헬스케어 센서 네트워크에서 데이터 보안을 지원한 자기구성 라우팅 프로토콜 설계

남진우* · 정영지*

*원광대학교 컴퓨터공학과

Design Self-Organization Routing Protocol for supporting Data Security in Healthcare Sensor Network

Jin-Woo Nam* · Yeong-Jee Chung*

*Dept of Computer Engineering, Wonkwang University

E-mail : pote333, yjchung@wonkwang.ac.kr

이 논문은 2008년 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(지방연구중심대학육성사업/헬스케어기술개발사업단).

요 약

헬스케어 환경을 지원하는 무선 센서 네트워크는 사람이나 이동성을 가진 사물에 대하여 연속적인 위치변화와 상태정보 등 해당 상황정보에 따른 맞춤형 서비스를 제공해야 한다. 또한 센서 네트워크를 통해 제공되는 사람의 생체정보와 개인 프라이버시 보안을 보장할 수 있는 데이터 전송을 고려하여야 한다.

본 논문에서는 노드 간 계층적 클러스터의 구성을 통한 동적 자기구성, 에너지 효율성을 보장하는 LEACH 프로토콜과 노드 간 데이터 전송에 대한 보안을 위해 사용되는 키 분배 프로토콜에 대해 분석한다. 이 분석 결과를 기반으로 센서노드에 메모리 소모량이 적은 키 풀 사전 분배 방식과 클러스터 단위 공용키 방식을 적용함으로써 보안을 강화한 데이터 전송 방식과 기존 LEACH 프로토콜의 취약점인 노드 이동성을 지원하는 자기구성 라우팅 프로토콜을 제안한다.

ABSTRACT

Wireless sensor network supporting healthcare environment should provide customized service in accordance with context information such as continuous location change and status information for people or movable object. In addition, we should consider data transmission guarantees a person's bio information and privacy security provided through sensor network.

In this paper analyzes LEACH protocol which guarantees the dynamic self-configuration, energy efficiency through configuration of inter-node hierarchical cluster between nodes and key distribution protocol used for security for data transmission between nodes. Based on this analysis result, we suggested self-configuration routing protocol supporting node mobility which is weakness of the existing LEACH protocol and data transmission method by applying key-pool pre-distribution method whose memory consumption is low, cluster unit public key method to sensor node.

키워드

Healthcare Service, Sensor Network, Routing Protocol, Key Pre-distribution

Ⅰ. 서 론

센서 네트워크는 초경량, 저전력의 무선 센서들을 센싱 지역에 분산시켜 수집된 데이터를 주변 센서노드들과의 협업을 통해 수집노드로 전송하는 무선 네트워크 기술을 의미한다. 초기의 센서 네트워크는 군용 및 재해, 오지 등의 환경 모니터링이 주축을 이루었다. 현재는 유비쿼터스 컴퓨팅 개념의 도입과 함께 이를 실생활에 적용시킬 수 있는 방안이 활발하게 연구되고 있다. 이러한 응용분야 중 헬스케어를 위한 서비스 환경을 제공해 줄 수 있는 센서 네트워크가 주요 이슈로 부각되고 있다. 일반적인 센서 네트워크 환경과 달리 헬스케어 환경에서는 이동성을 가진 대상에 대한 대량의 정보수집, 교환, 처리가 요구된다. 이와 같은 환경에서의 센서 네트워크는 에너지 효율성, 동적 자기구성, 이동성에 적합하도록 개발되어야 한다.

또한, 헬스케어 환경에서 무선통신을 통해 데이터가 유출되거나 변형되면 사람의 생체정보나 위급상황에 따른 대처가 늦어지거나 잘못되는 심각한 문제가 발생하게 된다. 이에 따라 보다 현실적이고 안전한 헬스케어 환경을 구현하기 위해서는 센서 네트워크 상 보안 매커니즘 개발이 반드시 필요하며, 노드들 사이에 안전한 데이터 전송을 위한 키 분배 방식이 필수적으로 요구된다.

