DOI: 10.3745/KIPSTC.2009.16-C.3.285

의료 센서 네트워크에서의 효율적인 전송 구조 및 Key Provisioning을 사용한 키 관리 기법 연구

서 재 원[†] · 김 미 희[††] · 채 기 준[†††]

요 약

유비쿼터스 기술의 발전과 함께 센서 네트워크는 다양한 분야에서 활용되고 있다. 그 중 특히 의료 분야는 중요한 응용 분야 중의 하나로 바디 센서 네트워크의 표준화 동향과 함께 관심이 집중되고 있다. 의료 센서 네트워크는 기존의 일반적인 환경의 센서 네트워크와는 다른 의료 환경만의 특징들을 가지고 있다. 따라서 본 논문에서는 이와 같은 특징들을 반영하여 계층적인 의료 센서 네트워크 구조를 제안하였고, 계층적인 구조를 바탕으로 하여 센싱 데이터 전송 방식을 소개하였다. 즉, 효율적인 센싱 데이터 전송을 위해서는 환자들의 요구 사항과 건강 상태를 고려하여 각 센서 노드들에게 우선 순위(Priority)와 경계값(Threshold Value)을 주었다. 이를 통해 클러스터 헤드에서 응급 데이터를 우선적으로 빠르게 베이스스테이션으로 전송하도록 하였다. 또한 이와 같은 구조와 전송 방식을 바탕으로 센서 네트워크를 위해 Eschenauer와 Gligor가 제안한 키 메커니즘을 기반으로 하여 새로운 키 관리 기법을 제안하였다. 이는 각 클러스터 헤드들이 높은 우선 순위를 갖는 응급 노드들에 대해서 이웃 클러스터로 응급 노드와의 키를 미리 전송해주는 Key Provisioning 방법을 사용하여 응급 노드들에 대해서 키 설립을 준비하도록 하여 키 설립이 보다 빠르게 이루어지도록 하였다. 이를 통해 키 설립 지연으로 인한 데이터 전송의 기다림 없이 바로 응급 노드들의 데이터를 클러스터 헤드로 전송할 수 있도록 한다. 이와 같은 계층적인 구조에서의 데이터 전송 방식과 이를 바탕으로 제안한 키 관리 기법은 수식 및 QualNet 시뮬레이터를 사용한 시뮬레이션을 통하여 네트워크 트래픽 오버헤드와 에너지 소모량을 분석하였으며, TmoteSKY 센서보드를 사용해 구현함으로써 그 효율성을 증명하고 실제 응용환경에서의 실현가능성을 입증하였다.

키워드 : 센서 네트워크, 의료 센서 네트워크, 바디 센서, 키 관리 메커니즘

Efficient Transmission Structure and Key Management Mechanism Using Key Provisioning on Medical Sensor Networks

Jaewon Seo[†] · Mihui Kim[††] · Kijoon Chae[†††]

ABSTRACT

According to the development of ubiquitous technologies, sensor networks is used in various area. In particular, medical field is one of the significant application areas using sensor networks, and recently it has come to be more important according to standardization of the body sensor networks technology. There are special characteristics of their own for medical sensor networks, which are different from the one of sensor networks for general application or environment. In this paper, we propose a hierarchical medical sensor networks structure considering own properties of medical applications, and also introduce transmission mechanism based on hierarchical structure. Our mechanism uses the priority and threshold value for medical sensor nodes considering patient's needs and health condition. Through this way Cluster head can transmit emergency data to the Base station rapidly. We also present the new key establishment mechanism based on key management mechanism which is proposed by L. Eschenauer and V. Gligor for our proposed structure and transmission mechanism. We use key provisioning for emergency nodes that have high priority based on patients' health condition. This mechanism guarantees the emergency nodes to establish the key and transmit the urgent message to the new cluster head more rapidly through preparing key establishment with key provisioning. We analyze the efficiency of our mechanism through comparing the amount of traffic and energy consumption with analysis and simulation with QualNet simulator. We also implemented our key management mechanism on TmoteSKY sensor board using TinyOS 2.0 and through this experiments we proved that the new mechanism could be actually utilized in network design.

Keywords : Sensor Network, Medical Sensor Networks, Body Sensor, Key Management Mechanism

※ 이 논문은 2008년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(NO. R01-2008-000-20062-0).
† 정 회 원 : SK C&C
†† 정 회 원 : North Carolina State University 컴퓨터공학과 Postdoc Researcher
††† 종신회원 : 이화여자대학교 컴퓨터공학과 교수(교신저자)
논문접수 : 2008년 10월 17일
수 정 일 : 1차 2008년 12월 29일, 2차 2009년 2월 4일
심사완료 : 2009년 2월 25일

1. 서 론

오늘날 유비쿼터스 기술의 발전과 함께 센서 네트워크의 활용 또한 증가하고 있으며 군사, 의료, 홈 네트워크에 이르기까지 다양한 응용 분야에서 사용되고 있다[1]. 그 중 의료

분야는 센서 네트워크가 활용될 수 있는 중요한 응용 분야 중의 하나이며, 근래에 들어 의료 기술의 발전과 바디 센서의 표준화 움직임 등에 따라 관심이 집중되고 있다. 이와 같은 의료 센서 네트워크를 활용하는 데에 있어서 의료 환경과 센서의 제한된 에너지 및 전파 범위를 고려한 계층적인 구조나 센싱 데이터의 전송 기법, 그리고 의료 데이터가 가지는 특수성을 고려한 보안 기법은 의료 센서의 활용에 있어 반드시 필요한 사항일 것이다. 지금까지 안전한 센서 네트워크 환경을 위한 다양한 키 관리 기법이 연구되고 제안되어 왔지만 이러한 기존의 기법들을 그대로 수정 없이 의료 환경에 적용하는 것은 적합하지 않다. 왜냐하면 의료 센서 네트워크의 사용을 위해서는 일반적인 센서 네트워크가 갖는 특징 뿐 만이 아니라 병원이나 환자 주변의 홈 네트워크와 같은 특수한 환경과 의료 데이터만이 가지고 있는 고유한 특징들을 반드시 고려해야 하기 때문이다.

따라서 본 논문에서는 의료 센서 네트워크만이 가지고 있는 고유한 특징들을 바탕으로 한 계층적인 구조와 이 구조에서의 센싱 데이터 전송 방식을 소개하고, 이에 적합한 효율적이고 빠른 데이터 전송을 보장하는 키 관리 기법을 제안하였다. 이를 위해 환자의 요구 사항과 건강 상태를 고려하여 노드들과 데이터에 대해 우선순위를 두어 센싱 데이터를 전송하도록 하였다. 또한 응급 데이터와 같이 높은 우선순위를 가진 응급 노드들에 대해 각 CH(Cluster Head, 클러스터 헤드)는 미리 응급 노드의 키 정보를 이웃 CH에게 전송함으로써 이웃 CH가 응급 노드와의 키 설립을 먼저 준비할 수 있도록 해 주어 응급 노드와 CH 간의 빠른 키 설립을 가능하게 한다. 이와 같은 연구를 통해 본 논문에서는 다음과 같이 효율적인 전송과 빠른 키 설립을 목표로 하고자 한다.

- *계층적인 구조를 활용한 효율적 전송 기법 :* 의료 센서 네트워크의 특성을 고려한 계층적인 센서 네트워크 구조를 제안하였고, 이를 기반으로 전송 트래픽 면에서 효율적인 전송 기법을 제안한다.
- *Key Provisioing을 이용한 키 관리 기법 :* 추가의 키 저장 공간인 Extra Key Space를 활용하여 응급 노드들이 보다 빠르게 키 설립을 완성 할 수 있도록 한다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어, 2장에서는 관련 연구로 센서 네트워크와 무선 바디 센서 네트워크(WBSN, Wireless Body Sensor Network)의 표준화 동향과 기존의 의료 센서 네트워크 관련 연구 및 본 논문에서의 키 관리 기법의 기반이 되는 Eschenauer와 Gligor가 제안한 키 관리 기법에 대해 살펴본다. 3장에서는 의료 센서의 고유한 특징들과 의료 센서 네트워크를 위한 계층적인 구조, 센싱 데이터 전송 방식을 소개하고, 이와 함께 Key Provisioning을 사용한 키 관리 메커니즘을 제안할 것이다. 4장에서는 본 논문에서 제안한 기법들을 수식과 시뮬레이션을 통해 분석하고 효율성을 증명할 것이며 5장에서는 제안한 키 관리 기법을 TmoteSKY 센서 보드를 사용하여 구현된 내용을 기술한다. 마지막으로 6장에서는 제안된 구조 및 기법을 마무리 하면서 향후 연구에 대해서 설명한다.

2. 관련연구

2.1 바디 센서 네트워크 표준화 동향

최근에 들어 무선 바디 센서 네트워크에 대한 관심이 높아지고 있는 가운데 무선 바디 센서 네트워크 또한 의료 분야에서 활발하게 사용되고 있는 응용 분야라 할 수 있다. 무선 바디 센서 네트워크는 무선 네트워크의 한 종류로서 입을 수 있는 장치(wearable device) 또는 사람 몸 안에 혹은 몸 위에 부착할 수 있는 센서들의 통신을 위한 네트워크를 의미한다. 이는 크게 비의료 분야와 의료 분야의 두 가지 응용 분야로 나누어 정의된다[2]. 비의료 분야는 주로 레져나 엔터테인먼트를 즐기기 위한 목적으로 사용되며 mp3 플레이어와 헤드셋간의 통신이 가장 대표적인 예이다. 의료 분야는 심전도나 근전도 등과 같은 사람의 생체 신호의 전송 및 통신과 관련된 분야를 의미하며 이는 본 논문에서의 연구 분야와 상당히 밀접한 관계가 있다.

무선 바디 센서 네트워크 표준화와 관련하여 2006년 11월 IEEE 802.15 워킹 그룹이 Wireless Medical BAN SG(Study Group)으로 승인되었으며, 2007년 5월에 IEEE 48차 회의에서 Wireless BAN으로 새롭게 명명하여 WBAN 표준화를 진행하였다. 그 후 2007년 10월 무선 바디 센서 네트워크를 위한 IEEE 802.15.6 TG(Task Group)가 조직되었으며 현재 2009년 말 표준화 완료를 목표로 하여 IEEE 802.15.6 TG를 중심으로 무선 바디 센서 네트워크 관련 표준화 작업이 활발히 진행되고 있다.

