An Energy-Efficient Clustering Design Apply Security Method in Ubiquitous Sensor Networks

USN에서 보안을 적용한 에너지 효율적 클러스터링 설계

Do-Hyun Nam, Hong-ki Min
남 도 현, 민 홍 기

Abstract

The ubiquitous sensor network consists of micro sensors with wireless communication capabilities. Compared to wired communication, wireless communication is more subject to eavesdropping as well as data variation and manipulation. Accordingly, there must be efforts to secure the information delivered over the sensor network. Providing security to the sensor network, however, requires additional energy consumption, which is an important issue since energy transformation is difficult to implement in a sensor network. This paper proposes a routing mechanism based on the energy-efficient cluster that features security functions capable of safely processing the data acquired from the sensor network. The proposed algorithm reduces energy consumption by fixing the clusters formed at the initial stage and using the pre-distribution scheme so that the cluster and node keys generated and exchanged at the initial stage are not re-generated or re-exchanged. Simulation experiments confirmed that the proposed approach reduces energy consumption compared to implementing security measures to the conventional cluster-based routing mechanism.

요 약

유비쿼터스 센서 네트워크(Ubiquitous Sensor Network)는 무선통신 기능을 가진 소형 센서들로 구성된 네트워크이다. 무선통신은 유선통신에 비해 데이터의 도청과 위조, 변조가 용이하다. 그러므로 센서 네트워크를 통해 전달되는 정보들의 신뢰성을 위한 보안 연구가 수행되어야 한다. 하지만 센서네트워크에 보안을 적용하기 위해서는 추가되는 에너지소모가 발생한다. 에너지 교체가 어려운 센서네트워크에서 추가적인 에너지소모는 중요한 문제이다. 본 논문은 센서네트워크에서 획득한 데이터를 안전하게 처리할 수 있는 에너지 효율적 클러스터 기반 라우팅을 제안한다. 제안방식은 초기에 형성된 클러스터는 고정시키고 클러스터 헤드노드만 교체하는 방식으로 최초에 생성 및 교환된 클러스터 키와 노드간 키가 다시 생성 및 교환되지 않게 하는 사전배포방식을 사용할 수 있다. 제안된 방법이 기존의 클러스터 기반 라우팅에 보안을 적용한 것보다 에너지 소모가 29.2% 적게 소모됨을 모의실험을 통하여 확인하였다.

Key words : 무선센서네트워크, 클러스터, 라우팅, 보안

Ⅰ. 서 론

센서 네트워크는 무선통신을 기반으로 하고 있다[1]. 무선통신은 유선통신에 비해 데이터의 도청과 위조, 변조가 용이하다. 그러므로 센서 네트워크를 통해 전달되는 정보들의 신뢰성 있는 전달을 위한 보안 연구가 수행되어야 한다. 하지만 센서네트워크에 보안을 적용하기 위해 추가로 에너지소모가 발생한다. 에너지 교체가 어려운 센서네트워크에서 추가적인 에너지소모는 중요한 문제이다[2,3,4].

USN에서 대표적인 보안 프로토콜로는 SPINS (Security Protocol for Sensor Networks)와 LEAP (Localized Encryption and Authentication Protocol)가 있다[5,6].

SPINS는 유니캐스트(Unicast) 통신에서 암호와 인

이 논문은 인천대학교 2006년도 자체연구비 지원에 의하여 연구되었음.

증을 모두 지원하는 SNEP(Sensor Network Encryption Network), 브로드캐스트(Broadcast) 통신에서 인증을 지원하는 μTESLA(the "micro" version of the Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol)로 구성되어 있다. SPINS는 하나의 키를 모든 센서가 공유하기 때문에 키가 공격되면 전체 노드의 안전성이 위협당할 수 있다.

LEAP는 서로 다른 네 개의 그룹 키, 클러스터 키, 노드간 키, 개인 키를 가지고 센서네트워크를 구성하기 때문에 SPINS보다 키 공격에 있어서 전체 노드에 미치는 영향이 적다. LEAP에서 노드간 키의 교환은 랜덤함수와 노드의 id를 이용하여 이루어진다. 노드간 키의 교환은 네트워크 구성이 변할 때마다 실행되는 단점이 있다.

또한 USN에서 대표적인 라우팅 프로토콜로는 LEACH (Low Energy Adaptive Clustering Hierarchy)가 있다[1,2,3]. LEACH는 클러스터를 기반으로 하는 라우팅방식으로 에너지 소모가 적은 프로토콜이다.