본 논문에서는 분산 센서 네트워크에서 노드 간 계층적 클러스터의 구성을 통한 동적 자기구성, 에너지 효율성을 보장하는 LEACH[1,2] 프로토콜과 노드 간 데이터 전송의 보안을 위해 사용되는 키 분배 프로토콜에 대해 분석한다. 이 분석 결과를 기반으로 센서노드에 메모리 소모량이 적은 키 풀을 사전 분배하여 클러스터 단위의 공용키를 설정함으로써 보안을 강화한 데이터 전송을 보장하고 기존 LEACH 프로토콜의 취약점인 노드 이동성을 지원하는 자기구성 라우팅 프로토콜인 LEACH_Mobile[3] 프로토콜을 제안한다.

Ⅱ. 관련 연구

본 절에서는 센서 네트워크의 자기구성과 제한된 전원 문제에 있어 유용한 해결방안인 LEACH 프로토콜을 분석한다. 그리고 헬스케어 환경과 같이 고정된 인프라 구조가 없으며 네트워크 토폴로지가 사전에 알려져 있지 않은 분산 센서 네트워크에서 적용되는 키 분배 프로토콜에 대해서 분석한다.

2.1 LEACH

LEACH 프로토콜은 주변노드들 간의 자기구성을 통한 계층적인 구조를 형성하는 클러스터링 알고리즘을 기반으로 네트워크의 범위성을 용이하게 하여 정보전달의 효율성을 높이고 센서노드 간의 에너지 소모를 균등하게 함으로써 네트워크 생존시간을 최대화하여 제한된 전원에 대한 유용한 해결책을 제시한다. LEACH 프로토콜 기반의 네트워크는 임의의 클러스터를 구성하고 클러스터마다 하나의 헤드 노드를 선출한다. 클러스터 내부의 센서노드들은 클러스터 헤드 노드로 데이터를 전송하고 클러스터 헤드 노드는 이를 병합하여 싱크에게 직접 전송한다. 에너지 소모가 균등하게 이루어지도록 일정 시간 마다 클러스터를 재구성하고 헤드 노드를 재 선출한다. 클러스터 내부의 일반 노드들은 클러스터 헤드 노드로 데이터를 전송하고 클러스터 헤드 노드는 이를 병합하여 싱크에게 직접 전송한다.

2.2 분산 센서 네트워크의 키 분배 프로토콜

센서 네트워크에서 노드들끼리의 안전한 통신을 위해서는 네트워크가 형성되기 전에 사전에 저장해 놓은 키를 사용하거나, 네트워크가 형성된 이후 이웃노드와의 통신을 위해 동적으로 생성한 pair-wise key와 group-wise key를 이용한다. 노드들 간에 안전한 통신을 위한 패스 키(path-key)를 설정하는 방식으로는 고정된 키 풀(key-pool)과 키 체인(key-chain)을 이용하는 결정론적 방법과 키 풀로부터 랜덤하게 선택된 키 체인을 이용하는 확률론적 방법이 있으며, 확장성과 저항성을 개선하기 위해 두 방식을 혼합한 하이브리드 방식이 있다[4].

Ⅲ. 보안을 강화한 LEACH_Mobile 프로토콜

최근 헬스케어는 환자 중심의 질병, 증상을 완화와 치료에서 점차 일반인의 건강을 증진하고 질병을 예방하는 개념으로 변화되고 있다. 이를 위해서 정보통신 기술과 의료 서비스를 융합하여 언제 어디서나 예방, 진료, 치료 그리고 사후관리를 받을 수 있는 헬스케어 응용 서비스가 제공되어야 한다. 즉, 댁내의 사람과 사물 같은 객체의 위치를 인식하고 이를 기반으로 연속적인 거주자의 상황정보에 따른 맞춤형 헬스케어 서비스를 제공해야 한다[5].

