논문 2011-48CI-2-10

WSN 환경에서 센서 노드의 에너지 값을 이용한 노드 인증 메커니즘에 관한 연구

(A Study on Node Authentication Mechanism using Sensor Node's Energy Value in WSN)

김 보 승*, 임 휘 빈**, 최 종 석***, 신 용 태****

(Boseung Kim, Huibin Lim, Jongseok Choi, and Yongtae Shin)

요 약

무선 센서 네트워크에서의 센서 노드는 제한적인 하드웨어 성능과 네트워크 토폴로지가 수시로 변하는 무선 통신을 이용하기 때문에 유선 네트워크보다 보안이 취약하다. 보안을 강화하는 기법 중 노드 인증 메커니즘은 노드의 ID를 이용한 데이터 위변조 공격이나 네트워크의 라우팅을 방해하는 라우팅 공격을 방어하는 데 이용한다. 본 논문에서는 베이스 스테이션이 인증 요청을 하는 노드의 시간에 따른 에너지 값을 이용해서 인증키를 생성하고, 다른 노드와의 데이터 전송을 위한 통신 절차를 수행하는 AM-E 메커니즘을 제안한다. 노드의 에너지 값은 시간에 따라 변하므로, 인증 요청을 할 때마다 인증키가 바뀌는 특징을 갖는다. 이러한 특징은 센서 네트워크의 보안성을 강화하여 보다 안전한 WSN을 구성하는데 일조할 것이다.

Abstract

Sensor nodes in wireless sensor networks are vulnerable to security than wired network due to using limited hardware performance and wireless communications that network topology changes frequently. Among techniques to enhance the security, the node authentication mechanism is used to defend against data forgery attacks using the ID of the node or to interfere with the routing of the network routing. In this paper, we proposed the AM-E mechanism that makes authentication key by using the energy value of node requesting authentication and performs the communication procedures for data transfer between different nodes. Because the energy value of node is changed depending on time, every time the authentication request is, an authentication key is changed. These features enhance the security of sensor networks and will help to configure the more secure WSN.

Keywords : 무선 센서 네트워크, 센서 노드, 에너지 값, 노드 인증 메커니즘

Ⅰ. 서 론

무선 센서 네트워크는 온도, 조도, 풍향 등을 측정할 수 있는 다수의 센서 노드들이 무선으로 통신하도록 구성된 네트워크이다. 각 센서 노드는 무선으로 통신하며, 정형화된 네트워크 토폴로지가 없기 때문에 대표적인 보안 요구 사항인 기밀성과 무결성을 제공하지 못하므로 유선 네트워크보다 더욱 다양한 보안 취약성이 존재한다. 센서 노드의 ID 정보를 활용하여 데이터를 위변조하는 공격이나 공격자가 센서 노드의 ID 정보를 위장하여 센서 네트워크의 라우팅을 방해하는 공격을 방어하기 위해서는 무선 센서 네트워크의 노드 인증 메커니즘이 필요하다.

따라서 본 논문에서는 무선 센서 네트워크를 구성하는 각 센서 노드의 에너지 갑을 이용한 AM-E (Authentication Mechanism using a Node's Energy in Wireless Sensor Network) 메커니즘을 제안한다. AM-E 메커니즘은 베이스 스테이션이 인증 요청을 하

* 정회원-교신저자, *** 학생회원, **** 정회원, 숭실대학교 컴퓨터학과
(Department of Computer Science, Soongsil University)
** 정회원, (주)지아이티 시스템서비스팀
(System Service Team, GIT Co., Ltd.)
접수일자: 2010년10월12일, 수정완료일: 2011년3월4일

는 노드의 시간에 따른 에너지 값을 이용해서 인증키를 생성하고, 다른 노드와의 데이터 전송을 위한 통신 절차를 수행한다.

본 논문의 구성은 다음과 같다. Ⅱ 장에서는 센서 노드의 ID와 시간에 따른 노드의 잔량 에너지 값을 이용한 AM-E 메커니즘을 제안한다. Ⅲ 장에서는 제안한 AM-E 메커니즘을 분석한다. Ⅳ 장은 본 논문의 결론 및 향후 과제이다.

Ⅱ. AM-E 메커니즘

1. 기존의 노드 인증 메커니즘

안전한 무선 센서 네트워크를 구성하기 위해 먼저 고려해야 할 사항은 노드 인증과 암호화 통신에 사용되는 암호화키(Cryptographic key)를 분배하는 것이다.

가. 대칭 키(Symmetric key)

대칭키 암호 방식은 센서 네트워크를 구성하는 모든 센서 노드가 단일키를 사용하는 것이다. 그러나 하나의 노드로부터 단일키가 노출이 될 경우, 센서 네트워크 전체의 정보를 노출시키는 단점이 있다. 이를 보완하는 랜덤-키 사전 분배(Random-Key Predistribution) 기법[1], q-합성수 랜덤 키 사전 분배(q-composite random key predistribution scheme) 기법[2], Bloom의 키 사전 분배 기법[3] 등이 있다.