2.2 의료 센서 네트워크 연구 동향

이와 같은 의료 센서 네트워크 분야에의 높아지는 관심과 함께 의료 센서 네트워크 분야에 대한 연구가 최근 활발하게 진행 중에 있으며 Victor Shnayder 등이 코드 블루 프로젝트를 통해 의료 센서 네트워크 하드웨어 및 소프트웨어 디자인에 대해 연구를 진행하였다[3][4]. 코드 블루 프로젝트를 통해서 의료 센서 네트워크를 위한 하드웨어와 소프트웨어 플랫폼을 개발하였고 멀티홉 라우팅에서부터 의료 모니터링을 위한 쿼리 인터페이스까지의 프로토콜을 제공하고 있다. 또한 MICAz 센서 보드와 Telos 모트의 디자인에 기반한 의료 센서를 개발하였으며 코드블루 아키텍처를 제안하였다. 그러나 코드 블루 프로젝트는 의료 센서 네트워크 기반 구조와 디자인에 초점이 맞추어져 있으며 키 관리 메커니즘에 관해서는 이와 관련된 요구사항을 분석하고 일반적인 필요성을 강조하였을 뿐 구체적인 연구는 진행하지 않았다.

의료 센서 네트워크 환경에서의 키 관리 기법은 최근에 들어 많은 관심을 가지고 연구되기 시작하였다.

K. Malasri와 L. Wang은 의료 센서 네트워크 환경에 적합한 SNAP(Sensor Network for Assessment Patient) 구조를 제안하고 이를 바탕으로 하여 ECC 기반의 키 교환 프로토콜을 제안하였고, 이를 통해 데이터의 기밀성과 무결성을 제공하는 대칭 암호화 및 복호화 방식을 제공하고 있다[5]. 이를 위해 보안을 제공하는 SNAP 구조를 소개하고 있으며

이는 환자의 프라이버시를 보호하고 의료 데이터의 무결성을 제공하는 동시에 에너지 효율성이 높은 기법이다.

또한 O. G. Morchón 등은 의료 바디 센서 네트워크 환경을 위한 DPKPS(Deterministic Pairwise Key Pre-distribution Scheme)에 기반한 키 관리 기법을 제안하고 이를 MICAz 센서에 구현하는 연구를 진행하였다[6]. 이를 통해 각 센서 네트워크 안에서 pairwise 키를 설립할 수 있도록 하였고 MICAz 센서 보드를 통한 구현과 시뮬레이션을 통해 에너지 전력과 차지하는 메모리 공간의 측면에서 효율적임을 증명하였다.

A. Wood 등도 ALARM-NET이라는 구조를 제안하여 모니터링 시스템에서의 센서 네트워크 구조를 제안하였다[7]. 이는 주로 바디 네트워크, 센서, 백본 네트워크 등이 모두 사용되는 주거 환경에서의 모니터링에 초점을 맞추고 연구를 진행하였으며 실시간 쿼리와 사용자 인터페이스를 통한 센서 데이터로의 접근을 제공하였다. 또한 end-to-end 간의 안전한 통신을 보장하였다.

C. C. Tan 등도 연구를 통해 바디 센서 네트워크 구조에서 ECC를 기반으로 하는 IBE(Identity Based Encryption)을 이용한 보안 기법을 제안하여 환자와 의사간에 안전한 통신을 제공하는 기법을 제안하였다[8].

이와 같이 의료 센서 네트워크 환경에서의 다양한 연구들이 진행되고 있지만 아직까지 환자의 응급 상황에 대비하거나 환자들의 우선 순위를 고려한 기법에 대해서는 연구가 부족한 실정임을 알 수 있다.

2.3 L. Eschenauer와 V. Gligor의 키 관리 기법

본 논문에서는 L. Eschenauer와 V. Gligor가 제안한 키 관리 기법(이하, EG 스킴)을 기반으로 하여 의료 센서 네트워크에 적합한 키 관리 기법을 새롭게 제안하였다[9].

L. Eschenauer, V. Gligor가 이를 통해 센서 네트워크에서 노드 간 Pairwise Key 설정을 위해 제안한 프로토콜은 베이스스테이션이 먼저 다량의 랜덤 키를 생성하여 이를 키 풀(Key Pool)에 저장하고 키 풀에서 무작위로 임의의 키 집합을 선택하여 키 링을 생성하여 이를 각 센서 노드에게 분배한다. 센서 노드들은 자신이 갖고 있는 키 링의 키 아이디 정보를 이웃 노드들에게 브로드캐스트함으로써 무선 통신 반경 내에서 자신의 이웃하는 노드들과 공유키를 찾는다. 두 링크 또는 그 이상 떨어져 있으면서 서로 공유하는 키가 없는 임의의 두 노드가 공유키를 갖기 위해서는 Path Key를 생성하여 공유한다. Path key를 설정하고자 하는 두 노드는 두 노드 간의 Direct Link Path를 통해 키를 교환하여 공유키를 설정한다. 키 분배 및 설립을 위한 상세 프로토콜은 다음과 같다.

- 1단계 : 'Key Pre-Distribution' 단계로서 이는 off-line 상태에서 이루어진다. 커다란 키 풀 P와 각 키 값에 해당되는 키의 아이디를 생성하고, P 개의 키 풀에서 무작위로 선택된 k 개의 키로 이루어진 키 링들을 생성한다. 각 센서 노드는 키 링을 선택해서 메모리에 장착하고 키 링의 아이디와 자신의 노드 아이디를 신뢰하는 제어 노드에 저장한다. 또한 자신에 관한 정보를 가지고 있는 제어 노드의 아이디를 메모리에 저장한다.
- 2단계 : 'Shared-Key Discovery' 단계로서 센서 노드는 자신이 가지고 있는 키 링에 속한 키의 아이디를 평문으로 한 홉 내의 모든 이웃 노드에게 브로드캐스트 한다. 그 후, 이웃 노드가 소유한 키의 아이디와 자신이 소유한 키의 아이디를 비교하여 공통키를 찾아내어 공통키가 존재할 경우 해당하는 키를 두 노드 사이의 키로서 자신의 로컬 키 그래프에 저장한다.
- 3단계 : 'Path-Key Discovery' 단계로서 한 홉 통신 범위 내의 A 노드와 B 노드 사이에 공유키가 없을 경우 이 노드들과 키를 동시에 공유하는 C 노드를 경유해서 Path Key를 설정한다. 즉, A 노드와도 키를 공유하고 있고 B 노드와도 키를 공유하고 있는 C 노드는 자신의 키 링에서 쓰이지 않은 키를 한 개 선택해서 A 노드와의 공유키로 암호화해서 A 노드로 보내고 B 노드와의 공유키로 암호화해서 B 노드에게 보내준다.

EG 스킴은 센서 노드의 개수가 매우 많더라도, 수백 개 정도의 키로 기존의 Pairwise Key와 동일한 안전성을 제공한다는 장점을 갖으며, 위의 2단계를 거쳐 두 노드 간에 공통 키를 갖게 될 확률은 선택하는 키 풀과 키 링의 개수에 따라 0에서 1까지 다양하게 존재하여 이는 EG 스킴의 확장성을 보여주고 있다. 또한 네트워크가 위와 같은 키 설립 단계들을 거쳐 두 노드 간에 키가 설립될 확률을 1에 가깝게 만드는 것이 가능함을 Erdös와 Rényi의 Random-Graph Theory[10]에 의해 증명하였다. 즉, 노드 수를 n 이라하고 두 노드들 사이에 키가 존재하여 링크가 존재할 확률을 p 라고 하면 네트워크를 랜덤 그래프인 $G(n, p)$로 나타낼 수 있다. 이 때, Erdös와 Rényi의 Random-Graph Theory에 의해 그래프 G가 연결되는 확률이 0.99, 0.999등의 값을 가지며 1에 가까워지는 것이 가능함을 증명하였다. 이와 같은 EG 스킴은 기존의 키 관리 기법에 비해 적은 계산량과 메모리 용량을 차지하고도 같은 수준의 보안성을 제공하고 있다.

3. 제안하는 전송 구조 및 키 관리 기법

3.1 의료 센서 네트워크의 특징 분석

의료 센서 네트워크는 병원과 같은 의료 환경과 환자들의 의료 정보라는 특수성을 갖고 있기 때문에 다른 일반적인 센서 응용 환경의 특징들과는 다른 고유한 특징들을 갖고 있다.

- 센서의 이동성

센서 노드는 대부분 환자의 몸에 부착되어 있으므로 환자의 움직임에 따라서 함께 이동한다. 따라서 센서 노드는 계속해서 위치를 바꾸며 이에 따라 센서 노드가 속해 있는 CH 또한 수시로 바뀌게 된다.

- 센싱 데이터들간의 비연관성

여러 환자로부터의 데이터 들은 서로 합쳐질 필요가 없다. 한 환자의 특징이 다른 환자의 특징과는 관계가 없으며 따라서 한 명의 환자로부터의 데이터 그 자체만이 의미 있는 값일 것이다. 예를 들어 일반적인 센서 네트워크에서의 데이터를 전송할 때와는 달리 의료 센서 네트워크에서는 중간 노드나 클러스터 헤드에서 여러 센싱 데이터들의 합이나 평균값 등을 계산할 필요가 없다.

- *의료 정보의 프라이버시 보호*

센싱된 정보들은 모두 환자 개개인의 건강 정보와 관련된 것이므로 허가되지 않은 사용자에게 공개되어서는 안되며, 안전하게 책임자(의사, 간호사, 보호자 등)에게 전달되어야 한다.

- *사용자(환자)에 따른 특성과 요구사항 반영*

각 환자마다 갖고 있는 질환과 신체 특성이 다르므로 데이터 처리에 있어 각 환자마다 다른 기준이 필요하다. 또한 환자의 요구사항도 고려하여 환자의 요청에 따라 모든 의료 데이터들을 다 조사하기를 원할 수도 있으며 혹은 건강의 이상 신호를 알리는 것과 같은 일부 데이터만을 필요로 할 수도 있다.

- *센서 노드의 구별 및 아이디*

각 센서 노드는 환자들을 구별할 수 있게 하는 아이디를 갖고 있어야 한다.