본 논문은 센서네트워크에서 보안 방법을 에너지 소모가 적게 사용할 수 있는 클러스터 기반의 라우팅 방법을 제안한다. 제안방식은 초기에 형성된 클러스터를 고정시킴으로 최초에 생성 및 교환된 클러스터 키와 노드간 키가 다시 생성 및 교환되지 않게 하여 에너지 소모를 적게 하였다. 클러스터를 계속 고정함으로 인해 클러스터 헤드노드의 에너지 소모가 집중되는 문제는 클러스터 내에서 클러스터 헤드노드를 순차적으로 교환함으로서 해결한다. 제안된 방법이 기존의 클러스터 기반 라우팅에 보안을 적용한 것보다 에너지 소모가 적음을 모의실험을 통하여 확인하였다.

II. USN에서의 보안과 라우팅

2.1. USN에서의 보안

USN에서 보안서비스는 데이터의 암호화 방식을 이용하여 데이터의 비밀성과 인증을 제공한다. 암호화 방식은 암호화 키와 복호화 키가 같은 대칭키 방식과 암호화 키와 복호화 키가 다른 비대칭키 방식이 있다. 비대칭키 방식은 에너지 소모가 커서 센서네트워크 환경에서는 적합하지 않다. USN에서 보안 적용은 에너지 소모가 큰 비대칭키 방식은 사용할 수 없고, 대칭키 방식을 사용한다. 하지만 일반적으로 대칭키 방식은 키의 교환과 관리에 대한 문제를 가지고 있다.

키의 교환은 최초에 배포하는 사전배포 방식과 네트워크 구성 후에 배포하는 사후배포 방식으로 구분된다. 사전배포방식은 에너지 소모측면에서 효율적이나 저장 공간이 부족한 센서노드가 모든 키를 가지고 있을 수 없는 제약사항이 있다. 연결될 확률이 높게 일정량의 키 집합을 가지는 방식도 있으나 센서노드간 연결성이 떨어진다. 그러므로 클러스터 기반 방식에서는 사용이 현실적이지 못하다. 사후배포방식은 네트워크가 구성된 이후에 신뢰하는 BS(Base Station)를 이용하여 센서노드간에 키를 교환하는 방법과 각 센서노드가 랜덤함수를 이용하여 세션키를 생성하여 사용하는 방법이 있다. BS를 이용한 방법은 먼 거리의 BS와 통신으로 추가되는 에너지 소모가 크고, 함수를 이용한 방식은 알고리즘이 다소 복잡한 단점이 있다.

USN에서 대표적인 암호화 프로토콜로는 SPINS가 있고, 키 교환 프로토콜로는 LEAP가 있다. SPINS는 SNEP와 μTESLA 두개의 모듈로 구성되어 있다.

SNEP는 대칭키 방식을 사용하여 데이터의 비밀성을 유니캐스트 통신환경과 브로드캐스트 통신환경에서 지원하고, 데이터의 인증은 비대칭키 방식을 사용하지 않고 MAC(Message Authentication Code)과 대칭키를 사용하여 유니캐스트 통신 환경에서 지원한다. SNEP의 데이터 인증은 브로드캐스트 통신환경에서는 지원하지 않는다. 브로드캐스트 통신환경에서의 인증은 별도의 μTESLA라는 프로토콜을 통해 제공한다. (그림 1)은 초기 카운터 값(C)를 동기화하는 방법이고 식 1은 SNEP의 암호화 및 인증 방법을 표현하고 있다. 최초에 모든 노드는 마스터 키(k)를 가지고 있고 노드간에 암호화 통신을 위해서 카운터 값 C를 공유하고 있다. C는 가장 최신의 데이터임을 확인하는 방법으로 사용된다. C는 데이터를 전송 후 자동으로 증가된다. 모든 노드는 k와 랜덤함수를 이용하여 암호키(ek)와 MAC키(mk)를 생성한다. E는 암호문을 말하고 D는 데이터를 말한다.

SPINS는 하나의 키를 모든 센서가 공유하기 때문에 키가 공격되면 전체 노드의 안전성이 위협당할 수 있는 문제가 있다.