나. 공개키(Public key)

공개키 인증 방식은 RSA 또는 ECC와 같은 공개키 암호 알고리즘을 사용하여 두 노드가 직접 안전하고 신뢰성 있도록 키를 생성하는 방법이다. 공개키 알고리즘에는 각 노드들이 자신의 고유의 공개키와 비밀키를 쌍으로 가지고 있으며, 키를 생성하고자 하는 상대방의 공개키와 자신의 비밀키를 사용하여 두 노드 사이에 공유되는 키를 생성한다.

다. SPINS

(Security Protocols for Sensor Networks)[4]

보안 프로토콜인 SPINS[4]는 무선 센서 네트워크의 안전성을 향상시키기 위해 UC 버클리에서 개발한 보안 프로토콜이다. SPINS[4]는 SNEP(Secure Network Encryption Protocol)과 μ-TESLA(the "micro" version of Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol)로 구성되어 있다. SNEP은 데이터의 기밀성(confidentiality), 인증(authentication), 무결성(integrity)teg적시성(freshness) 기밀공하는 일대일 통신이고, μ-TESLA는 베이스 스테이션(base station)으로부터 인증된 브로드캐스트(broadcast)를 제공한다.

2. 기존의 노드 인증 기법들의 장단점 분석

대칭키 인증 기법의 인증키 생성 주체는 상호 노드이다. 즉, 두 노드가 대칭키를 가지고 상호 간 인증을 한다. 장점은 비교적 간단한 인증 구조를 갖는다는 것이며, 단점은 노드가 증가함에 따라 인증키가 증가하게 되어 이에 대한 키 관리의 효율성이 저하된다는 것이다.

공개키 인증 기법의 인증키 생성 주체는 싱크 노드(또는 베이스 스테이션)이다. 즉, 싱크 노드가 공개키를 사용하여 센서 노드를 인증한다. 장점은 공개키 연산 수행을 싱크 노드(또는 베이스 스테이션)가 하여 센서 노드의 연산 오버헤드가 감소한다는 것이다. 단점은 노드 인증을 위한 인증기관이 필요하고, 인증기관에서 발행하는 인증서를 저장하기 위한 메모리 공간이 필요하다는 것이다.

μ-TELSA 인증 기법의 인증키 생성 주체는 동기화된 싱크 노드이다. 즉, 동기화된 싱크 노드와 센서 노드 간 일정 시간 간격에 맞추어 인증키를 송수신한다. 장점은 해시 체인을 이용하여 효과적인 데이터 인증을 한다는 것이다. 단점은 인증에 일정 시간이 필요하며, 키

표 1. 인증 기법들의 장단점
Table 1. Strengths and weaknesses of certification scheme.

	인증키 생성 주체	장점	단점
대칭키 인증기법	상호 노드	간단한 인증 구조	인증키 증가에 따른 키 관리로 효율성 저하
공개키 인증기법	싱크 노드	싱크 노드의 공개키 연산 수행으로 센서 노드의 연산 오버헤드 감소	노드 인증을 위한 인증기관과 인증서의 저장 공간이 필요
SPINS 인증기법	시간이 동기화된 싱크 노드	해시 체인을 이용	인증지연 시간과 키 체인의 저장 공간이 필요

체인의 저장 공간이 필요하다는 것이다.

표 1은 이러한 인증 기법들의 장단점을 요약한 것이다.

기존의 노드 인증 메커니즘을 무선 센서 네트워크에서 적용하고자 할 때, 각각의 특징에 따른 제약이 있음을 알 수 있다. 따라서 이러한 단점을 보완할 수 있는 노드 인증 메커니즘의 개선이 필요하다.

3. 제안하는 AM-E 메커니즘

본 절에서는 무선 센서 네트워크를 구성하는 노드를 인증하는 AM-E(Authentication Mechanism using Node's Energy in Wireless Sensor Network) 메커니즘을 제안한다. AM-E 메커니즘은 베이스 스테이션(base station)이 인증 요청을 하는 노드의 에너지 값을 이용해서 인증키를 생성하고, 이를 인증 요청한 노드에게 전송함으로써 인증 절차를 수행한다.

가. AM-E 메커니즘의 네트워크 모델

제안하는 AM-E 메커니즘은 하나의 베이스 스테이션과 다수의 노드로 구성된 무선 센서 네트워크 모델을 기반으로 한다.

노드는 베이스 스테이션에게 인증키 요청 메시지를 전송하고, 베이스 스테이션의 인증 과정을 통해 인증키를 받은 후 통신에 참여한다.