3.2 통신 구조 및 전송 방식

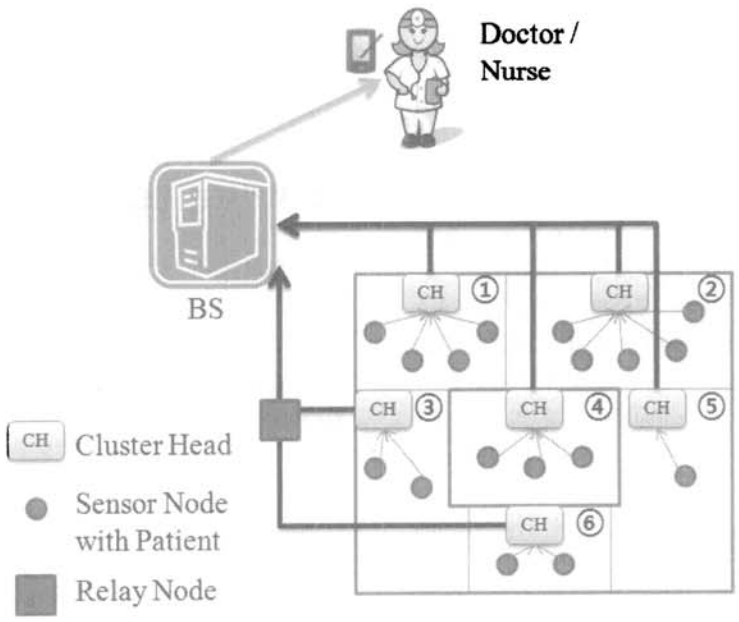
위 3.1절에서 살펴본 의료 센서 네트워크가 갖고 있는 특징을 고려하여 본 논문에서는 이에 적합한 계층적인 구조를 제안하고 이를 바탕으로 연구를 진행하였다. 이는 한 개의 병원이나 의료시설과 같은 공간을 하나의 단위로 하여 한 개의 공간 단위 내에서의 구조를 나타내고 있으며, BS(Base Station), CH(Cluster Head), 센서 노드로 구성되어 있다. 또한 필요에 따라 CH와 BS 사이에 단순한 데이터 전달을 위한 RN(Relay Node) 노드를 사용할 수도 있다. (그림 1)은 의료 센서 네트워크 구조의 한 예이다.

먼저, BS는 싱크로서 가장 상위 계층에 있으며 많은 수의 CH로부터 의료 정보들을 모아 의사, 간호사, 혹은 환자의 보호자에게 전달하는 역할을 한다.

다음으로 CH는 BS의 아래 계층에 속하며 많은 센서 노드들을 포함하고 있다. CH는 이동성이 없고 고정되어 있으며 병원과 같은 환경을 예로 들었을 때 한 방에 하나씩 설치되어 있는 것과 같이 끊김없이 연결되어 있다고 가정한다. CH는 센서 노드들의 이동에 따라 시간에 따라 각각 다른 노드들을 포함하게 된다. CH와 BS 사이에는 필요에 따라 RN를 이용할 수 있으며 RN은 CH가 전송한 데이터를 다시 BS에게 전송해주는 전달 노드의 역할을 한다.

마지막으로 센서 노드들은 구조의 제일 하위 계층에 속하게 되며 대개 환자의 몸에 부착되어 있고 환자의 움직임에 따라 이동하게 된다. 센서 노드가 새로운 지역으로 이동함에 따라 속하게 될 CH를 바꾸게 되고 따라서 센서 노드가 속해있는 CH는 수시로 바뀌며 이 때 새로운 CH와 다시 새로운 키를 설립하게 된다.

위의 계층적인 의료 센서 네트워크 구조에서는 3.1절에서 설명한 의료 센서 네트워크 환경의 특징들을 고려한 센싱 데이터 전송 방식이 필요할 것이다. 예를 들어, 정상적인 생체 신호는 이상을 알리는 생체 신호에 비해 그 의미가 떨어질 것이며, 한 공간에 서로 다른 질환을 갖고 있는 두 환자가 있다면 두 환자의 데이터는 서로 연관이 없을 것이다. 이를 위하여 계층적인 구조에서 CH에서 BS로의 효율적인 센싱 데이터 전송 방식을 제안하고자 한다.



(그림 1) 의료 센서 네트워크 구조

먼저, 앞서 제안한 의료 센서 네트워크 구조에서 CH는 다른 노드들에 비해 뛰어난 성능을 가졌다고 가정하며 따라서 많은 양의 데이터들을 수집하고 다시 BS로 전송할 수 있는 능력을 가지고 있다.

우리는 각 환자의 건강 상태를 고려하여 각 환자에게 일정한 경계값(Threshold Value)들을 정해준다. 예를 들어 경계값은 심장 질환 환자에게는 심박동수가 될 수 있을 것이며 근육이나 운동 능력에 문제가 있는 환자에게는 근전도 수치가 될 수 있을 것이다. CH는 이 경계값을 넘지 않는 데이터들은 BS로 전송할 필요가 없으며 만일 센싱 데이터가 경계값을 넘을 경우에만 BS로 즉시 전송한다. 즉, CH는 일정 경계값을 넘는 비정상적인 데이터에 높은 우선 순위를 두어 즉시 BS로 보내는 것이다. 또한 만일 저혈압 등과 같이 하한선이 있는 경우는 반대로 센싱되어진 값이 경계값보다 적을 경우에만 전송한다. 이와 같은 응급 데이터들은 경계값을 얼마나 넘었는지 차이에 기반하여 경고 수준과 응급 수준으로 나누어 볼 수 있다. 응급 수준의 데이터들은 경고 수준의 데이터보다 더 높은 우선 순위를 갖고 보다 빠르게 BS로 전송한다.

뿐만 아니라 환자의 요구사항을 고려하여 만일 환자가 모든 데이터들을 공개하기를 원하거나 혹은 환자의 건강 상태를 고려하여 보았을 때 환자의 모든 데이터가 조사·관찰되어야 할 경우에는 CH에서 경계값을 넘지 않은 데이터들을 없애는 대신에 BS로 전송해야 할 것이다. 하지만 이 경우 반드시 실시간으로 전송되어야 할 데이터 값들이 아니므로 일정한 주기를 갖고 응급데이터에 비해 상대적으로 천천히 BS로 전송하거나 CH에서 각 환자 당 센싱 데이터의 평균 수치 값을 계산하여 긴 주기 당 한 번만 전송하도록 할 수 있다.

위의 전송 기법을 CH에서의 BS로의 데이터 전송 동작에 대한 Pseudo Code로 나타내면 (그림 2)와 같다. 단 경계값이 상한선으로 고려되는 경우 즉, 측정된 데이터 값이 경계값보다 높을 때에만 우선 순위를 높이는 데이터로 고려하는 예에 대해서만 나타내었다.

그러므로 제안된 기법을 통해서 CH는 필요한 데이터만 전송함으로써 CH와 BS간의 트래픽양을 감소시킬 수 있을 것이며 이는 응급 데이터 발생시 CH에서 BS로 빠르게 전송하는 것을 보장할 수 있도록 만든다.

```
value : 센서 노드에서 CH로 전송하는 센싱 데이터
단, α>β>0 으로 정의됨

if( value>threshold+α )
        send it with "emergency" flag immediately.
else if( value>threshold+β )
        send it with "warning" flag immediately.
else if( value > threshold )
        send it immediately.
else
    calculate Avg(value_i) and send it periodically
```

(그림 2) CH의 전송 동작 Pseudo Code

3.3 Key Provisioning을 사용한 키 관리 기법 제안

본 절에서는 위에서 제안한 의료 센서 네트워크 구조를 바탕으로 하여 효율적이며 빠른 데이터 전송을 보장하는 앞서 2.3절에서 설명한 EG 스킴을 기반으로 한 키 관리 메커니즘을 제안한다.

EG 스킴에서는 모든 센서 노드들이 k 개의 키를 저장한 반면, 본 논문에서는 CH의 경우 k 개의 키 링 뿐만이 아니라 Extra Key Space라는 추가 저장 공간에 여분의 키를 저장할 수 있도록 하였다. 또한 2.3절에서 설명한 EG 스킴에서의 1단계와 2단계는 같은 메커니즘을 사용하도록 하였으나, 공통 키가 없을 경우인 3단계는 기존의 EG 스킴과는 달리 일반 노드와 응급 노드에 차이를 두어 새로운 메커니즘을 사용하도록 제안하였다.

앞서 설명한 의료 센서 네트워크 구조에서 센서 노드는 계속해서 움직이며 새로운 CH와 연결을 맺고 CH로 데이터를 전송하게 된다. 따라서 CH와 센서 노드간의 보안은 필수적인 요소이며 이를 위해서는 적합한 키 설립 기법이 필요할 것이다. 또한 새로운 CH와의 키 설립이 지연되어 중요한 데이터들이 실시간으로 전송되지 못하는 상황이나 중요한 데이터들을 놓치게 되는 상황을 막기 위한 기법들도 필요할 것이다. 이와 같은 점들을 고려한 CH와 센서 노드간의 키 설립 기법을 제안한다. 이 때 CH와 BS 사이에는 충분한 처리 용량을 갖고 있기 때문에 강력한 보안이 이미 제공되고 있다고 가정한다.

3.3.1 비응급 센서 노드를 위한 키 설립 기법

본 논문에서는 비응급 상황을 위해서 기본적인 EG 스킴을 활용하여 CH와 센서 노드간의 키를 설립한다. 노드가 설치되어 동작하기에 앞서서 모든 CH와 센서 노드들은 P개의 키를 가진 커다란 키 풀로부터 랜덤하게 선택되어진 k개의 키들을 갖고 해당하는 키 값과 키 아이디를 키 링에 저장하게 된다. 이 때 CH는 기존의 EG 스킴과는 다르게 k개의 키들을 저장하는 키 링 저장 공간 뿐 만이 아니라 추가로 여분의 키 저장 공간(Extra Key Space)을 갖는다. 이 여분의 키 저장 공간은 높은 우선 순위를 가진 응급 노드들과의 키 설립을 위한 공간이며 기존 EG 스킴에서 키 링을 위해 쓰이던 저장 공간의 일부를 Extra Key Space로 활용할 수 있을 것이다. 이와 같은 응급 노드를 위한 방법은 다음 절에서 사용 기법을 자세히 다루고 본 절에서는 일반 노드들을 위한 경우에 대해서 설명하도록 한다.

