WSN 환경에서 안전한 데이터 전달을 위한 IDE 기반의 계층적 노드인증 프로토콜

정회원 조 영 복*, 종신회원 이 상 호**

An IDE based Hierarchical Node Authentication Protocol for Secure Data Transmission in WSN Environment

Young-bok Cho* *Regular Member*, Sang-ho Lee** *Lifelong Member*

요 약

WSN 환경의 센서노드는 정보를 수집하고 베이스스테이션으로 전달한다. 베이스스테이션은 인증되지 않은 노드로부터 전달받은 데이터를 신뢰하기 어렵다. 따라서 다양한 방법으로 노드를 인증하고, 데이터의 안전성을 판단하는 방식들이 연구되고 있다. 기존 AM-E[12] 방식에서는 노드인증 후에 데이터를 전달한다. 이때 센서노드는 베이스 스테이션과 직접 AREQ/AREP 메시지를 통신하는 과정에서 인증메시지 송수신으로 인해 많은 에너지를 소비하게 된다. 또한 모든 노드는 인증을 위해 베이스스테이션과 직접 통신과정을 거치며 한정된 에너지를 과다하게 소비하는 문제점을 갖는다. 따라서 이 논문에서는 AM-E 방식과 동일한 보안성을 제공하면서 센서노드의 에너지소비를 최소화할 수 있는 IDE 기반의 계층적 노드인증 프로토콜을 제안한다. 제안방법은 안전성 측면에서는 기존 방식과 같이 메시지 재전송공격이나 메시지의 무결성 보장을 유지하면서 통신에 참여하는 노드수가 AM-E 방식보다 약 39% 증가되어 전체 네트워크 생명주기를 연장함으로 에너지 효율성을 증가시켰다.

Key Words : 무선센서네트워크, 인증, 계층적 구조, IDE, Energy Efficiency

ABSTRACT

In WSN environment, the sensor nodes collect sensed data, and transmit data to the BS. BS is difficult to trust the data from unauthenticated nodes. Therefore, many papers have been proposed about the node authentication and the safety of data. In the AM-E paper, data is delivered after node authentication. In this time, the sensor nodes are directly communicated to BS the AREQ/AREP message for authentication. Therefore, the sensor nodes consume more energy for authentication. Also, noes communicate directly with the BS for authentication will have problem due to the limited energy of nodes. In this paper, the same security with AM-E is supported, Furthermore, to minimize the energy consumption, IDE based hierarchical node authentication protocol is proposed. Compared with AM-E, the number of alive nodes is increased about 39%. Thus, the entire network life time is extended and energy efficiency is improved.

Ⅰ. 서 론

무선 센서 네트워크(Wireless Sensor Networks : WSN)는 실시간 트래픽 모니터링이나 군사적 자료 수집, 지진 활동의 분산 측정, 시간 오염측정 등 넓은 분야에서 적용될 수 있다. WSN는 초소형 센서들로 구성되기 때문에 저장 메모리, 연산량, 에너지 통신 반경 등 제약이 따른다[1,2,5,9]. 센서들은 적대적

* 충북대학교 컴퓨터과학과 네트워크 보안연구실 (bogicho@cbnu.ac.kr), ** 충북대학교 소프트웨어학과 (shlee@cbnu.ac.kr)
논문번호 : KICS2011-10-485, 접수일자 : 2011년 10월 20일, 최종논문접수일자 : 2012년 3월 18일