베이스 스테이션은 인증을 위한 키 생성, 암·복호화 등의 연산을 처리한다. 이는 많은 연산 처리 과정으로 인한 노드의 연산 오버헤드를 줄이게 한다. 노드의 인증키 요청 메시지를 통해 인증키 생성 과정을 수행하여 인증키를 생성한다.

제안하는 AM-E 메커니즘은 아래의 요구사항을 만족한다고 가정한다.

- 네트워크에 존재하는 베이스 스테이션은 인증 프로세스와 데이터베이스 프로세스로 구성된다.
- 베이스 스테이션의 데이터베이스에는 네트워크 내에 있는 노드의 ID 정보가 사전에 저장되어 있다.
- 노드는 네트워크에 진입 시 베이스 스테이션에게 인증을 요청한다.
- 라우팅 보안(secure routing)은 본 논문에서 다루지 않는다.

나. 인증키 메커니즘

인증키 메커니즘은 인증키 생성, 인증키 분배, 인증키 갱신 단계를 수행한다.

(1) 인증키 생성

베이스 스테이션은 인증 요청한 노드가 전송한 정보를 이용하여 개인키와 인증키를 생성한다. 표 2는

표 2. AM-E 메커니즘의 명령 및 변수 정의
Table 2. AM-E mechanism of the command and variable definitions.

표기	정의
Calculate	ID_A와 E_T^A를 계산
Search	베이스 스테이션의 데이터베이스를 검색
Verity	데이터베이스에서 검색한 결과
Ignore	다음 과정의 진행을 무시
Save	베이스 스테이션의 데이터베이스에 저장
Send to A	A에게 전송
ID_A	A의 ID
E_{PT}^A	A의 이전 잔량 에너지 값
E_{CT}^A	A의 현재 잔량 에너지 값
TS_A	A의 타임스탬프(time stamp)
$result$	데이터베이스에서 검색한 결과 값
T	True
F	False
PK_A	A의 개인키
AK_A	A의 인증키
H	해시 함수(hash function)
$A, B, \cdots$	네트워크에 있는 노드

Algorithm. 인증키 생성 알고리즘

입력 : 노드가 전송한 인증 요청 메시지
출력 : 개인키와 인증키

Procedure *AuthenticationKeyCreation*
  Calculate ID_A from a message of node **Then**
    Search Begin
    ID_A := Search the Database of Base station
    // If ID_A exist the Database of Base station, *result* is T
    // If ID_A doesn't exist the Database of Base station, *result* is F
    result:= Verify
    Search End
  IF *result*= F Then
    Ignore from a message of node
  ELSE Then
    Key Creation Begin
      $PK_A := H(ID_A \oplus E_{CT}^A)$
      $AK_A := H(PK_A \oplus E_{CT}^A)$
    Save $(PK_A, AK_A, E_{CT}^A, TS_A)$ to the Database of Base station
    Send (PK_A, AK_A) to node
    Key Creation End

{PK_A is a private key and AK_A is authentication key of node.}

그림 1. 인증키 생성 알고리즘
Fig. 1. Authentication key generation algorithm.

AM-E 메커니즘에서 사용하는 명령 및 변수의 정의이고, 그림 1은 AM-E 메커니즘의 인증키 생성 알고리즘이다.

베이스 스테이션은 노드가 전송한 인증키 요청 메시지로부터 노드의 ID_A을 얻는다. 노드의 ID_A 정보가 베이스 스테이션의 데이터베이스에 없으면 해당 노드의 인증키 요청 메시지를 무시한다. 노드의 ID_A 정보가 베이스 스테이션의 데이터베이스에 있으면 수식 (1)과 수식 (2)을 이용하여 인증키를 생성한다.

수식 (1)은 노드의 ID_A와 노드의 현재 잔량 에너지 값 E_{CT}^A을 XOR 연산을 한 후 해시 함수를 통해 노드의 개인키를 생성하는 식이다.

$$PK_A = H\left(ID_A \oplus E_{CT}^A\right) \tag{1}$$

수식 (2)은 생성한 개인키 PK_A와 노드의 현재 잔량 에너지 값 E_{CT}^A을 XOR 연산을 한 후 해시 함수를 통해 인증키를 생성하는 식이다.

$$AK_A = H\left(PK_A \oplus E_{CT}^A\right) \tag{2}$$

(2) 인증키 분배

베이스 스테이션에서 생성된 인증키는 그림 2와 같은 분배 과정을 수행한다.

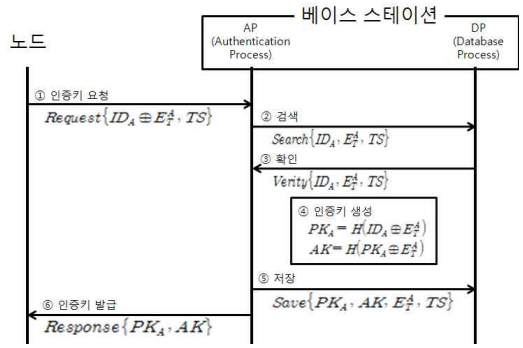

그림 2. 인증키 분배 절차
Fig. 2. Authentication key distribution procedure.