센서 노드들이 설치되어 동작하기 시작하면 센서 노드는 해당하는 구역의 CH에 속하게 되며 바로 CH와 센서 노드간의 키 설립 과정이 시작된다. CH와 센서 노드는 각각 갖고 있는 k개의 키들의 아이디를 서로에게 전송하게 된다. 이 때 공통된 키를 발견한다면 그 키가 CH와 센서 노드간의 Pairwise Key로 정해진다. 만일 공통된 키를 발견하지

못하는 경우에는 2.3절에서 소개한 기존의 EG 스킴에서 사용되었던 3단계인 Path Key 설립 방식을 사용하지 않는다. 왜냐하면 기존의 EG 스킴은 평면적인 네트워크 구조에 적합하도록 제안되어 본 논문에서의 계층적인 구조에서는 적합하지 않기 때문이다. 또한 본 논문에서 제안한 구조에서는 한 CH에 속한 센서 노드 수가 많지 않으며 다시 말해서 한 홉 내에 있는 센서 노드 수가 매우 적다는 것을 의미한다. 이를 통해 Path Key를 제공할 수 있는 중간 노드의 역할을 할 수 있는 노드가 있을 확률이 EG 스킴에서의 환경보다 낮다는 것을 알 수 있다. 따라서 본 논문에서 제안한 키 관리 기법에서는 공통 키를 발견하지 못한 경우에는 CH와 센서 노드는 각각 센서 노드가 가지고 있는 k개의 키 들 중 하나를 사전에 합의된 기준에 의해서 Pairwise Key로 선택한다. 예를 들어 센서 노드가 아이디가 1번, 40번, 100번인 키 들을 가지고 있다면 그 중 가장 작은 아이디를 가진 1번 키를 둘 사이의 키로 결정하게 되는 것이다. 이 때 센서 노드는 결정된 키 아이디에 해당되는 키 값을 알고 있지만, CH는 오직 키 아이디만 알고 있고 키 값을 갖고 있지 않은 상태이다. 따라서 CH는 해당 키 값을 알기 위해서 BS에 연결되어 있는 다른 모든 CH들에게 키 아이디를 담아 질의를 보내게 되고, 질의를 받은 CH들 중에서 해당 키를 자신의 키 링에 가지고 있는 CH는 키 값을 암호화하여 CH에게 전송한다. 이 때 CH들은 모두 BS를 통해 연결되어 있으므로 안전한 연결이 보장된다고 가정할 수 있다.

3.3.2 응급 센서 노드를 위한 키 설립 기법

앞서 3.3.1절에서 설명한 기법은 비응급 센서 노드들을 위한 방법으로 이와 더불어 응급 상황 발생이 높은 응급 센서 노드들을 위한 기법 또한 필요하다.

본 의료 센서 네트워크 구조에서 센서 노드들은 계속해서 이동하며 이동할 때마다 새로운 CH를 결정하게 되고 CH와 키를 설립하게 된다. 만일 새로운 CH와 센서 노드 사이에 공통 키가 있다면 즉시 키가 설립되겠지만 공통 키가 없다면 CH는 다른 이웃 CH에게 질의를 전송하고 이에 대한 응답을 받는 과정을 통해 키가 설립될 것이며 이 경우 키 설립이 지연될 것이다.

키 설립을 기다리는 동안 센서 노드는 키가 없으므로 센싱 정보를 CH에게 전송할 수 없을 것이다. 새로운 키 설립을 기다리는 동안 키로 암호화하지 않고 그대로 데이터를 CH에게 전송하는 것은 환자의 프라이버시 보호와 보안 측면에서 매우 위험한 일이기 때문이다.

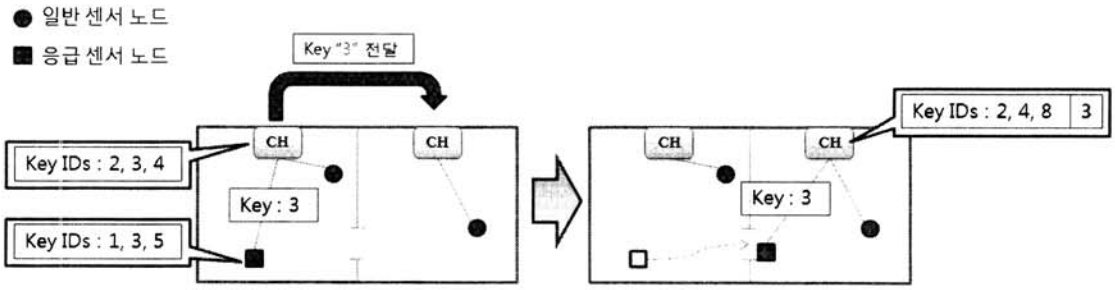
따라서 새로운 키가 설립될 때까지 일정 시간 동안 기다려야 하지만, 위급한 경우나 환자에 따라 일정 시간 동안 데이터를 보내지 못하는 것은 위험한 상황이 될 수 도 있다. 즉, 센서 노드가 한 CH에서 다른 CH로 위치를 바꾸는 그 순간 위급 상황이 발생하고 이 경우 공통키가 존재 하지 않아 키 설립이 늦어져서 응급 상황의 알림이 지체되면 이는 환자의 건강과 직결되는 위험한 상황이 될 수도 있다. 또한 환자의 모든 데이터가 면밀히 조사되어야 하는 경우에 만일 키 설립을 기다리고 있는 동안 중요한 센싱 정보가 발생하였다면 이를 CH에 전송하지 못하므로 중요한 데이터를 놓치게 될 것이다. 따라서 이와 같은 상황을 대비하여 응급 노드들을 위한 키 설립 메커니즘이 필요하다.

앞서 설명한 바와 같이 모든 CH는 k개의 키 링을 저장하는 공간과 함께 별도로 높은 우선 순위를 가지고 있는 응급 노드들을 위한 Extra Key Space를 가지고 있게 된다. 최근에 응급 상황이 발생한 경험이 있는 환자 또는 응급 상황이 발생할 가능성이 높은 환자나 지속적인 생체 정보의 관찰이 필요한 환자들이 높은 우선 순위를 갖는 환자들로 분류된다. 또한 이와 같은 환자들의 몸에 부착된 센서 노드들이 높은 우선 순위를 가진 응급 노드들로 여겨진다.

CH는 이러한 특별한 응급 노드들이 자신의 구역에 들어오게 되면 응급 노드와 키 설립을 마친 후 응급 노드와의 키 값을 지역적으로 해당 응급 노드의 다음 이동 경로에 위치해있는 이웃 CH들에게 전송하게 된다. 키 값을 받은 이웃 CH들은 이를 키 링과는 별도로 Extra Key Space에 저장하여 갖고 있는다. 또한 Extra Key Space는 제한된 저장 공간이므로 이를 관리하기 위해서는 저장된 지 가장 오래된 키 아이디를 먼저 삭제하는 방법이나 가장 덜 사용되는 노드의 키 아이디를 먼저 삭제하는 등과 같은 기법들을 적용하여 제한된 저장 공간을 보다 효율적으로 관리할 수 있을 것이다.

앞에서 나타낸 (그림 1)에서 1번 방안에 있는 노드를 부착한 환자는 이동시에 인접한 공간인 2번, 3번, 4번 공간으로만 이동이 가능하고, 5번과 6번 공간으로 가기 위해서는 2번, 3번, 4번 공간을 거쳐야 하므로 한번에 이동하는 것은 불가능할 것이다. 따라서 이 경우 1번 방의 CH는 환자가 이동 가능한 노드이자 지역적으로 이웃에 위치한 2번, 3번, 4번 방의 CH에게 키 정보를 전송한다. 이와 같이 Key Provisioning을 통해서 이웃 CH들은 키를 먼저 전해 받고 응급 노드와의 키 설립을 준비할 수 있다. 만일 CH가 한 응급 노드와 공통된 키 아이디가 없다고 하더라도 응급 노드가 도착하기 전에 미리 다른 CH로부터 키 값을 전해 받았으므로 그 값을 키로 정하여 빠르게 키 설립을 할 수 있다. 이와 같은 기법을 이용하여 CH와 센서 노드 간에 빠른 키 설립이 가능하여 응급 데이터를 빠르게 전송할 수 있을 것이다.

(그림 3)은 Key Provisioning을 사용한 응급 노드를 위한 키 설립을 보여주는 한 예이다. 사각형으로 표시된 노드는 응급 센서 노드이며 (a)와 같이 초기에 CH와 서로의 키 링을 비교하여 공통키를 발견하기 위해 시도하고 공통키 3을 발견하면 이를 CH와 응급 노드간의 키로 맺는다. 응급 노드와 키를 설립하고 나면 CH는 Key Provisioning을 위해 응급 노드와 맺어진 키인 3번 키를 미리 이웃 CH에게 전달하게 된다. 응급 노드가 이동하여 (b)에서의 그림과 같이 이웃 CH에 속하게 되면 이 때 이웃 CH는 응급 노드가 키 링에 가지고 있는 키 3번을 이미 Extra Key Space에 가지고 있으므로 CH와 응급 노드 간에 공통키를 발견하여 빠른 시간에 키 설립을 마칠 수 있다.



(a) 응급 센서 노드 이동 전 (b) 응급 센서 노드 이동 후

(그림 3) 응급노드의 이동에 따른 키 설립 예

4. 분석 및 시뮬레이션

본 장의 분석 및 시뮬레이션 결과 분석에 들어가기에 앞서서 5장 분석 및 시뮬레이션에서 사용되어지는 수식에 포함되는 기호들과 각 기호들이 나타내는 의미는 <표 1>과 같다.