환경에 노출될 수 있고 무선통신을 쉽게 도청할 수 있으며, 악의적인 공격자가 메시지를 변조하거나 재전송 공격을 시도할 수도 있기 때문에 안전한 무선통신을 제공하는 것은 매우 중요한 이슈이다. 안전한 WSN의 통신을 위해 다양한 측면에서 연구가 진행되고 있다. WSN는 센서노드(Sensor Node : SN)의 하드웨어적인 제약 및 무선 네트워크 특성에 따른 노드 탈취 및 손상, 감청, 서비스 거부 공격 및 싱크홀, 웜홀등 라우팅 공격에 매우 취약하다. 센서노드의 제약적인 특성으로 인해 기존 WSN의 보안 기법 적용이 쉽지 않다. 따라서 메시지 무결성, 기밀성 및 노드 인증 등의 보안요소 구현을 위해 경량화된 키 분배 및 인증기법 연구가 진행되고 있다. 센서노드에 적합하도록 기존 연산양이 많은 공개키 기반을 경량화하여 적용한 방식[2,11]과 낮은 컴퓨팅 능력과 안전한 키 분배를 고려해 설계된 SPINs의 μ-TESLA[4]와 LEAP[6]등이 있다. PIKE[7]는 대칭키 기반으로 대칭키 노출에 따른 네트워크 안전성 보장을 위한 사전키 분배방식들이 제안되었다[6]. 또한 키 분배가 필요 없으며 메시지 전송 횟수 등에서 장점을 지닌 ID기반 기법들도 연구되고 있다[11,12]. WSN은 무선통신의 특성으로 메시지의 도청이 용이하다는 단점을 가지고 있다. 따라서 이를 방지하기 위해 주고받는 데이터를 암호화하여 사용함으로 기밀성을 보장하는 방안들이 필요하다[12]. 참고문헌[12]의 AM-E는 인증키 생성시 센서노드의 아이디와 잔여 에너지 값을 이용한다. 인증키 생성을 위해 모든 SN은 베이스스테이션(Base Station : BS)과 직접통신을 수행하게 되는데 SN과 BS의 직접통신을 시도하는 것은 현실적으로 매우 어려운 일이다. 한정된 에너지를 소지한 노드가 멀리 위치한 BS와 직접통신을 시도한다면 인증메시지 송수신만으로 에너지 소비가 증가하고, 이렇게 에너지 소모가 많은 노드는 통신에 오래 참여할 수 없게 되는 문제점을 갖는다. 따라서 이 논문에서는 WSN 환경에서 안전한 데이터 전달을 위한 IDE(Identification Encryption) 기반의 계층적 노드 인증 프로토콜을 제안한다. 제안논문에서는 안전한 데이터 전달을 위해 통신에 참여하기 전 모든 SN는 인증절차를 거치고 인증된 노드만 통신에 참여할 수 있다. 이때 인증을 위해 SN의 에너지 소비는 최소화하기위해 참고문헌[12]에서 인증키 생성을 위해 SN와 BS가 직접 통신하는 방식을 제안논문에서는 계층구조로 노드를 논리적 분할하고 각 SN는 CH에게 그룹 키를 생성 받고 CH는 BS를 통해 인증 받은 후 세션 키를 부여 받는 구조를 갖는다. 제안 프로토콜은 각 노드측면에서 기존 방식보다 인증을 위한 메시지 전송횟수를 최소화하였고 인증된 노드를 통신에 참여시킴으로 안전한 데이터 전달을 보장한다. 제안논문은 참고문헌[12]의 AM-E방식에 비해 통신에 참여하는 노드수가 39%증가하였다. 또한 WSN 환경에서 다중 홉 통신을 지원하는 참고문헌[14]의 MET 방식보다는 통신에 참여하는 노드수가 9% 증가되었음을 시뮬레이션을 통해 증명하였다. 시뮬레이션 결과 통신에 참여하는 노드수가 많다는 것은 네트워크 생명주기가 연장되었음을 의미한다. 제안논문은 생명주기가 기존방식보다 연장되면서도 기존 AM-E에서 제공되는 안전성 측면에서 메시지 재전송 공격이나 메시지 무결성을 제공함으로 안전한 데이터 전달이 제공된다. 이 논문의 구성은 다음과 같다. 2장에서 관련연구로 기존 발표된 무선통신에서의 거리기반 에너지 소비율과 WSN을 위한 ID 기반의 인증 프레임 워크에 대해 기술하고 3장에서는 제안하는 WSN 환경에서 안전한 데이터 전달을 위한 IDE 기반의 계층적 노드인증 프로토콜을 기술한다. 4장에서는 제안 프로토콜을 증명하기 위한 실험환경과 실험 결과를 기술하고 5장에서는 결론 및 향후 연구에 대해 기술한다.

Ⅱ. 관련연구

2.1. 무선통신에서의 에너지 소비율

무선통신 환경에서는 데이터 전송시 통신거리가 길어질수록 더 많은 에너지를 소비하게 된다. 예를 들어 k-bits 메시지를 일정거리(d)만큼 전송하는데 소비되는 에너지의 양을 계산하면 (1)과 같다.

$$E_{tx}(k,d)=\begin{cases}k\times E_{elec}+k\times e_{fs}\times d^2, d<d_0\\ k\times E_{elec}+k\times e_{fs}\times d^4, d\geq d_0\end{cases}$$
$$E_{rx}(k)=k\times E_{elec} \quad (1)$$

식(1)에서 E_{tx}는 메시지를 전달하는데 소비되는 에너지양, E_{rx}는 메시지를 수신하는데 소비되는 에너지양을 의미한다. e_{fs}는 무선 통신으로 인한 에너지 소비를 의미하고, E_{elec}는 전송되는 증폭기의 에너지 소비를 의미한다. (식1)은 통신 거리가 멀어질수록 에너지 소비가 증가함을 나타낸다. 따라서 WSN을 구성하는 센서노드들의 특성에 맞게 데이터 전달을 위한 에너지 소비가 증가하지 않도록 고려해야 할 필요가 있다. 기존 방식은 SN과 BS가 직

접통신을 수행하기 때문에 이는 에너지 효율성 측면에서 효과적이지 못하다. 따라서 계층적 통신을 통해 이런 문제를 해결해야 할 필요가 있다.

2.2. 센서 네트워크를 위한 기존 방식

WSN에서 키 관리 기법들은 다양한 방법으로 연구되고 있다. 노드가 배치되기 전에 키를 분배하는 사전키 분배방식[3]과 마스터키의 사용여부에 따라 마스터 키 기반방식[6], 베이스 스테이션 기반 방식[10]으로 구분된다. 가장 대표적인 사전키 분배 방식은 3단계 과정을 통해 노드사이에 안전한 인증을 보장한다. 그러나 노드 연결 정도가 확률적으로 구성되기 때문에 WSN을 나타내는 전체 그래프가 완전하게 연결되지 않을 수 있다는 문제점을 갖는다. 또한 노드의 배치가 불규칙적이거나 배치된 환경에 물리적으로 통신을 방해하는 요소가 있는 경우 노드 연결문제는 더욱 심각해진다. 따라서 WSN에서는 하나의 키 메커니즘의 설계가 어렵다는 판단으로 4개의 암호 키와 키 설정 프로토콜을 가진 LEAP프로토콜이 제시되었다[7]. LEAP에서는 개인키, 그룹 키, 클러스터 키, Pairwise key 모두 4개의 암호 키로 구성된다. 이중 개인키와 그룹 키는 센서노드가 배치되기 전 탑재되기 때문에 악의적인 공격자에게 센서노드가 탈취 될 수 있다는 문제점을 갖는다. 또한 BS가 신뢰된 인증기관의 역할을 담당하면서 그 기능 중 일부를 CH에게 위임하는 방법으로 HIKES[10]가 제시되었다. 이 방법은 모든 노드에서 partial key escrow테이블을 이용해 키를 생성하고 CH로 선출될 수 있으며 데이터 통합 후 CH간 메시지 교환을 통해 BS에게 정보를 전송 가능하다. 그러나 센서노드를 인증하기 위해 BS와 많은 통신을 해야 하고 모든 노드가 partial key escrow테이블 저장으로 별도의 저장 공간이 필요하다는 문제점을 갖는다.