① 인증 요청

노드는 자신의 ID_A와 이전 잔량 에너지 값 E_{PT}^A의 XOR 연산을 한 값과 현재 잔량 에너지 값 E_{CT}^A, 타임스탬프 TS_A로 구성된 인증 요청 메시지를 베이스 스테이션에게 전송한다.

노드→베이스 스테이션 :

$$Request\left\{\left(ID_A \oplus E_{PT}^A\right), E_{CT}^A, TS_A\right\}$$

② 노드 정보 검색

베이스 스테이션은 수신한 인증 요청 메시지를 이용하여 노드의 ID_A와 이전 잔량 에너지 값 E_{PT}^A을 데이터베이스에서 검색한다.

베이스 스테이션 : $Search\left\{ID_A, E_{PT}^A\right\}$

③ 노드 정보 확인

데이터베이스에 인증 요청한 노드의 정보가 확인되면 인증키 생성 절차를 수행한다.

베이스 스테이션 : $Verity\left\{ID_A, E_{PT}^A\right\}$

④ 인증키 생성

노드의 ID_A와 현재 잔량 에너지 값 E_{CT}^A를 XOR 연산을 한 후 해시 함수 H를 통해 노드의 개인키 PK_A를 생성한다. 생성한 개인키 PK_A와 노드의 현재 잔량 에너지 값 E_{CT}^A를 XOR 연산을 한 후 이를 해시 함수를 통해 인증키 AK_A를 생성한다.

베이스 스테이션 : $PK_A = H\left(ID_A \oplus E_{CT}^A\right)$

$$AK_A = H\left(PK_A \oplus E_{CT}^A\right)$$

⑤ 저장

베이스 스테이션은 생성한 노드의 개인키 PK_A, 인증키 AK_A, 현재 잔량 에너지 값 E_{CT}^A, 타임스탬프 TS_A을 데이터베이스에 갱신하여 저장한다.

베이스 스테이션 : $Save\left\{PK_A, AK_A, E_{CT}^A, TS_A\right\}$

⑥ 인증키 발급

베이스 스테이션은 인증 요청을 한 노드에게 생성한 노드의 개인키 PK_A와 인증키 AK_A를 전송한다.

베이스 스테이션→노드 :

$$Response\left\{PK_A, AK_A\right\}$$

이와 같은 절차를 통해 베이스 스테이션은 생성한 개인키와 인증키를 노드에게 전송한다.

(3) 인증키 갱신

인증키 갱신은 전체 네트워크에서 발생하지 않고, 각각의 노드가 베이스 스테이션에게 새로운 인증키 정보 요청을 할 때 수행한다. 이는 인증키 갱신에 따른 네트워크에 속한 모든 모드의 불필요한 에너지 소모를 막고, 네트워크의 전체적인 키 갱신을 통한 전체 네트워크의 키 정보에 대한 동기화를 지양한다. 또한 각 노드마다 데이터를 전달하기 시작하는 시점부터 키 갱신을 수행하게 함으로써, 일부 경로에서의 키 정보 노출을 초래하지 않도록 하여 키 정보의 보안성을 강화한다.

다. 노드 인증 메커니즘

AM-E 메커니즘을 이용한 노드-to-노드 인증은 베이스 스테이션으로부터 상대 노드의 인증 정보를 요청한 후 이를 이용하여 데이터를 전송한다. 네트워크 내의 다른 노드와의 통신을 원할 경우, 노드 인증을 위한 그림 3과 같은 절차를 수행한다.

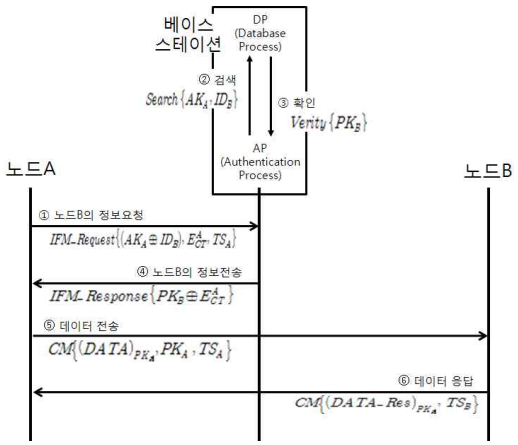

그림 3. 노드 인증 절차
Fig. 3. Node authentication procedure.

① 노드B의 정보요청

노드A가 노드B와 통신을 원할 경우, 노드B에 대한 정보를 요청하는 메시지를 베이스 스테이션에게 전송한다 .노드A의 인증키 AK_A와 노드B의 ID_B를 XOR 연산한 값과 현재 잔량 에너지 값 E_{CT}^A, 타임스탬프 TS_A와 함께 전송한다.