1) $A \rightarrow B: C_A$
2) $B \rightarrow A: C_B, MAC(k_{AB}, C_A \mid C_B)$
3) $A \rightarrow B: MAC(k_{AB}, C_A \mid C_B)$

Fig. 1. Counter change protocol
그림 1. 카운터(C)의 동기화 방식

$$A \rightarrow B : D_{(ek, C)}, MAC(mk, C \mid D_{(ek, C)}) \quad (1)$$

LEAP는 모든 노드가 사용하는 그룹 키와 노드와 노드 간에 사용하는 노드간 키, 그리고 클러스터 내에서 사용하는 클러스터 키와 BS와 각 노드 간에 사용하는 개인 키로 구성되어 있다. LEAP는 이와 같이 서로 다른 네 개의 키를 가지고 센서네트워크에서 사용하기 때문에 SPINS보다 키 공격에 있어서 전체 노드에 미치는 영향이 적다. LEAP의 키 교환 방식은 이웃노드를 찾아 서로 id를 교환하고 자신이 가지고 있는 랜덤함수와 이웃노드의 id를 이용하여 노드간 키를 생성한다. 일정 시간 이후에 노드간 키는 다시 생성하여 사용한다. 이처럼 네트워크 구성의 변화에 따라 노드간 키와 클러스터 키의 생성 및 교환에 에너지 소모가 많이 발생하는 단점이 있다.

2.2. 클러스터 기반 라우팅과 에너지 소모량

USN에서 라우팅은 에너지소모가 적은 계층적 방식 즉, 클러스터 방식이 주로 사용되고 대표적인 프로토콜로는 LEACH가 있다[1,2,3,4]. 클러스터 방식은 전체 그룹(GN) 내의 센서노드를 여러 개의 클러스터로 묶어 하나의 클러스터 내에는 하나의 클러스터 헤드 노드(CH)가 있고, 나머지는 클러스터 멤버노드(CM)로 구성된다. CM은 오직 CH에게만 데이터를 전송하고 CH는 CM에게 받은 데이터를 취합하여 BS에게 전송한다. 클러스터 방식은 CH의 에너지 소모가 크므로 주기적으로 CH를 교체하여 주어야 한다[8].

(그림 2)에서와 같이 LEACH방식은 다수의 라운드(round)라는 구간으로 구성되어 있고, 라운드는 셋업(set-up)과 다수의 프레임(frame)으로 구성되어 있다. 또한 프레임은 다수의 슬랏(slot)으로 구성된다.

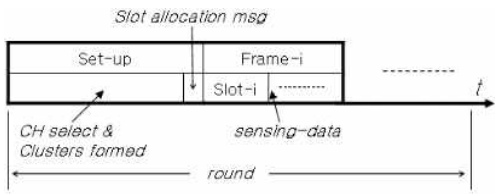

Fig. 2. Timelife of LEACH protocol
그림 2. LEACH의 생명주기

셋업과정은 CH 선정 및 CH에 최적화된 CM을 선정하는 과정이고, 프레임과정은 각 슬랏에 해당하는 CM이 획득한 데이터를 CH에게 전송하고, CH는 이를 취합하여 BS에 전송하는 과정이다. (그림 3)은 LEACH방식의 알고리즘을 표현한 것이다.

```
//---- setup state ----------
1) CH -> *GN: ADV 전송
2) CM -> CH: Join-REQ 응답
3) CH -> *CM: TDMA 전송
//---- frame state ----------
1) CM -> CH: sense data 전송
2) CH -> BS: aggregation data 전송
```

Fig. 3. LEACH Algorithm
그림 3. LEACH 알고리즘

CH는 확률값에 의해 랜덤하게 선출되고 그룹의 노드(GN)에게 ADV(Advertisement)메시지를 전송한다. CM은 ADV를 수신하여 가장 수신강도가 큰 CH를 자신의 CH로 정하고 Join-REQ메시지로 응답한다. CH는 자신의 CM들의 정보를 수신하여 TDMA(Time Division Multiple Access)정보를 생성하고 각 CM들에게 전송한다. CM들은 자신의 시간이 되면 CH에게 센싱 데이터를 전달하고, CH는 이를 취합하여 BS에게 전송한다. 셋업에서의 전체 에너지 소모량은 송신 경우 식 2를 이용하고 수신경우 식 3을 이용하여 식 4로 표현할 수 있다. 식 2의 송신 경우 센서노드가 기지국 또는 센서필드의 모든 노드들에게 전송하는 먼거리 전송(tx_{long})과 클러스터내의 노드들에게만 전송하는 짧은거리 전송(tx_{short})으로 구분된다[7].

$$E_{tx}(l,d) = \begin{cases} lE_{elec} + lE_{mp}d^4 & : tx_{long} \\ lE_{elec} + lE_{fs}d^2 & : tx_{short} \end{cases} \quad (2)$$

$$E_{rx}(l) = lE_{elec} \quad (3)$$

$$E_{l-setup} = l_m(kE_{mp}d^4 + E_{elec}(2N + kN - k^2 - k) + E_s\frac{M^2}{2\pi k}(\frac{N}{k} - 1)) + l(E_{elec}(k + N - 1) + E_{fs}\frac{M^2}{2\pi}) \quad (4)$$

여기서 l은 원 데이터 크기, l_m은 신호데이터의 크기, E_{elec}은 전자에너지 (electronics energy), E_{mp}는 먼거리 송신을 위한 증폭에너지(amplifier energy - multipath model), d는 기지국까지의 거리를 말한다. E_{fs}는 짧은거리 송신을 위한 증폭에너지(amplifier energy - free space model), k는 클러스터의 수, M은 M × M 지역의 한 변의 길이, N는 전체 노드 수이다.