〈표 1〉 수식 기호와 의미

파라미터	의미
C	전체 네트워크의 CH의 개수
Cn	한 CH에 인접한 CH들의 평균 개수
N	센서 노드들의 개수
P	센서 노드와 CH의 키 링에 서로 공통 키 아이디를 갖고 있을 확률
Pe	전체 네트워크에서 높은 우선 순위를 가진 응급 노드의 비율
R	(제안된 기법 사용시의 전송 주기) / (제안된 기법을 사용하지 않을 때의 전송 주기)
Pt	일정 시간동안 경계값을 넘는 응급 데이터가 발생할 확률
Po	전체 네트워크에서 지속적인 조사가 필요한 노드들의 비율
E	Extra Key Space에 저장 가능한 키 개수

4.1 키 설립 확률 분석

본 논문에서 소개한 계층적인 의료 센서 네트워크 구조에서 EG 스킴을 그대로 사용할 경우의 키 설립 확률과 제안한 키 설립 기법을 사용하였을 때의 키 설립 확률을 비교하여 본다.

먼저 EG 스킴과 본 논문에서 제안한 키 설립 기법을 비교하였을 때, 두 노드 간에 공통 키를 가질 확률은 모두 P로 두 기법 모두 같다고 할 수 있다. 그러나 공통 키를 발견하지 못할 경우에도 센서 노드와 CH는 키 설립이 필요한데, EG 스킴을 사용하여 Path Key를 이용하는 경우 센서 노드와 CH와의 키를 모두 갖고 있는 제 3의 노드가 필요하다. 그러나 본 논문에서의 계층적인 의료 센서 네트워크 구조 내에서는 한 개의 CH에 속한 센서 노드는 평균적으로 매우 적은 개수이고, 이는 한 센서 노드를 기준으로 통신 가능한 범위 내에 있는 즉, 한 홉 내에 있는 센서 노드 수가 기존의 EG 스킴에서의 환경보다 매우 낮다는 것을 의미한다. 따라서 본 논문에서 소개한 계층적인 구조에서는 Path Key를 전달해줄 수 있는 제 3의 노드가 존재할 확률이 매우 낮음을 알 수 있다. 그러므로 EG 스킴을 수정 없이 그대로 사용하는 경우 Path Key 설립 단계에서 키를 설립할 확률이 낮아 키를 설립하지 못하는 노드들의 수는 증가할 것이며, 반면에 제안한 기법을 사용한다면 공통키를 발견하지 못한 경우에도 높은 확률로 키 설립을 할 수 있을 것이다.

뿐만 아니라, CH가 여분의 키 저장 공간을 가지고 있고 응급 노드가 이동하기 전에 키 정보를 미리 보내주는 경우 각 CH가 가지고 있는 키들의 개수는 증가하게 된다. CH가 오직 EG스킴을 위한 k 개의 키 링만 가지고 있는 경우 $N \cdot (1 - P)$개의 노드들은 CH와 공통키를 갖지 못한다. 이에 비해서 본 논문에서 제안한 기법에 따라 CH가 여분의 키 저장 공간을 갖게 되면 공통키를 갖지 못한 노드들 중 응급 노드인 $N \cdot (1 - P) \cdot Pe$ 개의 노드들은 여분의 키 저장 공간인 Extra Key Space에 저장된 키들을 사용하여 키 설립을 완성하게 된다. 따라서 최종적으로는 $N \cdot (1 - P) - N \cdot (1 - P) \cdot Pe$ 개의 노드들이 공통키를 갖지 못한다. 이 식은 정리하면 $N \cdot (1 - P) \cdot (1 - Pe)$로 나타낼 수 있고 Pe는 1보다 항상 작고 0보다 큰 값이므로 다음과 같은 식이 성립한다.

$$N \cdot (1-P) \geq N \cdot (1-P) \cdot (1-Pe)$$

따라서 제안한대로 여분의 키 저장 공간을 가지고 있다면 CH와 센서 노드 간에 공통키를 가질 확률은 보다 높다는 것을 확인할 수 있다.

4.2 효율성 및 트래픽 오버헤드 분석

4.2.1 센싱 데이터 전송 방식의 효율성 분석

본 논문에서 제안한 계층적인 구조에서의 CH의 센싱 데이터 전송 방식의 효율성 분석을 위해 센서 네트워크에서 발생하는 트래픽 양을 비교 분석 하였다. 먼저 CH가 제안된 기법은 사용하지 않고 모든 센싱 데이터들을 짧은 주기로 전송하는 경우에 CH들과 BS 사이에 발생하는 트래픽의 양은 다음의 식 (1)과 같이 정의된다. C는 CH들의 개수이며,

R은 제안된 기법을 사용하지 않을 때의 전송 주기와 제안된 기법을 사용할 때의 비응급 데이터들의 전송 주기의 비율을 나타내기 위한 값이다. 예를 들어 제안된 기법을 사용하지 않아 1초가 전송 주기인 경우와 제안된 기법을 사용하여 보다 긴 주기인 10초가 전송 주기인 경우 R은 10이 될 것이다. 즉, 제안된 기법을 사용하지 않은 경우의 전송 주기는 모든 데이터들을 실시간으로 전송하기 위해서 상대적으로 매우 짧은 주기가 될 것이다.

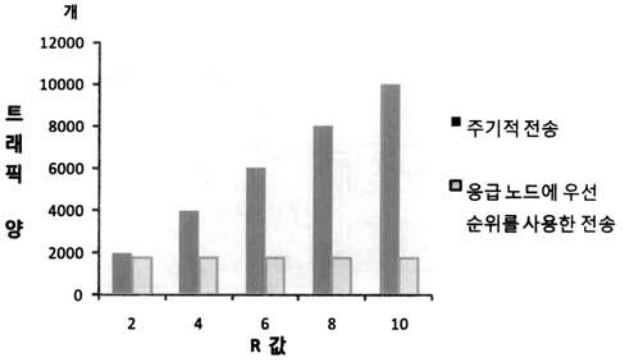
$$C \cdot R \tag{1}$$

한편, 제안한 기법을 사용하는 경우는 두 가지 경우로 나누어 계산하여 볼 수 있다. 먼저 경계값을 넘어 즉시 전송해야 하는 응급 데이터로 이는 $N \cdot Pt$로 나타낼 수 있다. 이와 더불어 지속적인 조사가 필요한 데이터들은 모아서 주기적으로 BS로 전송한다고 생각할 수 있으며 이 데이터들은 낮은 우선 순위를 갖고 있으므로 실시간으로 전해질 필요가 없으므로 큰 주기를 갖고 전송해도 무방하다. 먼저 전체 네트워크 상에서 지속적인 관찰이 필요한 노드의 수는 $N \cdot Po$이므로, 한 CH당 속한 지속적인 관찰이 필요한 환자의 센서 노드들의 수는 $(N \cdot Po)/C$와 같다. 이 때 한 CH 가 가지고 있는 노드 수 $(N \cdot Po)/C$의 수가 1을 넘으면 이는 일정 주기로 전송해야 할 트래픽의 수를 적어로 1개 포함하고 있다는 의미이며 이 때 일정 주기로 전송할 트래픽이 1개 있던지 또는 2개, 3개가 있던지 모두 모아서 한꺼번에 전송이 가능할 것이다. 따라서 $(N \cdot Po)/C$가 1이상인 경우에는 전체 네트워크에 대해서는 C번의 전송 회수가 필요하다. 그러므로 응급 데이터 전송과 지속적인 조사가 필요한 데이터들의 전송량을 합하면 다음과 같이 나타낼 수 있다.

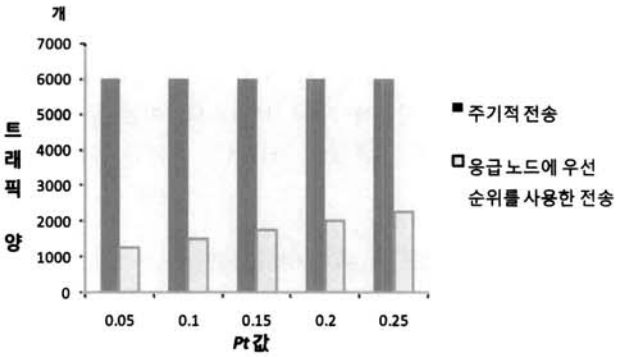
$$N \cdot Pt + N \cdot Po \text{ or } N \cdot Pt + C \tag{2}$$

이와 같은 (1)과 (2)의 수식을 이용하여 5000개의 노드들, 1000개의 CH들을 가진 네트워크라고 가정하였고 지속적인 조사가 필요한 센서 노드들을 30%라고 하여 Po값을 0.3으로 놓고 분석하였다. (그림 4)는 응급 노드 발생 확률인 Pt 값을 0.15로 고정하고 전송 주기와 관련된 R값은 변화시키며 전체 네트워크의 트래픽 양을 분석한 그래프이다. 다시 말해서 제안된 기법을 사용하여 보다 긴 주기로 조사가 필요한 데이터를 보내고 실시간으로 응급 데이터를 전송하는 경우와, 보다 짧은 주기를 갖고 모든 데이터를 전송하는 경우를 비교하였다.

(그림 5)는 R값을 6으로 고정시키고 Pt값을 변화시키며 트래픽 양을 분석한 그래프이다. 두 개의 그래프를 통해서 짧은 주기로 모든 데이터들을 BS로 전송했을 때보다 제안한 기법을 사용했을 때의 적은 양의 트래픽이 발생함을 확인할 수 있으며 이를 통해 효율성이 증가됨을 확인할 수 있다.



(그림 4) R값을 변화시킴에 따른 트래픽 양 비교



(그림 5) Pt값을 변화시킴에 따른 트래픽 양 비교

4.2.2 키 관리 기법의 효율성 및 오버헤드 분석

먼저, 기존의 EG 스킴을 본 논문에서 소개한 계층적인 의료 센서 네트워크 구조에서 사용하게 된다면 단지 CH와 센서 노드 사이에서의 키 설립 뿐 만이 아니라 센서 노드와 센서 노드 간의 키 설립 또한 이루어져야 한다. 왜냐하면 공통 키를 발견하지 못하고 Path Key 설립 단계에서 키를 설립할 경우 센서 노드와 CH 모두와 키를 갖고 있는 제 3의 노드가 필요하기 때문이다. 이처럼 모든 센서 노드들 사이에 키 설립을 위한 시도를 하게 된다면, 위의 4.1절에서 분석한 바와 같이 적은 수의 센서 노드들로 인해 키 설립이 성공할 확률도 적을 뿐만 아니라, 키 설립이 성공한다 하더라도 이는 데이터 전송이 아닌 단지 Path Key 설립만을 위해 키를 설립하기 위한 시도이므로 이 때 발생할 트래픽은 에너지 비효율적이며 낭비일 것이다. 그러므로 EG 스킴을 그대로 사용하는 것보다 제안하는 키 관리 메커니즘을 사용하는 것이 더욱 효율적이라 할 수 있다.