노드A→베이스 스테이션:
$$IFM\_Request\{(AK_A \oplus ID_B), E_{CT}^A, TS_A\}$$

② 검색

베이스 스테이션은 노드A가 보낸 메시지를 통해 인증키 AK_A와 노드B에 대한 정보를 데이터베이스에서 검색한다.

베이스 스테이션: $Search\{AK_A, ID_B\}$

③ 확인

인증키 AK_A가 정상적으로 발급된 노드이면, 데이터베이스에서 노드A가 요청한 노드B의 개인키 PK_B를 확인한다. 만약 인증키 AK_A가 발급되지 않은 노드이면, 이후의 과정은 수행하지 않는다.

베이스 스테이션: $Verity\{PK_B\}$

④ 노드B의 정보 전송

베이스 스테이션은 노드B의 개인키 PK_B를 노드A의 현재 잔량 에너지 값 E_{CT}^A를 XOR 연산하여 노드A에게 전송한다.

베이스 스테이션→노드A:
$$IFM\_Response\{PK_B \oplus E_{CT}^A\}$$

⑤ 데이터 전송

노드A는 노드B의 개인키 PK_B를 이용하여 메시지를 전송한다. 노드B의 개인키 PK_B로 전송한 메시지를 암호화하고, 노드A의 개인키 PK_A와 타임스탬프 TS_A를 전송한다. 이를 통해 노드B는 노드A의 개인키 PK_B를 획득한다.

노드A→노드B: $CM\{(DATA)_{PK_A}, PK_A, TS_A\}$

⑥ 데이터 응답

노드B는 노드A에게 데이터 응답 메시지를 전송한다. 노드B는 획득한 노드A의 개인키 PK_A를 이용하여 데이터 응답을 암호화하고, 타임스탬프 TS_B와 함께 전송한다.

노드B→노드A: $CM\{(DATA\_Res)_{PK_A}, TS_B\}$

이와 같은 과정을 통해 노드-to-노드 인증을 한다. 베이스 스테이션으로부터 인증 여부를 확인받은 노드는 상대 노드의 개인키를 이용하여 데이터를 암호화하여 통신한다.

Ⅲ. AM-E 메커니즘 분석

본 장에서는 AM-E 메커니즘의 성능을 비용 측면과 보안성 측면을 분석하여 SPINS[4]와 비교한다.

1. 비용(cost) 분석

본 절에서는 AM-E 메커니즘의 비용을 분석한다. AM-E 메커니즘의 인증키 생성 비용과 인증키를 발급받은 노드가 다른 노드에게 데이터 전송할 때의 통신비용을 SPINS[4]와 비교하였다.

가. 네트워크 및 시스템 환경

네트워크 환경은 $500m \times 500m$ 영역에 100개의 센서 노드와 한 개의 베이스 스테이션으로 구성하였고, 센서 노드는 그리드(grid) 구조로 배치하였다. 센서 노드는 배치에 따라 베이스 스테이션에게 직접 데이터를 전송할 수 있거나 다른 노드들을 중계 노드로 하여 여러 홉을 경유하여 데이터를 전달할 수 있다. 다른 네트워크의 가정 사항은 SPINS[4]와 동일하다.

시스템 환경의 센서 노드는 SPINS[4]와 동일한 성능으로 구성하였고, 베이스 스테이션은 센서 노드보다 우수한 연산 능력을 가진다. 인증 기법을 실행하는데 소모되는 에너지는 Nachiketh의 논문[5]를 참고하였고, 각 노드의 송수신에 대한 에너지 소모는 NAI Labs Technical Report[6]을 참고하였다. 모든 노드는 active 모드일 때만 에너지 소모를 하고, sleep 모드일 때의 에너지 소모는 고려하지 않았다. 표 3은 센서 노드와 베이스 스테이션의 시스템 환경이다.

표 3. 시스템 환경
Table 3. environments of system.

		센서 노드	베이스 스테이션
CPU		8bit, 4MHz	32bit, 2.4GHz
Storage	Instruction Flash	8KB	32KB
	RAM	512byte	1KB
Bandwidth		10Kbps	250Kbps
Communication		916MHz Radio	
Energy to Transmit		21μJ/byte	
Energy to Receive		14μJ/byte	

나. 인증키 생성 비용 분석

AM-E 메커니즘의 인증키 생성 비용은 노드가 베이스 스테이션에게 인증키 요청 메시지를 전송하고, 인증키를 수신할 때까지의 비용을 계산하여 SPINS[4]와 비교하였다. 표 4는 AM-E 메커니즘과 SPINS[4]에서의 에너지 소모를 계산할 때 사용하는 변수이다.

