)

1992년~1994년 Research Staff, CALC, USA

1995년~1996년 Teaching Staff, City University of New York

1999년~2003년 MTS, AT&T Labs, New Jersey, USA

2003년~2005년 Research Staff, City University of New York

2005년~2007년 삼성종합기술원 수석연구원

2007년~현 재 삼성전자 Digital Media & Communications 연구소 수석연구원

관심분야 : Wireless Networks, Mobile Solutions, IT Service Design 등