2.3. 센서 네트워크를 위한 IDE 기반의 인증 프레임워크

ID기반의 암호화는 1984년 Shamir[9]에 의해 제안되었고 그 후 다양한 응용 기법들이 제시되었다[10][11][12]. IBE 방식은 사전키 분배가 필요 없어 연산양이 적은 WSN 환경에 적용이 중요 이슈가 되고 있다. IBE는 RSA와 동일한 보안레벨을 제공하고 있으나 이미 공개된 ID를 사용하기 때문에 별도의 키 생성과 키 교환 및 키 저장 과정이 불필요함으로 빠른 수행시간과 낮은 메모리 사용이 특징이라 볼 수 있다. ID기반 2모드 인증 프레임워크는 크게 통신 준비단계와 통신단계로 나눠진다. 준비단계는 이웃노드 리스트와 라우팅 경로 설정을 통해 클러스터헤드(CH)를 찾는 단계이고, 통신 준비단계는 각 노드들이 배치된 후 통신을 시작하기 전 단계로서 각 노드는 Hello message를 통해 이웃 테이블 작성 및 라우팅 경로 설정을 통해 최초 CH를 찾는다. 통신 준비 단계는 크게 4단계로 구분된다. (단계1) 센서노드는 자신의 주변 노드들에게 자신의 ID가 담긴 Hello Message를 전송하고, (단계2) 주변 노드는 자신이 받은 Hello Message에 포함된 ID와 공통키의 존재 여부 확인을 위해 ID를 교환한다. (단계3) 공통키가 존재하면 해당 ID를 신뢰할 수 있는 노드 리스트로 추가하고 통신을 위해 경로표를 설정한다. (단계4) 단계 1,2,3의 반복 작업을 통해 작성된 경로 표를 기반으로 라우팅 알고리즘을 이용해 CH를 찾고, 각 노드의 라우팅 정보를 업데이트 한다. 통신단계에서는 두 노드 사이 통신을 위한 프로토콜로서 신뢰할 수 있는 노드 간 통신과 신뢰할 수 없는 노드 간 통신으로 나누어진다. 키 생성은 통신전 MAC 메커니즘으로 생성한 키 K_E를 사용해 통신 메시지를 암호화 하고, 키 생성함수 F는 $K_A = F_A(F(ID_A) \cap F(ID_N))$, $K_E = F_E(F(ID_E) \cap F(ID_N))$를 단방향 해쉬함수로 생성하고 이렇게 생성된 키는 사전에 분배된다. 노드 인증 단계에서는 센서네트워크 내에서 각 노드가 가진 신뢰 할 수 있는 이웃노드의 리스트와 CH가 가진 멤버노드(MN) 리스트를 기반으로 인증이 이루어진다. 그러나 2모드 인증 프레임워크에서는 최초 센서노드가 배치 전 사전 분배 받은 키(K_E)와 ID 교환을 통해 생성된 신뢰할 수 있는 이웃노드 리스트를 이용해 해당 노드의 인증 여부를 결정한다. 만약 CH가 변경되는 시점에서 공격 노드에 의한 CH 변경 메시지는 클러스터 내 치명적인 위협으로 작용될 수 있다. 또한 네트워크 사이즈가 큰 경우 MN들은 먼 거리에 있는 다른 노드들의 통신 메시지를 오버히어링 할 수 없어 그 대응은 더욱 힘들어지는 문제점을 갖는다. 또한 보안 메커니즘을 사용하는 경우 인증을 위해 전송되는 AREQ 메시지의 수가 너무 많아 노드에서 통신에 참여하기전 과다한 에너지를 소비하게 되는 문제점도 갖는다.

Ⅲ. IDE 기반의 계층적 노드 인증 프로토콜

이 장에서는 WSN 환경에서 안전한 데이터 전달을 위해 IDE 기반의 계층적 노드인증 기법을 사용한다. 인증을 위해 생성되는 인증요청 메시지(AREQ)에 대한 출처 인증과 인증을 위해 빈번히 BS와 직접통신을 수행함으로 발생되는 에너지 소비 문제를 해결한다. 또한 제안 프로토콜에서는 보안성 측면에서 기존에 충족되지 못했던 노드인증과 메시지 재사용 문제에 대한 보안 메커니즘을 강화하여 안전하게 데이터 수집이 이루어질 수 있는 프로토콜을 제안한다.

3.1 제안 모델 설계

제안모델은 IDE 기반의 계층적 노드인증 기법을 사용한다. BS을 1차 인증기관(CA)으로 하위의 모든 CH 인증을 담당 한다. 인증 받은 CH는 2차 인증기관(sCA)으로 자신이 구성하는 클러스터의 MN 인증을 수행하고 통신에 사용될 키 생성을 위해 노력한다.