표 4. 변수 정의
Table 4. Variable definitions.

정의	설명
E_{AM-E}	AM-E 인증 메커니즘의 전체 비용
KG_{AM-E}^{Auth}	AM-E 인증 메커니즘에서 하나의 노드에서의 키 생성 비용
KA_{AM-E}^{E}	AM-E 인증 메커니즘에서 하나의 노드에서의 키 갱신 비용
E_{SPINS}	SPINS의 전체 비용
KG_{SPINS}^{Auth}	SPINS에서 하나의 노드에서의 키 생성 소모 비용
KA_{SPINS}^{E}	SPINS에서 하나의 노드에서의 키 갱신 소모 비용
n	노드 개수
M_{Size}	전체 메시지 크기
M_{Total}	전체 메시지의 개수
H_E	해시 함수의 단위 비용
T_E	비트당 전송시 단위 비용
R_E	비트당 수신시 단위 비용

수식 (3)은 제안하는 AM-E 인증 메커니즘의 인증키 생성 비용을 계산하는 수식이고, 수식 (4)은 SPINS[4]의 인증키 생성 비용을 계산하는 수식이다. 전체 네트워크의 인증키 생성 비용은 n개의 노드가 키 생성과 키 갱신을 할 때, 비용의 합으로 나타낼 수 있다.

$$E_{AM-E} = \sum_{i=1}^{n} \left(KG_{AM-E}^{Auth} + KA_{AM-E}^{E} \right) \quad (3)$$

$$E_{SPINS} = \sum_{i=1}^{n} \left(KG_{SPINS}^{Auth} + KA_{SPINS}^{E} \right) \quad (4)$$

수식 (5)은 제안하는 AM-E 인증 메커니즘의 키 생성에 따른 비용을 계산하는 수식이고, 수식 (6)은 SPINS[4]의 키 생성에 따른 비용을 계산하는 수식이다. 키 생성 요청 메시지를 수신하는 단위수신비용과 메시지에 대한 해시 함수를 두 번 수행하므로 단위해시비용 H_E가 두 번 소모되며, 생성한 키를 노드에게 전송하는 단위송신비용을 소모한다.

$$KG_{AM-E}^{Auth} = \sum_{i=1}^{M_{Total}} \left(R_E + M_{Size} \times H_E \times 2 + T_E \right) \quad (5)$$

$$KG_{SPINS}^{Auth} = \sum_{i=1}^{M_{Total}} (R_E + M_{Size} \times H_E + T_E) \quad (6)$$

수식 (7)은 제안하는 AM-E 메커니즘에서 하나의 노드가 한 번의 키 갱신에 따른 비용을 계산하는 수식이고, 수식 (8)은 SPINS[4]에서 하나의 노드가 한 번의 키 갱신에 따른 비용을 계산하는 수식이다. 키 갱신을 하는 노드는 키를 수신하는 과정에서 필요한 단위수신비용이 소모된다.

$$KA_{AM-E}^{E} = R_E \quad (7)$$

$$KA_{SPINS}^{E} = R_E + M_{Size} \times H_E \quad (8)$$

그림 4는 AM-E 메커니즘과 SPINS[4]의 인증키 생성 비용을 비교한 그래프이다. 전체 네트워크에서 인증키를 요청하는 노드가 증가함에 따른 인증키 생성 비용을 산출하였다.

전체 네트워크에 대한 AM-E 메커니즘의 인증키 생성 비용은 약 $132mJ$이 소모되며, SPINS[4]는 약 $140mJ$이 소모되는 것으로 나타났다. 즉, 제안한 AM-E 메커니즘의 인증키 생성 비용이 SPINS[4]보다 약 0.06% 정도 적다고 할 수 있다.

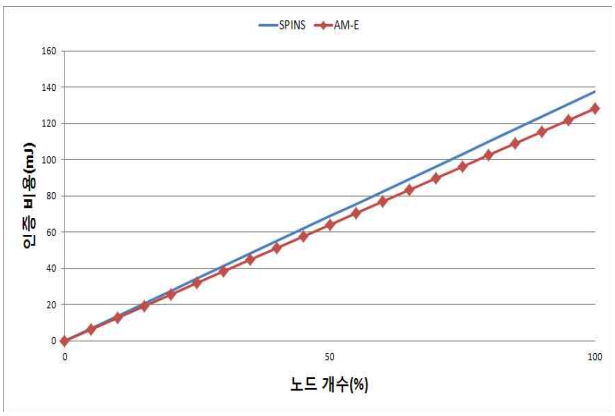

그림 4. 인증키 생성 비용 결과
Fig. 4. Authentication key generation costs resulting.

다. 통신비용 분석

통신비용은 AM-E 메커니즘과 SPINS[4]의 통신 절차에 따른 데이터 전송 횟수를 계산하여 비교하였다. 그림 5는 AM-E 메커니즘의 통신 절차를 나타낸 것이고, 그림 6은 SPINS[4]의 통신 절차를 나타낸 것이다.