본 절에서는 제안하는 키 관리 기법을 사용하는 경우 트래픽 오버헤드를 비교하여 봄으로써 그 효율성을 증명하고자 한다. 이를 위해 모든 CH가 오직 k 개의 키 링만을 가지고 있는 경우와 k 개의 키 링과 더불어 여분의 키 저장 공간을 가지고 있는 두 가지 경우를 비교하여 보았다. 이 때 공통키가 존재하는 경우는 두 경우에 모두 각 노드는 한 번씩의 전송이 일어나므로 $N \cdot P$ 로 나타낼 수 있을 것이다. 공통키가 존재하지 않는 경우에 대한 계산은 다음과 같다.

먼저, CH가 오직 k 개의 키 링만 가지고 있는 경우의 트래픽 오버헤드를 계산해 보면 CH와 노드간에 공통 키를 갖

고 있지 않은 확률은 *(1 - P)*로 나타낼 수 있으며 전체 네트워크에서 초기에 CH와의 공통 키를 발견하지 못한 노드들의 개수는 $N \cdot (1 - P)$와 같다. 이와 같이 공통 키가 존재하지 않은 센서 노드들에 대해서 새롭게 키를 설립하기 위해 한 개의 CH를 기준으로 했을 때 필요한 트래픽의 종류는 다음의 세 가지이다. 첫째, 해당 CH가 다른 CH들에게 해당 키를 가지고 있는지 질의를 던지는 트래픽으로 최악의 경우 이는 자신을 뺀 다른 모든 CH에게 보내는 패킷이므로 $(C - 1)$로 나타낸다. 둘째, 해당하는 키를 가진 이웃 CH들이 질의를 보낸 CH에게 키 값을 실어서 응답 패킷을 보내주는 것으로 이는 $(C - 1) \cdot P$와 같다. 셋째, 센서 노드에게 알려주는 ACK 프레임으로 한 개의 CH를 기준으로 했을 때 1개가 필요할 것이다. 따라서 위의 세 종류의 개수를 모두 합쳐서 전체 네트워크에 대해서 공통 키를 찾지 못한 노드들에게 부가적으로 필요한 트래픽의 양은 다음과 같이 나타낼 수 있다.

$$N \cdot (1-P) \cdot \{(C-1) + (C-1) \cdot P + 1\} \quad (3)$$

다음으로, CH가 k 개의 키 링 뿐만이 아니라 여분의 키 저장 공간을 가지고 있을 경우에 대해서 고려해보아야 한다. 이 때 높은 우선 순위를 갖는 응급 노드들에 대해서 CH는 미리 이웃 CH들에게 키 정보를 전송하게 되고 이 때 필요한 트래픽의 수는 다음과 같다.

$$C \cdot Cn \cdot (N/C) \cdot Pe \quad (4)$$

또한 공통 키가 없는 노드들 중에서 응급 노드가 아닌 노드들에 대해서는 위의 식(3)과 같은 양의 트래픽이 필요하게 된다. 따라서 이는 다음과 같다.

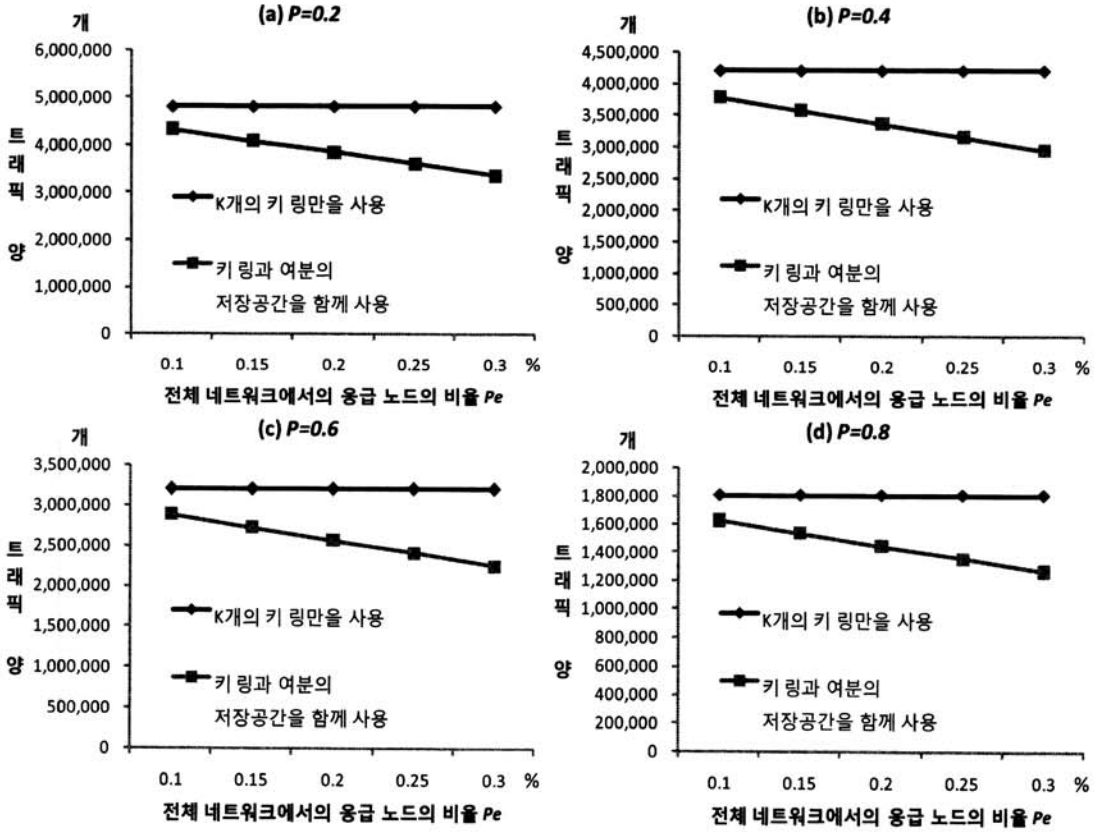
$$N \cdot (1-P) \cdot (1-Pe) \cdot \{(C-1) + (C-1) \cdot P + 1\} \quad (5)$$

그러므로 공통키가 존재하는 경우의 $N \cdot P$와 공통키가 존재하지 않을 경우의 트래픽 양 수식 (3)과 수식 (4)와 (5)를 더한 값을 비교하여 트래픽 양을 분석하였다. 이를 위해 전체 네트워크에 5000개의 센서 노드와 1000개의 CH를 갖고 있다고 가정하였다. [그림 6]은 *Pe*값을 0.1에서 0.3까지 0.15간격으로 변화시켜 가면서 트래픽 발생 수를 계산해본 결과이다. 또한 [그림 6]의 (a)에서 (d)까지 P값을 0.2, 0.4, 0.6, 0.8로 변화를 주어 각각의 경우에 대해 트래픽 발생 수를 비교해보았다. 이를 통해서 제안한 키 관리 기법을 통해 여분의 키 저장 공간을 둔 경우 네트워크 트래픽 오버헤드가 더 적음을 확인할 수 있다.

4.3 시뮬레이션 결과 및 분석

4.3.1 센싱 데이터 전송 방식의 시뮬레이션 내용 및 결과

본 논문에서는 계층적인 의료 센서 네트워크 구조에서의



(그림 6) P와 Pe의 변화에 따른 트래픽 양의 비교

센싱 데이터 전송 방식의 효율성을 증명하기 위하여 시뮬레이터 QualNet 4.5를 이용하여 발생 트래픽과 에너지 소모량을 측정하는 시뮬레이션을 진행하였다.

QualNet 은 설계된 프로토콜 및 어플리게이션을 분석하고 성능 검증을 수행하기 위하여 가상의 네트워크를 구축하여 그 결과를 예측하고 문제점을 분석할 수 있는 소프트웨어이다[11]. WLAN을 비롯하여, 센서 네트워크, 모바일 애드혹 네트워크, 유선 랜, WAN, 셀룰러 네트워크, 위성 네트워크에 대한 기본적인 라이브러리를 가지고 있으며 사용자가 이 프로토콜을 수정하여 확장 사용할 수 있다. 이처럼 시뮬레이션을 수행하기에 적절한 여러 환경을 제공하고 있어 현재 널리 사용되고 있는 네트워크 시뮬레이션 도구이다. 본 논문에서는 QualNet 4.5 버전을 사용하였고 IEEE 802.15.4 프로토콜을 사용하고 있는 센서 네트워크 라이브러리를 활용하여 시뮬레이션을 진행하였다.

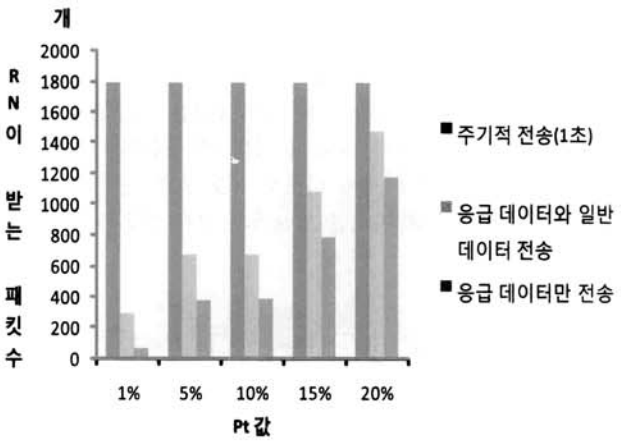
QualNet을 이용하여 우리의 계층적인 구조를 바탕으로 한 센싱 데이터 전송 방식을 시뮬레이션하기 위해 1개의 RN, 1개의 CH, CH에 속한 4개의 센서 노드로 네트워크를 구성하였다. 이를 1800초 동안 시뮬레이션 하였으며 4개의 센서 노드들은 각각 매 1초마다 CH로 센싱 정보를 전송하고 CH는 센서 노드로부터 전달 받은 패킷들을 RN으로 전달한다. 이 때 RN에서 BS로의 패킷 전달은 CH에서 RN으로의 트래픽 발생량과 동일하므로 생략하였다.