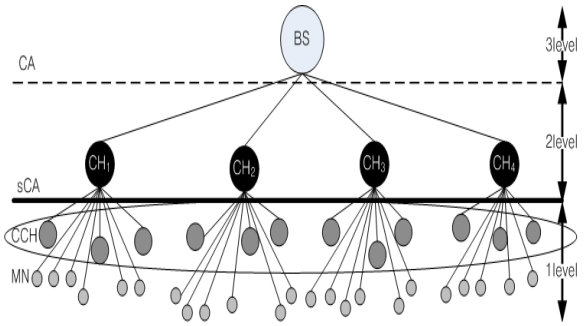

그림 1. 제안 방법의 구조
Fig. 1. The structure of proposed method

[그림1]은 제안모델의 구조를 도식화한 것이다. 제안 논문에서는 안정된 통신을 위해 세션키(α_i)와 그룹키(GK_i)를 사용한다. 세션키는 BS와 CH사이 안전한 통신을 위해 사용되고, 그룹키는 CH와 MN 사이 안전한 통신을 위해 사용된다. 제안 논문에서는 아래 가정을 기본으로 한다.

- BS와 인증DB는 언제나 안전한 통신을 가정한다.
- 모든 노드는 사전에 자신의 아이디와 패스워드, BS에서 발급한 (m)값을 할당받아 가지고 있다.
- 인증DB는 각 노드의 ID, PW, 비밀 정보값(δ_i), BS의 키값(p)을 키쌍으로 노드정보테이블을 저장하고 있다
- 모든 노드는 통신을 위해 H(m)=k를 계산한다. BS는 H*(k)=(m) 확인 가능하다.
- BS는 모든노드의 ID와 PW를 노드테이블로 저장하고 악의적인 노드에 대한 정보를 관리하기 위해 EM 테이블을 구성하고 있다 악의적인 노드가 감지되면 EM 메시지를 전송하고 테이블 업데이트를 수행한다.
- BS의 주변에 위치한 CH는 단일 홉 통신을 이용해 BS와 통신을 수행하고, BS와 1홉 이상의 거리에 있는 CH는 주변 노드정보를 이용해 다중 홉 통신을 수행한다. 이때 안전한 다중 홉 통신을 지원하기위해 CH들간의 상호 신뢰는 CA인 BS가 보장 된다.

[표1]은 제안 프로토콜에서 사용될 기호를 정의하였다. 제안 프로토콜을 크게 세션키 생성과정과 그룹키 생성과정으로 구분하여 설명한다.

표 1. 인증키 생성에 사용되는 기호 정의
Table 1. Symbol definitions that used to generate an authentication key

Symbol	Description
ID_i	i번 노드의 아이디
δ_i	i번 노드의 비밀 정보값
$nonce$	메시지 신규성을 위한 랜덤 난수 값
PW_i	i번 노드의 패스워드
GK_i	i번 클러스터간 비밀통신을 위한 그룹키
α	BS와 CH간 통신에 사용될 세션키
p	BS의 공개키
TS	타임스탬프
MKP_{ID_i}	i클러스터헤드의 멤버노드 키 풀
$EM(0, ID_{CH})$	긴급메시지로 함께 전송하는 ID의 위험성을 브로드케스팅

3.2 베이스스테이션(BS)과 클러스터헤드(CH)사이 세션키 생성

$(step.1)$ 클러스터헤드 인증요청 단계

CH는 BS에게 인증요청 메시지(Authentication REQuest message:AREQ) 메시지를 전송한다. 메시지에는 CH의 개인정보인 아이디와 패스워드, 메시지의 재사용을 방지하기 위한 난수 nonce값을 해쉬하고 암호화한 메시지에 자신의 아이디를 함께 전송한다. TS은 타임스탬프로 메시지 전달지연과 메시지 재사용을 방지하기 위해 함께 전송된다.

$$CH_i \quad : p = h(ID_i \oplus PW_i \oplus nonce_i)$$
$$m = E_k(p)$$
$$CH_i \rightarrow BS : AREQ\{TS_1, E_{ID_i}[m] \| ID_i\}$$

$(step.2)$ CH 노드 인증

BS는 CH로부터 전달받은 AREQ 메시지를 이용해 CHi의 인증을 시도한다. BS는 AREQ 메시지를 노드 i의 PW를 이용해 복호화하고 ID와 PW를 인

증DB 전송한다. 인증DB의 노드정보 테이블에 저장된 키쌍(Key Pair(ID_i, PW_i, δ_i)이 존재하는 노드는 정당한 노드로 판별한다. 인증DB는 키 쌍에서 비밀정보값을 BS에게 repVerify 메시지를 통해 전달함으로 CH노드의 인증을 완료한다. 그러나 만약 CH의 키 쌍이 존재하지 않을 경우 CH는 정당하지 않은 노드로 판단하여 전체노드에게 CH 정보(ID)를 긴급메시지와 함께 방송한다. 또한 BS는 EM 발송과 동시에 자신의 EM 테이블을 업데이트 하여 악의적인 노드 정보를 관리한다.

$$
\begin{aligned}
&BS \quad : D_{PW_i}(E_{ID_i}[m]) \\
&\qquad p = D_k(E_k(p)),\ H^*(p) = (ID_i, PW_i, nonce_i) \\
&BS \rightarrow DB: AREQ(ID_i, PW_i) \\
&if = key\ pool : DB \rightarrow BS: repVerify(ID_i, PW_i, \delta_i) \\
&if \neq key\ pool : BC^*: EM(0, ID_i),\ update\ EM\ Table \\
&BS \qquad : (ID_i, PW_i, \delta_i)
\end{aligned}
$$