AM-E 메커니즘의 데이터 전송은 4단계 절차를 수행하고, SPINS[4]의 데이터 전송은 6단계 절차를 수행한다.

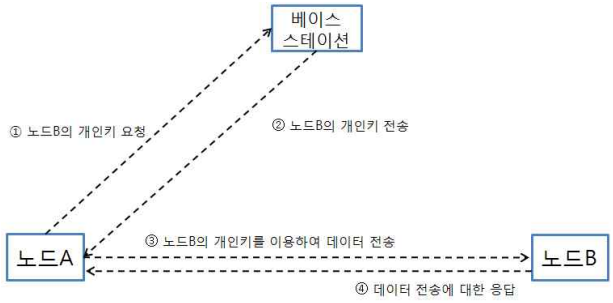

그림 5. AM-E 메커니즘의 통신 절차
Fig. 5. AM-E mechanism of the communication process.

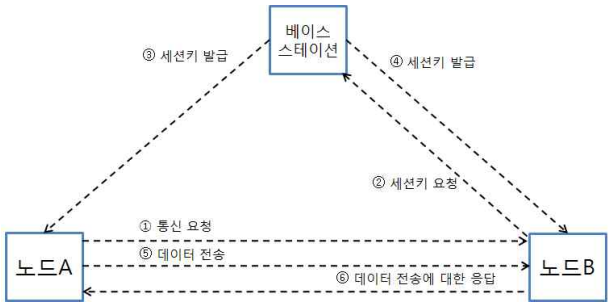

그림 6. SPINS[4]의 통신 절차
Fig. 6. SPINS[4] of the communication process.

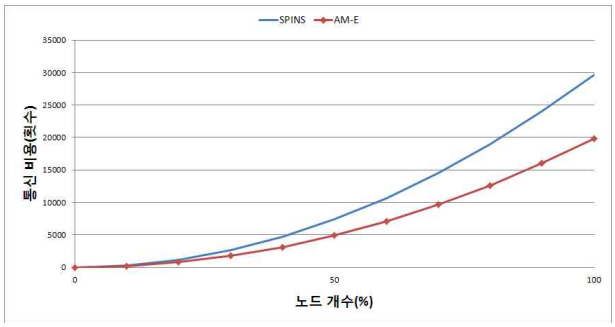

그림 7. 통신비용 결과
Fig. 7. Communication cost results.

그림 7은 AM-E 메커니즘과 SPINS[4]의 통신비용을 비교한 그래프이다. 통신에 참여하는 각 노드는 다른 노드와 풀-메시(Full-Mesh) 구성하기 위한 데이터 전송 횟수를 산출하였다.

전체 네트워크에 대한 AM-E 메커니즘의 통신비용은 약 2만 번이고, SPINS[4]는 약 3만 번인 것으로 나타났다. 즉, AM-E 메커니즘의 통신비용이 SPINS[4]보다 약 0.7% 정도 적다고 할 수 있다.

2. 보안성 분석

본 절에서는 무선 센서 네트워크의 보안요구사항과 공격 유형을 정의하고, 각각의 공격 유형에 따라 보안성을 만족할 수 있음을 증명한다.

무선 센서 네트워크의 보안요구사항으로는 데이터의 무결성 및 기밀성, 데이터와 키 정보에 대한 적시성이 있다. 데이터의 적시성을 보장하기 위해서는 현재 데이터에 대한 시간 정보와 같은 추가적인 정보를 이용하여 새로운 데이터임을 보장해야 한다. 키 정보에 대한 적시성을 보장하기 위해서는 키의 비구별성과 전방향 보안성을 만족해야 한다.

무선 센서 네트워크의 공격 유형에는 노드 간의 통신 시 데이터에 대한 공격과 베이스 스테이션까지의 데이터 전달을 방해하는 라우팅 공격으로 구분할 수 있다. 표 5는 이에 대한 공격 가능한 유형을 기술한 것이고, 표 6은 각 공격의 성공에 대한 어드밴티지(advantage) Adv 및 인시큐리티(insecurity) $INSec$를 정의하기 위한 기호이다.

정의 1. 키의 적시성 - 비구별성

노드와 베이스 스테이션 간에서 제안하는 보안기법 S에 대하여 ATKN의 Adv와 $INSec$는 아래와 같이 정의한다.