또한, 헬스케어 환경에서의 센서 네트워크는 사람의 생체정보 등의 보안이 매우 중요하다. 보안이 결여된 센서 네트워크에서는 공격자가 쉽게 트래픽을 엿볼 수 있고 주변노드에게 잘못된 정보를 제공함으로써 센서노드로 인식시킬 수 있다. 이는 헬스케어 환경에서 잘못된 대처로써 심각한 문제를 발생시키게 된다.

본 절에서는 헬스케어 환경을 지원하기 위하여 다수의 노드가 밀집된 공간에서 주변노드간의 클러스터를 구성함으로써 제한된 전원문제와 정보전달의 효율성 그리고 노드의 이동성을 보장하며 키 사전 분배 방식을 이용한 클러스터 단위의 공용키를 설정하여 데이터 전송에 대한 보안을 지원한 LEACH_Mobile 프로토콜을 제안한다.

3.1 LEACH_Mobile 프로토콜 실행단계

LEACH_Mobile 프로토콜의 실행단계는 라운드로 이루어져 있으며 클러스터를 구성하는 Set-Up Phase로 시작하여 베이스 스테이션에 데이터를 전송하는 Steady-State Phase가 이어진다. LEACH_Mobile 프로토콜의 기본 개념은 이동하는 노드가 주어진 TDMA 스케줄에 따른 시간 슬롯에서 클러스터 헤드로부터 이동노드에 데이터 요청 메시지를 전송하여 특정 클러스터 헤드 노드와 통신이 가능한지의 여부로서 클러스터의 멤버가 될 노드를 결정하고 클러스터를 재구성하는 것이다. 이동노드는 주어진 시간 슬롯에서 클러스터 헤드로부터 요청 메시지를 받지 못하면 Join 요청 메시지를 송신한다. 그런 후 특정 클러스터 헤드로부터 수신한 광고 메시지에 대한 Join 응답 메시지로써 현재 라운드에서 속하게 될 클러스터를 재결정하게 된다. 이로써 Steady-State Phase를 마치고 다음 라운드 단계인 Set-Up Phase가 반복된다.

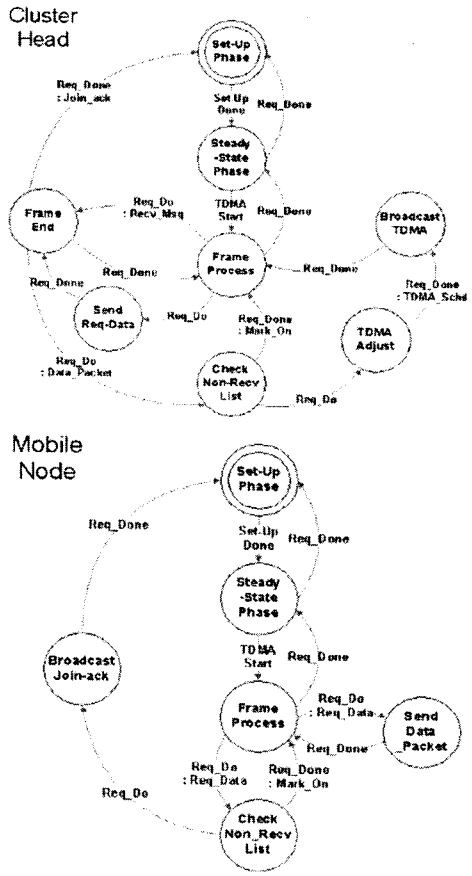

그림 1. LEACH_Mobile 프로토콜의 메시지 교환 과정

3.1.1 Set-Up Phase : 클러스터 구성

Set-Up Phase에서는 모든 노드가 확률함수를 사용하여 클러스터 헤드를 결정하고 클러스터 헤드가 이웃 노드에 광고 메시지를 Broadcast 하여 클러스터를 구성한다. 이때 매체 접근 제어(MAC) 프로토콜은 CSMA 방식을 사용한다. 광고 메시지를 수신한 비 헤드 노드들은 자신이 속할 클러스터의 헤드 노드를 선택하고 이를 헤드 노드에게 알린다. 여기서 모든 노드는 주어진 시간에 클러스터 헤드 노드로 데이터를 전송한다고 가정한다.