$(step.3)$ BS와 CH간 통신을 위한 세션키 생성

BS는 CH의 인증확인 메시지를 인증DB로부터 수신한 후 CH와 통신을 위해 사용될 세션키를 생성한다. 세션키 생성을 위해 임의의 CH_i는 자신의 개인정보와 생성한 임의 난수($nonce_i$)를 이용해 임시키 $k = g^{nonce_{1,2,\ldots,i,b,\ldots,n}} \bmod p$를 생성한다. 여기서 n은 CH의 노드수를 나타낸다. 또한 세션키 생성에 사용한 임시키(k_i)는 클러스터 수만큼 계산하여 저장한다. 각각의 임시키는 노드 자신을 제외한 나머지 임의의 수를 이용해 만든다. 즉 $k_i = g^{nonce_{1,2,..b,..n-1}} \bmod p$로 계산된다.

$$
\begin{aligned}
&BS \ : k = g^{nonce_{1,2,\ldots i,b..n}} \bmod p, \\
&\qquad k_i = g^{nonce_{1,2,\ldots,b..n}} \bmod p, \\
&\qquad k_n = g^{nonce_{1,2,\ldots i,b..n-1}} \bmod p \\
&\quad \alpha_i = h(ID_i, k_i) \| p \ , \ m^* = E_{\delta_i}(ID_i, a_i, nonce_i) \| TS_2 \\
&BS \rightarrow CH_i : AREP\{TS_2, E_{ID_i}(m^*)\} \\
&\qquad CH_i : TS_2, D_{PW_i}[E_{ID_i}(m^*)] \\
&\qquad\quad m^* = D_{\delta_i}(E_{\delta_i}(ID_i, a_i, nonce_i) \| TS_2) \\
&\qquad\quad (ID_i, a_i, nonce_i) \\
&BS \leftarrow CH_i : E_{\alpha_i}(data)
\end{aligned}
$$

세션키 생성은 CH의 아이디(ID_i), 와 임시키(k_i)와 BS 공개키를 해쉬해서 생성된다. 패스워드(PW_i), 비밀 값(δ_i)과 랜덤난수($nonce_i$)를 개인키로 암호화하여 메시지를 생성하고 CH의 아이디로 암호화 하여 타임스탬프와 함께 CH로 인증요청응답(Authentication REPlay message:AREP)를 통해 전달하게 된다.

CH는 BS로부터 전달받은 AREP 메시지를 자신의 암호키로 복호화하고 개인키를 이용해 메시지를 복호화 하여 세션키 (α_i)를 획득한다. CH는 획득한 세션키를 이용해 수집된 데이터를 암호화하고 BS에 전달함으로 안전한 데이터 전달을 보장받는다. [그림 3]은 위 (step1~step3)과정을 도식화한 것이다.

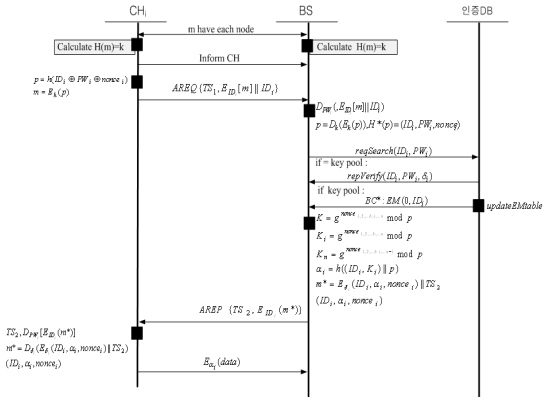

그림 2. CH와 BS사이 세션키 생성과정
Fig. 2. The session key generation between CH and BS

3.3 클러스터헤드(CH)와 멤버노드(MN)사이 그룹키 생성

$(step.1)$ MN인증

CH와 MN사이 통신에 사용될 그룹키(GK_i) 생성은 다음과 같다. 클러스터의 멤버노드인 MN_j는 CH에게 연결메시지(Join)를 통해 자신의 정보를 암호화하고 메시지 재사용을 방지하기 위해 nonce값을 함께 전달한다. CH는 MN으로부터 수신한 연결메시지를 수집하여 멤버노드 키 풀(Member node Key Pool:MKP_{CH})를 생성한다. 여기서 s은 클러스터에 속한 전체 멤버 노드수를 의미한다. 그룹키 생성에 사용될 키풀은 멤버 노드 수만큼 계산하여 저장한다.

$$
\begin{aligned}
&MN_j \qquad : \ m_j = E_k(ID_j, PW_j, nonce_j) \\
&MN_j \rightarrow CH_i : Join\{TS3, m_j\} \\
&\qquad CH_i : D_k(E_k(ID_j, \delta_j, nonce_j) \\
&\qquad\quad MKP_i = g^{1,2,\ldots i,j,\ldots s} \bmod p
\end{aligned}
$$

$(step.2)$ 그룹키 생성

CH는 BS에게 $AREQ_{MN}$를 통해 MN의 인증을 요청한다. $AREQ_{MN}$ 메시지를 수신한 BS는 사전에 발급한 세션키를 이용해 메시지를 복호화하고

MKP_{CH}를 기반으로 클러스터의 멤버노드를 인증하여 모두 정상적인 노드인 경우 그룹키(GK_{CH})를 생성을 위해 비밀 정보값(β)을 계산한다. 계산된 비밀 정보값과 CH와의 세션키를 XOR하여 그룹키(GK_{CH})를 생성한다. 만약 키풀이 인증되지 않을 경우 BS는 긴급메시지(0)를 통해 CH에게 인증되지 않은 노드정보를 전달한다.

$$
\begin{aligned}
&CH_i \rightarrow BS: AREQ_{MN}\{TS4, E_{\alpha_i}(m_j, MKP_i)\}\\
&\quad BS: D_{a_i}(E_{a_i}(m_j, MKI_i))\\
&\quad \beta = h(ID \bullet \delta_{MN_1} \oplus ID \bullet .... \oplus ID \bullet \delta_{MN_s})\\
&\quad \gamma = h(PW \bullet \delta_{MN_1} \oplus PW \bullet ... \oplus PW \bullet \delta_{MN_s})\\
&\quad GK_i = h(\beta \oplus \gamma)
\end{aligned}
$$

전송받은 MKP_{CH}와 ID_i의 임의의 수를 이용해 통신에 사용할 그룹키를 계산했다. 생성된 그룹키를 이용해 정보를 암호화하고 암호화된 정보를 복호화 할 수 있다면 양쪽노드 모두 성공적으로 그룹키가 생성되었다는 것을 의미함으로 CH가 가지고 있던 임시키를 삭제한다.