Ⅲ. 보안을 적용한 에너지 효율적 클러스터링

USN의 라우팅 방식 중 에너지 소모가 적은 클러스터 기반 라우팅 방식을 사용하였다. 또한 보안은 하나의 키가 노출되어도 안전성에 영향이 적게 하기 위해 키는 여러 개를 사용하였다.

클러스터 방식은 클러스터 내의 노드들의 에너지소모를 균등하게 하기 위해 클러스터를 라운드마다 재구성하기 때문에 클러스터 키와 노드간 키 그리고 노드간에 공유하고 있는 C값이 변화되어 이에 대해 재생성 및 교환이 일어나는 문제점이 있다.

본 연구는 클러스터 라우팅 방식에서 라운드가 반복되어도 클러스터를 고정시켜 키의 재생성 및 교환이 이루어 지지 않는 방법을 제안하여 에너지 소모를 최소화한 보안 라우팅 방법을 제안한다.

3.1. 클러스터 환경에서의 키 셋업

클러스터 기반의 라우팅은 (그림 4)에서 보는 것처럼 브로드캐스트 통신과 유니캐스트 통신이 모두 사용되고 있다. 브로드캐스트 통신은 CH가 그룹노드(GN)에게 전송하는 경우와 CH가 CM에게 전송하는 경우가 있다. 이때 CH와 GN간에는 그룹 키(*gk*)가 사용되고 CH와 CM간에는 클러스터 키(*ck*)가 사용된다. 유니캐스트 통신의 경우는 CM이 CH에게 전송하는 경우와 CH가 BS에게 전송하는 경우가 있다. 이때 CM과 CH간에는 노드간 키(*pk*)가 사용되고 CH와 BS간에는 개인 키(*ik*)가 사용된다.

모든 노드 i는 초기에 마스터 키(*k*)를 BS로부터 받는다. 모든 노드는 랜덤키 생성함수인 식 5를 이용하여 식 6에서처럼 마스터 키(*k*)를 사용하여 개인 키(*ik*)와 MAC키(*mk*)를 생성한다. BS도 식 5를 이용하여 모든 키의 개인 키를 생성하여 가지고 있는다.

$$K_{NodeID} = f_k(NodeID) \tag{5}$$

$$ik_i = f_k(i), \quad mk_i = f_{ik}(i) \tag{6}$$

노드 i와 노드 j의 노드간 키는 *ik*와 노드 *id*를 이용하여 생성하고, 클러스터 노드들의 클러스터 키는 랜덤 값 r을 생성 후 식 8을 이용하여 생성할 수 있다. 그러므로 노드간 키는 식 7로 표현되고, 클러스터 키는 식 8로 표현된다.

$$pk_{ij} = f_{ik_j}(i) \tag{7}$$

$$ck_i = f_{ik_i}(r) \tag{8}$$

*ik*와 *mk*는 최초에 생성할 수 있지만 *pk*와 *ck*는 클러스터 구성 후에 생성 및 공유가 가능하다. 제안 방식은 모든 노드가 공유하는 그룹 키(*gk*)는 위험성이 커서 사용하지 않는다.

3.2. LEACH에서 보안 키 교환 방법

```
//---- setup state ----------
LOOP
1) CH→* : id_ch, N_ch, MAC(mk, id_ch|N_ch)
2) CM→BS: N_req, id_ch, N_ch, (mk, id_ch|N_ch|N_req)_ik_cm
3) BS→CM: res, MAC(mk, N_req|res)
4) CM→CH: id_cm, C, MAC(mk, N_ch|id_cm|C)
//--Sharing key: Counter, ck, pk -----
5)   CH→BS: CInfo, C_g, MAC(mk, CInfo|C_g)
6)   BS→GN: (C, ck, pk)_ik, MAC(mk, (C,ck,pk)_ik)
7) CH→CM: TDMA_(pk,c), MAC(mk, C| TDMA_(pk,c))
//---- frame state ----------
     LOOP
8)     CM→CH: D_(pk,c), MAC(mk, C|D_(pk,c))
9)     CH→BS: D_(ik,c), MAC(mk, C|D_(ik,c))
     END LOOP
END LOOP
```

Fig. 4. LEACH protocol apply security method
그림 4. 보안을 적용한 LEACH 프로토콜

(그림 4)는 대표적인 클러스터 방식인 LEACH에 SNEP보안과 LEAP보안을 적용한 알고리즘 이다.