3.1.2 Steady-State Phase : 클러스터 헤드

클러스터가 구성된 후 클러스터 헤드는 TDMA 스케줄에 따른 데이터 수집을 위해 데이터 전송 요청 메시지를 각 시간 슬롯에서 비 클러스터 헤드 노드에 전송하고 요청을 받은 비 클러스터 헤드 노드는 데이터를 전송한다. 그리고 클러스터 헤드는 프레임이 끝날 때마다 수신된 데이터 리스트를 검사하여 데이터를 수신하지 못한 노드를 비 수신 노드 리스트에 추가하고 다음 프레임이 끝났을 때까지 데이터를 전송 받지 못하면 해당 노드를 클러스터 멤버에서 제거, 새로 참여하는 노드에 이 시간 슬롯을 할당하게 된다. 이후 새로 생성된 TDMA 스케줄을 모든 클러스터 멤버 노드에 전송한다. 이 방법은 데이터 요청 메시지에 응답하지 않는 노드는 이동하여 현재 클러스터 영역을 벗어났다고 가정한 것이다. TDMA 스케줄에 따른 시간 슬롯이 완료되면 수신한 데이터를 병합하여 클러스터 헤드 노드의 상위노드(수집 노드, 베이스 스테이션)로 데이터를 전송한다.

3.1.3 Steady-State Phase : 이동노드

클러스터가 구성된 후 이동노드는 TDMA 스케줄에 의해 할당된 시간 슬롯에서 데이터 요청 메시지를 기다리게 되며 에너지 소모를 최소화하기 위해 주어진 TDMA 스케줄에서 할당받은 시간까지 무선통신 라디오를 꺼놓을 수 있다. 만약, 프레임이 끝날 때까지 데이터 요청 메시지를 수신하지 못하면 프로토콜 수행 과정을 다음 프레임으로 진행시키게 되며 다음 프레임이 끝날 때까지 데이터 요청 메시지를 수신하지 못하면 클러스터 참여 요청 메시지를 Broadcast 한다. 참여 요청 메시지를 수신한 클러스터 헤드 노드는 Set-Up Phase와 같이 광고 메시지를 전송하고 이동노드는 수신된 광고 메시지의 수신 세기에 기반하여 현재 라운드에 속하게 될 클러스터를 결정하게 된다. 이동노드가 자신이 속할 클러스터를 결정하게 되면 해당 클러스터 헤드 노드에 클러스터 참여(Join-ack) 메시지를 전송함으로써 공지를 한다. 그리고 해당 클러스터 헤드 노드는 클러스터 멤버 리스트와 TDMA 스케줄을 갱신하여

클러스터에 속한 비 클러스터 헤드 노드들에게 TDMA 스케줄을 전송하여 새로 참여한 이동노드를 비롯한 모든 멤버 노드들은 다음 프레임부터 TDMA 스케줄을 갱신한다.

3.2 키 풀 사전 분배 방식을 이용한 클러스터 단위의 공용키 설정

본 논문에서는 센서노드에 키 풀을 사전 분배하여 클러스터 구성 시 클러스터 단위의 공용키를 설정하고자 한다. 분산된 센서 네트워크에서 센서노드들의 배치위치를 정확히 알 수 있다면 공용키를 설정할 노드들을 예측하여 키 분배를 쉽게 해결할 수 있다. 하지만 센서노드들의 이동이 수시로 일어나기 때문에 키 선 분배 방법은 키 설정 확률을 높이는 데 제한적이다. 따라서 본 논문에서는 이를 해결하기 위하여 메모리 소모량이 적은 키 풀을 센서노드들의 메모리에 미리 할당한다. 그리고 클러스터 헤드 노드가 해당 클러스터 내의 공용키를 키 풀에서 임의로 선택하고 비 클러스터 헤드 노드들에게 TDMA 스케줄과 함께 키의 인덱스를 전송하여 클러스터 구성 후의 공용키를 설정하도록 하였다. LEACH_Mobile 프로토콜의 클러스터 단위의 공용키 설정 동작과정은 다음과 같다.