($step.3$) 그룹키 분배

BS는 CH에게 $AREP_{MN}$ 메시지를 통해 그룹키를 전달한다. CH는 복호화를 통해 그룹키를 획득하고 자신의 멤버노드들에게 아이디로 암호화하여 전달한다. 멤버노드들은 전달받은 메시지를 자신의 패스워드를 통해 복호화 하여 그룹키를 획득하게 된다.

$$
\begin{aligned}
&BS \rightarrow\ CH_i: AREP_{MN}\{TS_5, E_{\alpha}(GK_i, \beta, \gamma, nonce_i)\}\\
&\quad CH: D_{\alpha}(E_{\alpha}(GK_i, \beta, \gamma, nonce_i)\\
&\quad\quad (GK_i, \beta, \gamma, nonce_i)\\
&MN \leftarrow^{*} CH: \{TS_6, E_{ID_{MN}}(GK_i, nonce_i)\}\\
&MN_j\quad\quad : GK_i
\end{aligned}
$$

MN과 CH는 위 (step. 1)~(step. 3)까지 3단계를 거쳐 그룹키를 할당받는다. 제안 방법은 기존 방법과 같이 키 생성은 모두 BS에서 담당하게 된다. 그러나 MN이 직접 BS와 통신하지 않고 계층적 구조를 생성하여 MN은 CH와 통신을 수행하고 CH는 BS와 통신을 수행함으로 MN의 인증 및 키 분배를 수행한다.

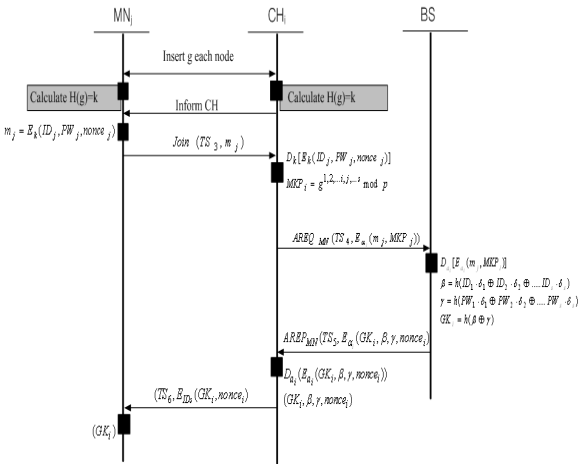

그림 3. MN과 CH 통신에 사용될 그룹키 생성과정
Fig. 3. The group key generation between MN and CH

Ⅳ. 실험 및 평가

이 장에서는 제안 프로토콜의 성능을 분석하기 위해 노드인증에 사용되는 인증키 생성비용과 인증키를 이용한 데이터 전송시 통신비용과 안전성을 평가한다. [표 3]은 제안 프로토콜을 실험하기위해 시뮬레이션에서 사용될 시스템 환경과 변수를 정의한다. 제안 논문에서는 모든 노드가 활동모드(active mode)인 경우 에너지 소모량을 고려한다.

4.1 에너지 효율성 분석

제안 프로토콜의 에너지 효율성 분석은 MN과 CH에서 인증키 수립에 소모되는 에너지량(식2)을 기반으로 한다. 인증키 수립에 소모되는 에너지량은 한 라운드 동안에 MN에서 소모되는 에너지양(식3)과 CH에서 소모되는 에너지양(식4)으로 아래와 같이 계산한다.

$$AE_{cluster} = \sum_{i=1}^{r}(AE_{CH} + AE_{MN}) \qquad (2)$$

CH의 경우 제안 논문에서는 다중 홉 통신을 수행하기 때문에 다중 홉 통신에 필요한 에너지양은 (식3)과 같다.

$$AE_{CH} = T\left[(2\delta + \mu R^k)\left(\frac{d^2}{R^2-1}\right) + (1+\mu R^2)\right] \qquad (3)$$

MN의 경우 CH와 단일 홉 통신을 수행하기 때문에 T주기 동안 단일 홉 통신에 필요한 에너지양은 (식4)와 같다.

$$AE_{MN} = T(\delta + \mu d^k) \qquad (4)$$

다음은 위에서 생성된 인증키를 사용해 통신에 참

여했을 때 소비되는 에너지양을 계산한다. 하나의 클러스터에서 통신에 참여시 소비되는 에너지량(식7)은 한 라운드 동안 인증키를 사용해 CH가 통신에 참여시 소비되는 에너지(식5)와 MN이 통신에 참여시 소비되는 에너지(식6)의 합으로 계산된다.

$$E_{CH} = m \times E_{elec}\left(\frac{n}{k} - 1\right) + m \times \frac{n}{k} + m \times e_{fs} d_{BS}^2 \quad (5)$$

$$E_{MNs} = m \times E_{elec} + m \times e_{fs} \times d_{CH}^2 \quad (6)$$

(5), (6)을 기반으로 하나의 클러스터에서 인증키를 사용해 통신에 참여시 소비되는 에너지양은 (7)과 같다.

$$E_{duster} = E_{CH} + \left(\frac{n}{k} - 1\right) E_{MNs} \quad (7)$$

이렇게 하나의 클러터 기반으로 산출된 에너지량을 한 라운드 단위로 정리하면 (8)과 같다.

$$E_{tot} = m\left\{2nE_{elec} + nE_{DA} + e_{fs}(kd_{BS}^2 + nd_{CH}^2)\right\} \quad (8)$$

4.2 실험결과

제안 프로토콜을 이용해 전체 네트워크 동안 통신에 참여한 노드수를 시뮬레이션(NS-2)하였다. 시뮬레이션 하기위한 환경조건은 [표1]과 같이 정의한다.