Setup State:

셋업상태는 라인 1에서 모든 노드가 확률함수를 이용하여 랜덤하게 CH를 선정하고 BS를 포함한 모든 노드에게 자신의 id와 랜덤값을 MAC값과 함께 전달한다. 이때 BS와 전체그룹노드(GN)만이 알고 있는 mac키가 MAC에서 사용된다. CH의 모든 정보를 수신한 CM은 수신강도가 가장 큰 CH를 선정하여 클러스터를 구성한다. CM은 수신한 정보의 신뢰를 위해 라인 2처럼 BS에게 수신한 정보와 랜덤값 그리고 MAC값과 함께 다시 보낸다. 이때 CM과 BS간의 통신도 MAC키가 포함된 MAC함수가 사용된다. 라인 3은 BS가 CM에게 요청받은 정보의 결과를 전달하는 과정으로 요청한 랜덤값과 결과값을 MAC함수로 연산하여 전달한다. CM은 이를 수신하여 확인하고 라

인 4 처럼 자신의 CH로 선정된 센서노드에게 자신의 id와 카운터 값을 전달한다. 이때 CM은 처음 수신한 값, 자신의 id, 카운터 값, MAC값을 함께 전달하여 CH가 확인할 수 있게 한다.

Sharing Key:

라인 5는 CH가 BS에게 자신이 수집한 클러스터의 모든 센서노드의 id와 카운터 값의 집합을 전달한다. 이때 CH와 BS간의 통신은 MAC키가 포함된 MAC정보가 사용된다. 모든 정보를 수신한 BS는 클러스터 키를 생성하고 클러스터 내의 모든 센서노드의 카운터 값 C와 노드간 키를 생성하여 라인 6처럼 모든 노드에게 전달한다. 이때에는 데이터의 암호를 위해 개인 키가 사용된다. 이후 CH는 CM에게 TDMA 스케쥴정보를 생성하여 라인 7처럼 개인 키로 암호화 하여 전송한다.

Frame State:

다음으로 프레임상태는 라인 8에서는 클러스터 내의 CM들이 TDMA방식으로 자신의 데이터 송신 슬랏에 해당될 때 실제 데이터를 센싱하고 CH에게 암호화하여 전송하는 부분이다. 이때 CM과 CH사이에 노드간 키가 사용된다. 라인 9에서처럼 클러스터 내의 CM들에게 데이터를 수신한 CH는 데이터를 취합하여 BS에게 암호화하여 전송한다. CH와 BS사이는 개인 키가 사용된다. 라인 8과 라인 9는 일정시간 반복적으로 일어난다.

3.3. 제안 클러스터링 방식과 보안 키 교환 방법

제안방식의 키 교환방식은 (그림 5)에서 보는 것처럼 라인 1에서 라인 9까지의 셋업과정과 키교환과정 그리고 프레임 과정이 (그림 4)의 LEACH방식에 보안을 적용한 것과 동일하다. 하지만 제안방법은 라인 1에서 라인 7까지의 내용이 최초에만 한번 일어나고 반복되지 않는다[9,10]. CH의 에너지 소모가 커지면 라인 10과 라인 11의 재셋업이 일어난다. 재셋업은 초기에 구성된 클러스터 형태는 고정된 상태에서 CH만 교체가 일어나서 클러스터내의 에너지소모 균등화를 이룬다. 클러스터가 지속적으로 유지되기 때문에 클러스터 내에서 사용하는 클러스터 키는 재생성 및 교환이 필요하지 않다. 또한 효율적인 클러스터 수는 5%이므로 클러스터 내의 노드 수는 20개 정도가 된다. 그러므로 CH와 CM간의 노드간 키도 최초셋업에서 모두 생성하여 각 노드가 모두 보유하고 있을 수 있다[3,4].

```
//---- initial setup state ----------
1) CH→* : id_ch, N_ch, MAC(mk, id_ch|N_ch)
2) CM→BS: N_req, id_ch, N_ch, (mk, id_ch|N_ch|N_req)_ik_cm
3) BS→CM: res, MAC(mk, N_req|res)
4) CM→CH: id_cm, C, MAC(mk, N_ch|id_cm|C)
//--Sharing Key: Counter, ck, pk -----
5)  CH→BS: CInfo, C_g, MAC(mk, CInfo|C_g)
6)  BS→GN: (C, ck, pk)_ik, MAC(mk, (C,ck,pk)_ik)
7) CH→CM: TDMA_(pk, c), MAC(mk, C| TDMA_(pk, c)
LOOP
//---- frame state ----------
    Repeat
8)    CM→CH: D_(pk, c), MAC(mk, C|D_(pk, c))
9)    CH→BS: D_(ik, c), MAC(mk, C|D_(ik, c))
    Until slot_cnt;
//---- re-setup state ----------
10) CH→CM:
        TDMA_(ck, c), MAC(mk, C| TDMA_(ck, c))
END LOOP
```