CH가 RN로 패킷을 전달하는 방법은 모두 세 가지 경우로 하여 각각을 비교하고 제안한 메커니즘의 효율성을 증명하였다. 첫 번째 경우는 CH가 센서 노드로부터 받은 패킷들을 매우 짧은 주기로 실시간에 가깝게 전송하는 것으로 본 시뮬레이션에서는 1초마다 한번씩 RN으로 전송하도록 하였다. 두 번째 경우는 Threshold 값 이상의 데이터를 발생 시킨 응급 발생 노드의 데이터는 발생 즉시 CH가 RN으로 전송하고, 이와 동시에 지속적인 조사가 필요한 낮은 우선순위의 노드들의 데이터는 보다 큰 주기인 10초 간격으로 전송하는 방법이다. 세 번째 경우는 지속적인 조사가 필요한 노드가 없다고 가정하고 응급 발생 노드들의 데이터만 RN으로 전송하는 방법이다.

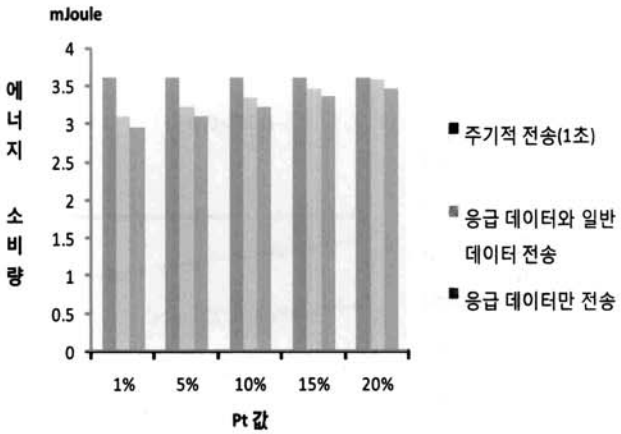
(그림 7)은 *Pt*값의 변화에 따라 RN이 받는 패킷 양의 변화를 보여준다. 이를 통해 주기적으로 전송하는 것에 비해 제안한 센싱 데이터 전송 방식을 사용할 때에 RN이 받는 패킷 수는 적으며 따라서 네트워크에 발생하는 트래픽 오버헤드가 줄어듬을 예상할 수 있다.

(그림 8)은 각 센서 노드의 에너지를 측정하기 위해 QualNet에서 각 노드의 에너지 측정 방식을 MICAz로 파라미터 값을 정하고 각 노드의 에너지를 측정하였으며 응급 데이터가 발생할 확률인 *Pt*값이 변화함에 따라 RN으로 패킷을 전달하는 CH의 에너지 소비량의 변화를 보여주고 있다. 이를 통해 제안한 센싱 데이터 전송 방식을 사용할 때에 전달해야 할 패킷 수가 줄어들고 이에 따라 소비되는 에너지양도 줄어듬을 알 수 있다.

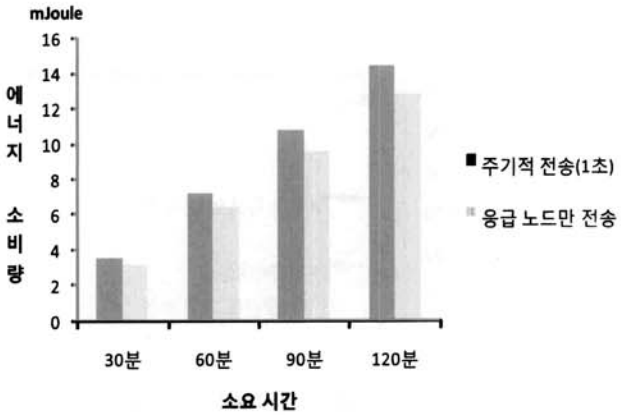
이는 1800초 동안의 시뮬레이션이므로 시간이 지남에 따라 주기적인 전송과 응급노드와 관찰 노드의 전송 사이에는 더 많은 에너지 차이가 생길 것으로 예상해 볼 수 있다. 이를 바탕으로 *Pt*값을 고정시키고 각 시뮬레이션 시간을 증가시켜보면서 CH의 에너지 소비량을 측정하여 보았다. (그림 9)는 이와 같은 시뮬레이션의 결과를 보여주며, 짧은 주기로 계속적으로 전송할 때와 응급 노드만 전송할 때의 에너지 차이가 점점 커짐을 보여준다. 따라서 이러한 추세를 생각



(그림 7) *Pt*값의 변화에 따라 RN이 받는 패킷 양 비교



(그림 8) Pt값의 변화에 따른 CH의 에너지 소비량



(그림 9) 소요 시간에 따른 에너지 소비량

한다면 실제 응용 환경에서 수 일 동안 센서가 동작할 경우 제안한 센싱 데이터 전송 방식의 에너지 소비가 보다 효율적임을 알 수 있다. 다음 그래프를 통해 제안된 메커니즘의 효율성을 증명하였다.

4.3.2 키 관리 기법 시뮬레이션 내용 및 결과

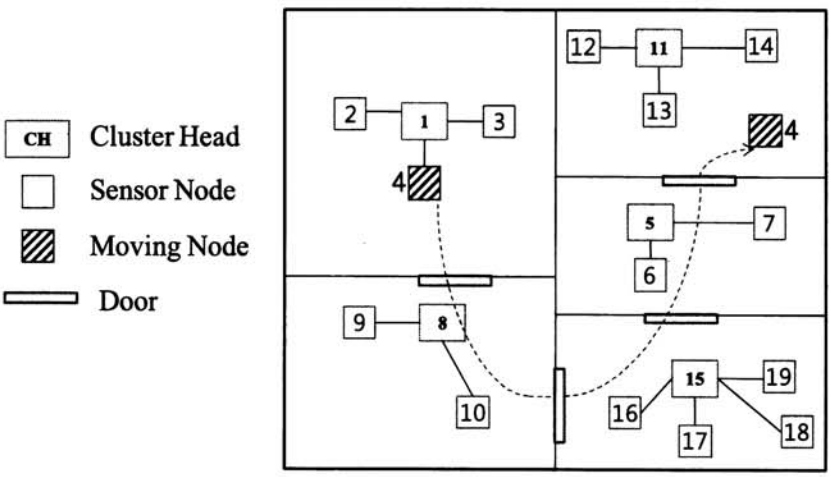
Key Provisioning을 이용한 키 관리 기법을 QualNet 시뮬레이터를 이용하여 시뮬레이션을 진행하였다. 이를 위해서 총 600초 동안 시뮬레이션을 진행하되 (그림 10)과 같이 전체 네트워크를 1개의 BS, 5개의 CH, 14개의 센서 노드로 구성하였고, 이 중 한 개의 센서 노드인 4번 노드는 1번 CH에서부터 8번, 15번, 5번, 11번 CH의 구역으로 차례로 이동하도록 시나리오를 구성하였다. 또한 센서는 이동하여 새로운 CH를 만날 때마다 새로운 키를 설립하기 위해 서로 자신의 키 링 정보를 담은 패킷을 전송하여 키를 설립하기 위해 시도한다. 즉, 0초에서 100초까지는 1번 CH의 구역에 속해 있도록 하여 1번 CH에게 데이터를 전송하며, 101초가 되면 4번 노드는 이동하여 8번 CH의 구역으로 들어온다. 이 때, 4번 노드는 1번 CH에게 더 이상 데이터를 전송하지 않고, 자신이 속한 8번 CH에게 데이터를 전송하게 될 것이다. 따라서 데이터 전송을 위해 8번 CH와 키 설립을 시도하게 되고, 계속해서 8번 CH에게 데이터를 전송한다. 이 후 201초가 되면 4번 노드는 15번 노드의 구역으로 이동하여 들어가며 이처럼 각각 5번, 11번으로 차례로 이동하도록 시나리오를 구성하였다. 예를 들어, 이 상황은 4번 노드를 부착한 환자가 병원 내에서 일상적으로 병실, 휴게실, 화장실 등으로 이동하는 것으로 고려해 볼 수 있을 것이다.

각 노드들은 k값을 3으로 하여 총 3개의 키 링을 갖고 있으며 Extra Key Space에도 추가 3개의 키를 저장할 수 있도록 하였다. 또한 해당 CH와 0.6의 공통키를 가질 확률을 가지고 키를 설립하게 되도록 미리 각 노드와 CH의 키 링에 키를 분배하여 시나리오를 구성하였다. <표 2>를 통해서 나타난 것과 같이 노드 4번이 각 CH와의 공통키를 갖고 있는지를 알 수 있다. 즉 노드 4번은 CH 1번, 15번, 11번과는 공통키를 가지고 있지만 8번, 5번과는 공통키를 가지고 있지 않다.

공통키가 존재하는 경우 키 설립 시간은 서로의 키 링을 받아 공통된 키만 찾으면 되므로 거의 0초에 가깝게 측정되어 0초로 간주할 수 있다. 반면 공통키가 존재하지 않는 경우에 대해서 Key Provisioning 기법을 사용하지 않는다면 이웃 CH들에게 질의를 던지고 응답을 받아야 하므로 시간이 지연될 수 있다. 이 경우 처음 CH로부터 신호를 받고 키 설립이 완료 되었음을 알리는 ACK 메시지를 받을 때까지의 시간을 측정한 결과가 <표 2>에 나타난 시간과 같다. 그러므로 Key Provisioning을 사용한 경우 0초에 가까운 시간이 걸리므로 각각 1165.24 msec 초와 827.87 msec가 걸리는 것은 이와 비교하여 상대적으로 긴 시간이라 할 수 있을 것이다. 이는 Key Provisioning을 사용한 경우 키 설립 지연으로 인해 데이터가 누락되거나 환자 정보가 암호화 되지 않은 상태에서 전달되는 경우를 방지할 수 있게 해 주는 것을 의미한다.