표 4. 시스템 환경과 변수정의
Table 1. System Environment and Parameters

시스템 환경	설명
CPU	ATmega128 L, f=8Mhz
플래시메모리	128Kbytes
ROM / RAM	4Kbytes / 36Kbyte
네트워크 크기	100m × 100m
BS 위치	50m × 50m
전체 노드수 (n)	1,000
노드간 거리(d)	10m
메시지 길이(M)	3840bit
자유공간손실(e_{fs})	$10pJ/bit$
회로에너지 소모(E_{elec})	$50nJ/bit$
데이터통합(E_{DA})	$50nJ/bit$
통신반경(R)	(Mulit)10m / (Single)20m
CH 개수(k)	2
최대홉수(h)	3
암호화/복호화	0.64ms / 0.42ms
지연 손실(μ)	2 / 4.3
라운드(r)	2000
총 에너지량(δ)	50J, 150J

많은 노드가 통신에 지속적으로 참여한다는 것은 전체 네트워크의 생명주기를 연장한다는 것과 같이 해석될 수 있다. 따라서 기존 계층방식으로 제안된 LEACH 방식과 LEACH 방식을 다중홉 통신으로 수정한 MTE 방식, 그리고 계층기반에서 안전성을 제공하는 AM-E 방식과 제안방식을 동일 조건에서 시뮬레이션 한 결과 [그림 3]과 같다.

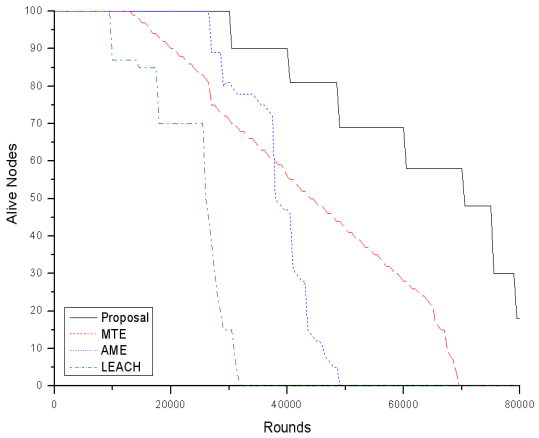

그림 4. 생존노드 수
Fig. 4. Number of alive nodes

[그림 3]에서와 같이 다중 홉 통신을 제공하는 MTE 방식[14]과 제안 논문을 비교해보면 통신에 참여하는 노드수가 약 9.7%정도 향상되었다. MTE 방식의 경우는 모든 CH가 다중홉 통신을 기반으로 데이터가 전달되기 때문에 기존 LEACH 방식보다는 에너지 소비율이 감소하였으나 제안 방식에 비해 높은 에너지 효율을 보이고 있다. 또한 MTE 방식은 노드 인증을 제공하고 있지 않다. 따라서 제안 논문은 노드 인증을 제공하여 안전한 데이터를 전송하는 AM-E방식과 에너지효율을 비교한 결과 통신에 참여하는 노드수가 약 39% 높음을 실험을 통해 보였다.

4.3 노드의 안전성 분석

제안논문은 노드 인증을 통한 신뢰 할 수 있는 노드만 데이터 전송에 참여할 수 있으며 노드의 에너지 효율을 높여 전체 네트워크 생명주기를 연장하는 방식이다. 제안논문의 안전성 측면을 살펴보면 악의적인 공격자에게 메시지가 노출될 가능성은 존재한다. 그러나 MN, CH, BS사이에서 사용되는 모든 메시지에 각각의 난수를 생성하여 함께 암호화하여 전달하기 때문에 악의적인 공격자가 메시지를 획득하는 경우에도 메시지의 내용을 확인 할 수 없

고 가로챈 메시지를 변형 할 수 없어 메시지 재전송 공격이 불가능하게 된다. 또한 통신에 참여하는 모든 노드는 통신에 참여하기전 반드시 노드인증 과정을 통해 인증된 노드만 통신에 참여하여 센싱 정보를 전달 할 수 있다 따라서 특정 노드에 DoS 공격은 경우는 사전에 방지 할 수 있어 안전한 통신을 제공 할 수 있다.