Fig. 5. Proposed protocol
그림 5. 제안방식 프로토콜

라인 10의 재셋업 상태는 CH가 현재 CH id의 다음 id가 되는 센서노드를 CH로 선정한 후, 새로운 TDMA정보를 생성하고 CM에게 암호화 하여 전송하는 과정이다.

제안된 보안 클러스터 라우팅 방식에서 키의 생성과 교환은 초기셋업에서 다 이루어진다. 개인 키와 MAC키의 경우는 센서노드를 초기에 배포할 때 설정된 마스터 키로 스스로 생성되기 때문에 교체가 필요없고, 클러스터 키와 노드간 키는 초기셋업 과정에서 생성되어 배포된다. 일반적인 클러스터 방식이 셋업에서 CH와 클러스터정보가 변하기 때문에 클러스터 키와 노드간 키 그리고 암호화시 사용되는 카운터 값은 다시 생성 및 교환이 필요하다. 그러나 제안된 방식은 초기셋업 이후에 반복되는 재셋업에서 클러스터가 변화하지 않기 때문에 클러스터 키의 생성과 교환은 필요가 없다. 셋업에서 CH의 변화는 일어나기 때문에 노드간 키의 생성과 교환은 필요하다. 하지만 제안방식은 초기에 생성된 클러스터 내의 센서노드 수가 많지 않기 때문에, 모두 생성하여 각 센서노드가 저장하고 있기가 가능하다. 이것은 클러스터 방식은 5%의 클러스터 수가 효율적이기 때문에 각 클러스터의 노드 수 는 20개 내외이고 클러스터 정보가

변화되지 않기 때문이다[3,4].

3.4. 보안 키 교환에 따른 에너지 소모량 비교

제안방식의 키 교환 에너지 소모량은 식 2와 식 3 그리고 (그림 5)를 이용하여 구할 수 있다. 초기셋업에서 송신과 수신의 횟수는 식 9로 표현되고, 에너지 소모량은 식 10으로 표현된다. 재셋업에서 송신과 수신의 횟수는 식 11로 표현되고, 에너지 소모량은 식 12로 표현된다. BS는 에너지를 충분히 가지고 있기 때문에 BS에서의 송신과 수신은 에너지 소모를 계산하지 않는다.

$$C_{p-initsetup} = 2k(tx_{long}) + (N-k)tx_{short} + 2(N-k)rx + (N-k)tx_{long} + (N-k)tx_{short} + (k(N-k)+3(N-k))rx \quad (9)$$

$$E_{p-initsetup} = lE_{elec}(8N + kN - 6k - k^2) + lE_{mp}d^4(k+N) + 2lE_{fs}\frac{M^2}{\pi k}(N-k) \quad (10)$$

$$C_{p-resetup} = 2tx_{short} + 2(\frac{N}{k} - 1)rx \quad (11)$$

$$E_{p-resetup} = lE_{elec}(3+N-k) + lE_{fs}\frac{M}{\pi k^2} \quad (12)$$

제안방식은 초기셋업은 최초의 라운드에서 한번만 일어나고 이후의 라운드에서는 재셋업만 반복적으로 일어난다. 하지만 기존의 클러스터 방식은 초기셋업이 계속 반복적으로 일어나고, 이에 따른 많은 키의 교환이 발생되므로 에너지 소모가 크다.

실제 데이터 전송을 하는 프레임에서의 에너지 소모량은 키 교환을 위한 별도의 전송이 없기 때문에 클러스터 기반 라우팅은 모두 식 13으로 동일하다.

$$E_{frame} = lE_{elec}(N-k) + (lE_{elec} + lE_{mp}d^4)k + (lE_{elec} + lE_{fs}\frac{M^2}{2\pi k})(N-k) \quad (13)$$

Ⅳ. 실험 및 고찰

제안된 방식의 타당성을 확인하기 위해 Visual C++ 6.0 프로그램을 사용해 LEACH방식에 보안을 적용한 것과 비교하여 모의실험을 하였다. 이때 실험 환경은 E_{elec}는 50 nJ/bit, E_{fs}는 10 $pJ/bit/m^2$, E_{mp}는 0.0015 $pJ/bit/m^4$, l은 512 bit, l_m은 64bit, k는 5개, N은 100개, M은 100m, 초기에너지는 0.2J로 적용하였다. (그림 6)은 5개의 클러스터가 형성된 화면이다. 기지국은 센서노드의 밖에 위치하고 있다.