5. 구현 결과 및 분석

제안한 키 설립 기법은 TinyOS 2.0 환경하에서 모티브



(그림 10) 시뮬레이션에서 사용된 노드4의 이동 경로

〈표 2〉 노드 4번의 각 CH 에 따른 키 설립 시간 비교

CH 번호	1	8	15	5	11
공통 키 존재 여부	O	X	O	X	O
Key Provisioing을 사용하지 않을 때 키 설립 시간	0 *sec*	1165.24 *msec*	0 *sec*	827.87 *msec*	0 *sec*

사의 대표적인 센서 모트 중의 하나인 TmoteSKY 상에 구현하였다. TmoteSKY는 msp430 마이크로 콘트롤러와 CC2420 RF Chip을 탑재하고 있으며, 센서가 보드에 통합되어 있는 on-board 센서노드이다. IEEE 802.15.4 표준과 호환되며 250 kbp 의 높은 데이터 전송률을 보인다.

구현을 위해서 총 4개의 센서 모트를 사용하였으며 사용된 구성 및 시나리오는 다음과 같다.

(1) 센서 노드 구성

- 2개의 모트는 클러스터 헤드 역할을 하며, CH1과 CH2로 각각 나타낸다.
- 2개의 모트는 센서 노드 역할을 하며 Mote3과 Mote4로 각각 나타낸다.

(2) 구현 시나리오

- Mote3은 CH1의 구역에서 CH2의 구역으로 이동하는 센서 모트의 역할을 한다. 이를 위해 초기 12.5초 동안은 CH1에게 패킷을 전송하고, 그 이후에는 CH2에게 패킷을 전송한다.
- Mote4는 CH1의 구역에 속하여 이동하지 않는 센서 모트의 역할을 한다. 이를 위해 속해진 CH의 변경없이 계속해서 CH1에게만 패킷을 전송한다.
- 모든 센서 노드들은 0.125초마다 자신이 속한 클러스터 헤드에게 패킷을 전송하며, 이와는 별도로 추가적으로 Key Provisioning과 관련된 요청 메시지, 응답 메시지 등은 필요한 즉시 전송할 수 있도록 구현하였다.

(3) 각 노드들의 키 정보

모든 노드들은 사전에 필요한 키 링 정보들을 가지고 있도록 하였다. 각 센서 노드들은 배열을 사용하여 총 3개의 키를 저장할 수 있는 크기의 키 링을 가지고 있으며, CH들은 키 링 외에 추가로 Extra Key Space에 3개의 Extra Key를 저장할 수 있도록 설정하였다. 각 노드들이 키 링에 가지고 있는 키들의 정보는 <표 3>과 같이 구성하였다.

모든 센서 노드들의 동작이 시작되면 Mote3은 CH1과의 키를 찾기 위해 시도하고 즉각 공통 키인 <30>을 키로 설정한다. 그 후 CH2의 구역으로 이동하게 되면 CH2와 Mote3은 공통 키가 없으므로 키 설립을 위한 추가적인 과정이 필요하다. 만일 Mote3이 응급 노드라면 Key Provisioning 기법을 사용할 것이며, 응급 노드가 아니라면 CH2는 Mote3의 메시지를 처음 받았을 때 키 설립을 위해 다른 CH에게 부가 키 요청 메시지를 보낼 것이다.

이와 같은 센서 모트들이 올바르게 동작하는 것은 TinyOS 2.0에서 제공되는 Printf 라이브러리를 이용하여 확인해볼 수 있었다. 또한 각 노드 당 사용되는 저장 공간을 분석하여 보았을 때, CH의 동작을 위해서는 22603 bytes ROM, 988 bytes RAM, 22634 bytes program 의 메모리가 필요함을 확인하였고, 센서 노드의 동작을 위해서는 21720 bytes ROM, 962 bytes RAM, 21752 bytes program의 메모리가 사용되었다. 이와 같은 구현 과정을 통해 실제 환경에서의 센서 노드를 이용한 응용 가능성을 입증하였다.

6. 결 론

본 논문에서는 의료 센서 네트워크 환경의 특징을 고려하여 Key Provsioning을 사용한 효율적이고 빠른 데이터 전송을 제공하는 키 관리 기법을 제안하였다.

의료 센서 네트워크 환경에서는 센서 노드의 이동성, 센싱 데이터들간의 비연관성, 센싱된 의료 정보의 프라이버시 보호, 사용자(환자)들의 요구 사항 반영, 노드의 구별 및 아이디 등의 특징을 고려하여야 한다. 이와 같은 의료 환경에서의 특징들을 고려한 의료 센서 네트워크를 위한 BS, RN, CH, 센서 노드들로 구성된 계층적인 구조를 제안하였다. 이와 같은 계층적인 구조를 바탕으로 환자의 건강 상태를 고려하여 각 센서 노드들에게 우선 순위를 주어 관리하였고, 센싱 데이터 전송을 위해서 각 노드마다 경계값을 정하고 경계값이 넘는 데이터들은 높은 우선 순위를 가지고 즉시 전송하는 기법을 사용하였다.

또한 센싱 데이터 전송에 있어서 보안을 함께 제공하기 위해서 EG 스킴을 기반으로 하는 키 관리 기법을 제안하였다. 이를 위해 Extra Key Space를 각 CH에 추가하여 응급 노드들에 대해서는 이웃 CH들에게 키를 미리 전달하여 응급 노드와의 키 설립을 미리 준비하도록 하는 Key Provisioning 기법을 제안하였다.

이들은 각각 수식을 통한 분석과 QualNet 시뮬레이터를 이용한 시뮬레이션을 통해서 네트워크 트래픽이 감소하는 사실과 에너지 사용량이 감소함을 확인할 수 있었다. 또한 시뮬레이션에서 살펴본 것과 같이 Key Provisioning 기법을 사용하여 키 설립을 하는 경우 사용하지 않았을 때와 비교하여 보다 빠르게 키 설립이 완료되었다. 따라서 본 논문에서 제안한 기법은 오버헤드와 에너지 소모, 그리고 소요 시간 측면에서 보다 효율적일 것이다. 뿐만 아니라

〈표 3〉 각 노드들의 키 링 정보

Mote Number	키 링에 있는 키들의 아이디		
Mote 1 (CH1)	10	30	50
Mote 2 (CH2)	20	40	60
Mote 3	5	30	70
Mote 4	10	40	80

TmoteSKY에 직접 구현하여 봄으로써 실제 센서 환경에서의 응용 가능성을 확인할 수 있었다.

앞으로 향후 연구에서는 제안한 키 관리 기법을 보다 개선시키고 상세히 분석하여 여분 저장 공간이 필요로 하는 저장 공간의 크기를 최소화하면서 최대의 효율을 낼 수 있는 기법에 대한 연구를 진행하여 볼 것이다. 특히 기존의 EG 스킴과 동일한 키 저장 공간을 사용하면서 그 중의 일부를 일반 키 링 저장 공간과 Extra Key Space 저장 공간으로 활용하는 경우에 대해 고려하여 볼 것이며 이때의 최적의 Key Space의 크기에 대해 분석할 것이다. 이는 응급 환자를 위한 의료 센서 노드의 동작에 유용하게 활용될 수 있을 것이다.

참 고 문 헌

[1] 김신효, 강유성, 정병호, 정교일, "u-센서 네트워크 보안 기술 동향", 전자통신동향분석, 제20권, 제1호, pp.93-99, 2005년 2월.

[2] 김도현, 이성협, 윤양문, "WBAN 표준화 동향", Standard and Technology Review, pp.25-33, 2007년 9월.

[3] V. Shnayder, B.-R. Chen, K. Lorincz, T. R. F. Fulford-Jones, and M. Welsh, "Sensor Networks for Medical Care," Technical Report TR-08-05, Harvard University, April, 2005.

[4] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton. "Codeblue: An Ad hoc Sensor Network Infrastructure for Emergency Medical Care," Proc. of Workshop on Wearable and Implantable Body Sensor Networks, 2004.

[5] K. Malasri and L. Wang, "Addressing Security in Medical Sensor Networks," Proc. of the 1st ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments, pp.7-12, 2007.

[6] O. G. Morchn, H. Baldus and D. S. Snchez, "Resource-Efficient Security for Medical Body Sensor Networks," Proc. of International Workshop on Wearable and Implantable Body Sensor Networks 2006, pp.80-83, 2006.

[7] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic., "ALARM-NET: Wireless Sensor Networks for Assisted-Living and Health Monitoring," Technical Report CS-2006-01, University of Virginia, 2006.

[8] C. C. Tan, H. Wang, S. Zhong and Q. Li, "Body Sensor Network Security : An Identity-Based Cryptography Approach," Proc. of the first ACM conference on Wireless network security pp.148-153, April, 2008.

[9] L. Eschenauer and V.D. Gligor, "A key management scheme for distributed sensor networks," Proc of 9th ACM Computer and Communications Security 2002, pp.41-47, 2002.

[10] J. Spencer, "The Strange Logic of Random Graphs, Number 22 in Algorithms and Combinatorics", Springer-Verlag, 2000.

[11] http://www.scalable-networks.com

서 재 원

e-mail : seojw@ewhain.net

2006년 이화여자대학교 컴퓨터학과(학사)

2008년 이화여자대학교 컴퓨터정보통신공학과(석사)

2008년~현 재 SK C&C

관심분야 : 센서 네트워크 보안, 유비쿼터스 네트워크 보안, 키 관리 기법

김 미 희

e-mail : iceblueee@gmail.com

1997년 이화여자대학교 전자계산학과(학사)

1999년 이화여자대학교 컴퓨터학과(석사)

1999년~2003년 한국전자통신연구원 연구원

2003년~2007년 이화여자대학교 컴퓨터학과(박사)

2007년~2009년 이화여자대학교 컴퓨터공학과 전임강사

2009년~현 재 미국 North Carolina State University 컴퓨터공학과 Postdoc Researcher

관심분야 : 무선 네트워크(센서네트워크, 유비쿼터스네트워크, 메쉬 네트워크) 보안, 물리계층 보안

채 기 준

e-mail : kjchae@ewha.ac.kr

1982년 연세대학교 수학과(학사)

1984년 미국 Syracuse University 컴퓨터학과(석사)

1990년 미국 North Carolina State University 컴퓨터공학과(박사)

1990년~1992년 미국 해군사관학교 컴퓨터학과 조교수

1992년~현 재 이화여자대학교 컴퓨터공학과 교수

관심분야 : 네트워크 보안, 인터넷/무선통신망/고속통신망/센서네트워크 (보안)프로토콜 설계 및 성능분석