표 1. 용어의 정의 및 표기

표기	설명
r	클러스터 실행 라운드
S	TDMA 스케줄
K_I	키 풀의 키 인덱스
A	클러스터 헤드의 광고 메시지
J	클러스터 참여 요청 메시지
E	encryption (암호화)
K_{set}	Set-Up Phase 공용키
K_{steady}	Steady-Stae Phase 공용키

• 센서노드 배치 전 : 모든 센서노드의 메모리에 키 풀을 할당한다.

• Set-Up Phase 단계 : 모든 센서노드는 해당 r에 따른 K_{set} 설정, $E(A, K_{set})$전송한다. 여기서 모든 센서노드는 시간 동기화되어 있다고 가정한다.

• Set-Up Phase 단계(클러스터 구성) : 클러스터 헤드는 사전 분배된 키 풀에서 랜덤함수를 통해 키 값을 선택, $E((S, K_I), K_{set})$ 메시지 전송한다.

• Steady-State Phase 단계 : 클러스터 헤드로부터 수신한 (S, K_I) 메시지에 따라 K_I를 이용하여 데이터 전송 시 보안을 위한 공용키 K_{steady}을 설정한다.

• Steady-State Phase 단계(이동노드) : 참여할 클러스터에서 참여요청 메시지 전송 시 해당 r의 K_{set}을 이용하여 $E(J, K_{set})$를 전송하고 클러스터 참여에 따른 S을 수신한 후 해당 클러스터 내에서 사용하는 K_{steady}를 공용키로 설정한다.

Ⅳ. 결 론

본 논문에서는 헬스케어 환경에서 노드의 이동성을 보장하며 노드 간 데이터 전송 시 보안을 강화한 LEACH_Mobile 프로토콜을 제안하였다. 제안 기법은 센서노드에 메모리 소모량이 적은 키 풀을 사전 분배하여 클러스터 단위 공용키 설정을 적용함으로써 데이터 전송 시 키가 외부로 유출되는 것을 차단하였으며 센서노드의 키 전송/수용 과정을 제거하기 때문에 키 관리 측면에서 기존 기법보다 효율적이다. 또한 노드 간 계층적 클러스터의 구성을 통한 자기구성과 에너지 효율성 그리고 빈번한 위치이동에 따른 이동성을 지원함으로써 헬스케어 환경에 보다 적합한 응용서비스를 지원할 수 있다.

향후 본 연구를 기반으로 헬스케어 환경에서 센서노드에 대한 이동성과 데이터 보안 측면에서의 성능분석을 통해 제안한 프로토콜의 효율성을 입증한다.

참고문헌

[1] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient Routing protocols for wireless microsensor networks," In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Vol. 2, pp. 908-918, 2000.

[2] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," Wireless Comm. IEEE, Vol. 1, No. 4, pp. 660-670, 2002.

[3] 김도성, 정영지, "모바일 센서 노드 지원을 위한 자기구성 라우팅 프로토콜," 한국정보처리학회 춘계 학술발표대회 논문집, 제13권, 제1호, pp. 1295-1298, 2006

[4] Seyit A. Camtepe and Bulent Yener, "Key distribution Mechanism for Wireless Sensor Networks: a Survey," TR-05-07, Department of Computer Science, Rensselaer Polytechnic Institute, 2005.

[5] 안동인, 신창선, 주수종, "헬스케어 홈 서비스를 위한 실내위치 기반의 상황정보 지원 시스템," 한국컴퓨터종합학술대회 논문집, 제33권, 제1호, pp. 64-66, 2006.