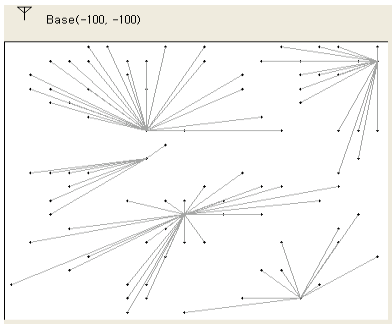

Fig. 6. Simulation of proposed method
그림 6. 노드 배치 및 클러스터링 시뮬레이션

4.1. LEACH방식과 제안방식의 에너지소모량 비교

LEACH방식에 보안을 적용한 방식인 LEACH-sec 방식과 제안 클러스터링 방식에 보안을 적용한 방식인 RRCH-sec방식과의 에너지 소모량을 비교하여 보았다. 먼저 네트워크 수명은 <표 1>과 (그림7)로 표현된다.

Table 1. Number of node still alive per round
표 1. 라운드별 네트워크 수명

round	LEACH-sec	RRCH-sec
20	100	100
40	100	100
60	100	100
80	100	100
100	98	100
120	95	100
140	86	100
160	60	99

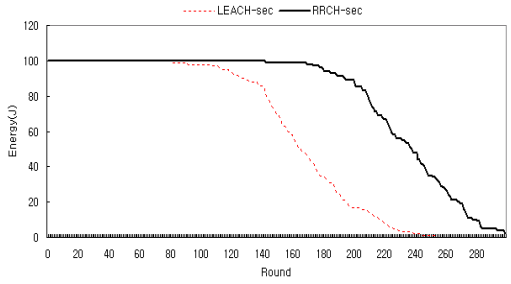

Fig. 7. Number of node still alive per round
그림 7. 라운드별 네트워크 수명

(그림 7)에서 보듯이 LEACH방식에 보안을 적용하게 되면 네트워크 수명이 급격하게 줄어드는 반면에 제안 클러스터링 방식에 보안을 적용한 것은 네트워크 수명에 큰 변화를 가져오지 않는 것을 확인할 수 있다. 이것은 LEACH에 보안을 적용시킬 경우 매번 셋업마다 키 교환 과정이 있으므로 에너지 소모가 큰 것이다. 반면에 제안방법은 초기에 키 교환이 모두 일어나므로 라운드를 반복한다고 해서 급격하게 에너지 소모가 증가하지 않는다.

<표 2>는 각 방식별로 전체에너지 소모량을 표현한 것이다. (그림 8)은 보안을 적용한 경우를 포함한 LEACH방식과 RRCH방식을 표현한 것이다. LEACH 방식에 보안을 적용한 것보다 RRCH방식에 보안을 적용한 것이 에너지 소모량의 변화가 작음을 확인할 수 있다.

Table 2. Total energy consume per round
표 2. 라운드별 전체에너지 소모량

Round	LEACH-SEC	RRCH-sec	Reduction(%) vs LEACH
10	0.1290	0.0920	28.7
20	0.2477	0.1737	29.9
30	0.3626	0.2579	28.9
40	0.4832	0.3449	28.6
50	0.6058	0.4268	29.5
60	0.7247	0.5146	29.0
70	0.8439	0.5964	29.3
80	0.9698	0.6821	29.7
90	1.0919	0.7702	29.5
100	1.2025	0.8493	29.4
		Average	29.2

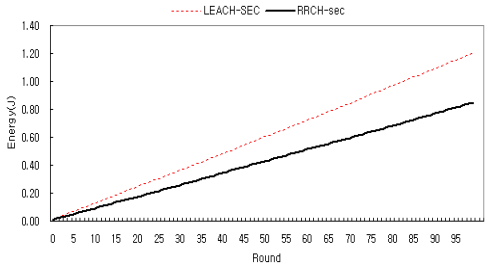

Fig. 8. Total energy consume per round
그림 8. 라운드별 전체에너지 소모량

4.2. 고찰

지금까지 본 논문에서 제안한 방식의 타당성을 확인하기 위하여 LEACH방식에 보안을 적용한 것과 제안 클러스터링 방식에 보안을 적용한 것의 에너지 소모를 모의실험을 통하여 비교하여 보았다.

본 연구는 기존의 LEACH방식에 보안을 적용한 것보다 제안 클러스터링 방식에 보안을 적용한 것의 전체 에너지 소모가 라운드 100번에 대해 29.2% 적게 소모됨을 확인하였다.