V. 결 론

이 논문에서는 WSN 환경에서 안전한 데이터 전달을 위한 방법으로 IDE 기반의 계층적 노드인증 프로토콜을 제안 하였다. 초기 WSN에서는 노드가 수집한 데이터를 무조건 BS에게 전달하거나 CH에게 전달함으로 전달받은 데이터는 인증되지 않은 데이터로 안전성 여부를 판단 할 수 없었다. 그 후 WSN의 특성을 고려하여 기존 여러 가지 방법으로 통신에 참여하는 노드를 인증하여 안전한 통신을 제공하는 방법들이 제안되어 왔다. 그러나 노드의 인증을 위한 AREQ/AREP의 메시지들이 많아 노드의 한정된 에너지 사용에 큰 부담으로 작용되고 BS와 SN사이 직접적인 통신으로 인한 노드의 에너지를 과다하게 많이 소비하게 됨으로 노드의 본질적 데이터 수집의 역할을 담당 할 수 없게 되는 문제점을 갖는다. 따라서 제안 논문에서는 무선네트워크에서 에너지 소비가 전달하는 메시지의 크기와 거리에 비례한다는 근거에 따라 네트워크를 계층적으로 구성하고 각 BS와 통신을 중간의 CH가 담당하도록 구성하였다. 또한 통신에 참여하는 모든 노드의 인증은 BS가 담당하게 되는데 노드 인증 전 CH의 인증과정을 거쳐 인증된 CH는 sCA 역할을 부여하고 MN의 인증에 참여하도록 제안하였다. 노드인증에 사용되는 IDE 기반의 계층적 노드인증 프로토콜은 전체 네트워크에서 소비되는 에너지양을 최소화하면서 통신에 사용될 세션키와 그룹키를 생성하여 전달하고, 인증된 노드만이 통신에 참여 할 수 있도록 함으로 전달되는 데이터의 안전성을 보장한다. 제안 논문의 에너지 효율성 측면에서 AM-E방식보다 통신에 참여한 노드수가 약39% 증가하였고, 다중홉 통신을 제공하는 MTE방식 보다는 약 9%가량 증가하였다. 그러나 MTE 기반의 경우 노드인증이 제공되고 있지 않아 통신에 참여하는 노드와 전달되는 데이터의 안전성 측면은 제공되지 않고 있다. 따라서 제안 프로토콜은 기존방식(AM-E)과 동일한 안전성을 제공하면서 에너지 효율을 향상시켜 전체 네트워크 생명주기를 연장하였다. 향후 제안 프로토콜의 보안성 측면의 향상을 위한 연구가 계속 진행될 필요가 있으며 다양한 보안 공격에도 안전한 데이터 전달을 위한 연구가 필요하다.

참 고 문 헌

[1] W. Ke, P. Basu, S. Abu Ayyash, and T.D.C. Little, "Attribute Based Hierarchical Clustering in Wireless Sensor Networks", *MCL Technical Report* No. 03-24-2003

[2] Seema Bandyopadhyay and Edward J. Coyle, "An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks", *INFOCOM2003*

[3] L.Eschenauer and V.D.Gligor, "A key management scheme for distrivuted sensor networks" *In 9th ACM conference on computer and communications security* , pp. 41-47, 2002

[4] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", *Wireless Networks*, Vol. 8. No. 5, pp. 521-534, 2002.

[5] Q. Huang, J. Cukier, H. Kobauashi, B. Liu and J.Zhang, "Fast Authenticated Key Establishment Protocols for Self-organizing Sensor Networks", *InProc. of the 2nd SCM International Conference on Wireless Sensor Networks and Application*s, pp.141-150, 2003.

[6] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks", *In 10th ACM Conference on Computer and Communication Security(CCS),* 2003.

[7] H. Chan, A. Perrig, "PIKE:Peer Intermediaries for Key Establishment in Sensor Networks", *IEEE Infocom*, Vol. 1, pp. 524-535, 2005.

[8] R.M.S. Silva, N.S.A.Pereira, M.S.Nunes, "Applicability Drawbacks of Probabilistic Key Management Schemes for Real World Applications of Wireless Sensor Networks",. *Proceeding of the Third International Conference on Wireless and Mobile*

Communication(ICWMC'07), pp.51-58, 2007

[9] W. S. Juang, "Efficient User Authentication and Key Agreement in Wireless Sensor Networks", *WISA 2007*, LNCS 4298, pp. 15-29, Springer-Verlag, 2007.

[10] J.Ibriq and Imad Mahgoub, "A Hierarchical key establishment scheme or Wireless sensor networks", *Proceedings of 21st International conference o*n advanced Networking and applications(AINA07), pp.210-219, 2007

[11] W. S. Juang, "Efficient User Authentication and KeyAgreement in Wireless Sensor Networks", *WISA 2007*, LNCS 4298, pp. 15-29, Springer-Verlag, 2007.

[12] T.T Huyen, Eui-Nam huh, "A reliable 2-mode authentication framework for Ubiquitous sensor network", *Journal of Korean Society for Internet Information*, 2008

[13] N. T.T. Huyen and E. Huh. "An efficient signal range based key pre-distribution scheme ensuring the high connectivity in wireless sensor network. In ICUIMC '08, page 441~447, 2008

[14] Sung-Hwa Hong and Byoung-Kug Kim,"Flooding Level Cluster-based Hierarchical Routing Algorithm For Improving Performance in Multi-Hop Wireless Sensor Networks", Journal of korea information and communications society, Vol 33,No3, pp pp123-134, 2008

[15] Boseung Kim, Huibin Lim,Jongseok Choi and Yongtae Shin,"A Study on Node Authentication Mechanism using Sensor Node's Energy Value in WSN" Journal of The Institute of Electronics Engineers of Korea, Vol 48-CI, No2, pp 86~95, 2011

조 영 복 (Young-bok Cho) 정회원

2006년 3월 충북대학교 전자계산학과 석사

1981년 3월~현재 충북대학교 전자계산학과 박사과정

<관심분야> 센서네트워크, 라우팅, 클러스터링, 정보보안

이 상 호 (Sang-ho Lee) 종신회원

1989년 2월 숭실대학교 전자계산학과 박사

1981년 3월~현재 충북대학교 전자정보대학 교수

<관심분야> 컴퓨터네트워크, 정보보호, 데이터통신