LEACH방식은 클러스터의 구성이 반복적으로 일어나기 때문에 라운드마다 셋업에서의 에너지 소모가 크다. 또한 보안을 위하여 변화되는 클러스터 키와 노드간의 키를 재생성하고 교환하기 때문에 추가적인 에너지 소모가 많이 생기게 된다. 반면 제안 클러스터링 방식은 최초의 셋업 이후의 재셋업은 클러스터를 유지한 상태에서 클러스터 헤드의 교체만 이루어지기 때문에 셋업이 간단하고 반복적인 키의 생성과 교환도 일어나지 않음으로 에너지 소모가 적음을 확인하였다.

V. 결 론

본 논문은 센서네트워크에서 획득한 데이터를 안전하게 처리할 수 있는 보안 메커니즘을 적용한 클러스터 기반 라우팅 방식을 제안하였다. 기존의 클러스터 기반 라우팅 방식이 주기적으로 클러스터 헤드와 클러스터가 변경되어 그에 따른 클러스터 키와 노드간 키 그리고 카운터 값이 재생성 되고 배포되는 문제가 있다. 제안방식은 한번 형성된 클러스터는 고정된 상태에서 클러스터 헤드의 교체만 이루어지게 하므로 반복적인 키의 생성과 공유가 일어나지 않게 하는 방식이다. 제안방식은 센서네트워크에서 보안을 적용한

에너지 효율적 클러스터링 방법으로 기존의 클러스터 기반 라우팅에 보안을 적용한 것보다 에너지 소모가 라운드 100번에 대해 29.2% 적음을 모의실험을 통하여 확인하였다.

본 논문은 초기의 클러스터링이 계속 유지되므로 초기 클러스터링이 중요하다. 그러므로 향후 효율적인 초기 클러스터 방식에 대한 연구가 필요하다.

참고문헌

[1] C.Intanagonwiwat, R.Govindan, and D.Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks" in *Proceedings of the ACM/IEEE international Conference on Mobile Computing and Networking* (MOBICOM), 2000

[2] Wendi B.Heinzelman, Anantha P.Chandrakasan, and hari Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks" in *Proceedings of the Hawaii International Conference on System Sciences, Jan. 2000*

[3] Wendi B.Heinzelman, Anantha P.Chandrakasan, and hari Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks" *IEEE Transactions on Wireless Communications, Vol. 1, NO. 4, 2002*

[4] A.Manjeshwar and D.P.Agrawal. "TEEN: A Routing Protocol for enhanced Efficiency in Wireless Sensor Networks". in *1st International Workshop on Paralled and Distributed Computing Issues in Wireless, 2001.*

[5] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *In Proceedings. of the 10th ACM CCS '03*, October 2003

[6] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, "SPINS: Security Protocols for Sensor Networks," *In Proceeding of Seventh Annual ACM International conference on Mobile Computing and Networks(Mobicom)*, July 2003

[7] W. Ye, J. Heidenmann, and D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks", in Proceedings of IEEE INFOCOM, New York, NY, June 2002.

[8] S. Bandyopadhyay, et. al., "An Energy-Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks", in IEEE INFOCOM 2003.

[9] Do-Hyun Nam, Hong-Ki Min. "An Efficient Ad-Hoc Routing Using a Hybrid Clustering Method in a Wireless Sensor Network" in IEEE WiMob 2007

[10] 남도현, 민홍기. "센서 네트워크에서 클러스터 헤드의 load-balancing을 통한 에너지 효율적인 클러스터링" 정보처리학회논문지C 제3,. 2007.6

저 자 소 개

남 도 현 (정회원)

2000년 : 인천대학교 전자계산과 졸업 (공학사)
2004년 : 중앙대학교 정보대학원 (공학석사)
2008년 : 인천대학교 대학원 정보통신과 (공학박사)
1996년 ~ 2004년 : 인크루트 연구소장
2003년 ~ 현재: 클립소프트 연구소장
2003년 ~ 현재 : 인하공업전문대학 겸임교수
<주관심분야>
센서네트워크, 보안, 디자인패턴

민 홍 기 (정회원)

1979년 : 인하대학교 전자공학과 졸업 (공학사)
1981년 : 인하대학교 대학원 전자공학과 (공학석사)
1985년 : 인하대학교 대학원 전자공학과 (공학박사)
1985년 ~ 1991년 : 한국과학기술연구원 선임연구원
1993년 ~ 1994년 : Univ. of Delaware 방문교수
1991년 ~ 현재 : 인천대학교 교수
<주관심분야>
센서네트워크, 신호처리, 재활공학, HCI