1) $Adv_S^{SPF}(ATKN, m) = \left| P\left(SPF_{atk}^{m}(1^m)\right) - P\left(SPF_{atk}^{r}(r)\right) \right|$

2) $INSec_S^{SPF}(m, r) = \max\left\{Adv_S^{SPF}(ATKN, m)\right\}$

m : 공격자 노드 $ATKN$가 생성한 임의의 메시지

r : 임의의 메시지

정리 1. 키의 적시성 - 비구별성

ATK-SPF에 대하여 $INSec_S^{SPF}(m, r) \le \varepsilon$

ε : 무시할 만큼 작은 값

증명. 제안하는 AM-E 메커니즘의 현재 키 정보는 단방향 해시 함수(hash function) H에 의해 생성된다. 따라서 해시 함수 H의 성질에 의해 입력하는 값과 상관성이 존재하지 않는 임의의 값을 출력한다.

ATK-SPF 공격의 Adv는 현재 키 정보를 알아낼 수 있는 확률과 불규칙한 메시지를 생성하여 키 정보를 알아내는 확률 값의 차이이며, 해시 함수 H의 성질에 의해 ATK-SPF의 $INSec$는 무시할 만한 값이다. 즉, 공격자 노드 ATKN가 ATK-SPF 공격에 의해 키 정보를 획득할 확률은 매우 희박하다.

표 5. 공격 유형
Table 5. Attack type.

공격 유형	설명
ATK-SPF	공격자 노드 ATKN은 베이스 스테이션이 전송하는 신호 q를 위장하여 주위의 노드에게 전송한다. 각 신호 q를 받은 노드는 이에 대한 응답으로 인증된 메시지를 공격자 노드 ATKN에게 보낼 수도 있다. 이를 통해 공격자 노드 ATKN은 현재의 키 정보 AK_i를 획득하고자 한다.
ATK-GUS	공격자 노드 ATKN은 ATK-SPF를 통하여 현재의 키 정보 AK_i를 획득하였을 때, 이후 사용될 AK_{i+1}를 알아내기 위하여 $AK_i = H\left(PK_x \oplus E_T^x\right)$가 되는 임의의 PK_x와 E_T^x를 추측하여 네트워크 전체의 키 정보를 알아내고자 시도한다.

표 6. 기호 정의
Table 6. Symbol definitions.

기호	정의
$Adv_S^{ATK}(ATKN, x)$	보안기법 S 에 대하여 공격자 노드 ATKN가 임의의 노드 x에 대해 ATK 공격에 성공할 어드밴티지
$P\left(ATK_{atk}^{x}(x)=1\right)$	임의의 노드 x에 대한 공격에 성공할 확률
$INSec_S^{ATK}(x, y)$	보안기법 S 에 대하여 임의의 노드 x, y를 가지고 ATK 공격에 성공할 최대 어드밴티지
ϵ	무시할 만큼 작은 값, $0<\epsilon<1$

정의 2. 키의 적시성 - 전방향 보안성

ATK-GUS의 어드밴티지 Adv와 인시큐리티 $INSec$는 아래와 같이 정의한다.

1) $Adv_S^{GUS}(ATKN, r, K_a) = \left| P\left(GUS_{atk}^{K_a, r}(F^{i-j}(K_a) = K_j)\right) \right|$

2) $INSec_S^{GUS}(K_a, r) = \max\left\{Adv_S^{GUS}(ATKN, r, K_a)\right\}$

K_j : 공격자 노드 $ATKN$가 획득한 현재의 키 정보

r : 임의의 메시지

K_a : 키 값

정리 2. 키의 적시성 - 전방향 보안성

ATK-GUS에 대하여 $INSec_S^{GUS}(K_a, r) \leq \varepsilon$

ε : 무시할 만큼 작은 값

증명. 정리 1에 의해 ATK-SPF에 대한 $INSec$를 p라 하면, $p < \varepsilon$이다. 또한, 임의의 메시지 r를 입력하는 값으로 하여 단방향 해시 함수를 적용하여 K_j와 일치할 $INSec$값을 q라 하면, ATK-GUS의 $INSec$은 정의에 의해 $p \cdot q$가 되며, $0 < p$, $q < 1$이므로, $p \cdot q < p < \varepsilon$이다. 따라서 $INSec_S^{GUS}(K_a, r) \leq \varepsilon$이다.

제안한 AM-E 메커니즘과 SPINS[4]는 모두 키 정보의 적시성과 전방향 보안성 기밀성을 만족시킨다. 그러나 SPINS[4]는 노드가 베이스 스테이션과 시간 동기화가 되어 있어야 한다는 것과 키 체인의 일부 노출이 전체 네트워크의 키 정보 노출이 될 수 있다는 위험성이 있다. AM-E 메커니즘은 노드의 인증 요청 메시지에 의해 노드의 개인키와 인증키를 생성함으로 SPINS[4]의 시간 동기화 문제를 해결하였다. 또한, 인증키 생성을 하기 위한 입력 값은 시간에 따른 노드의 에너지 값을 이용하도록 함으로써, 일부 키 정보의 노출이 전체 네트워크에서 사용되는 키 정보의 노출로 이어지는 것을 방지하였다.

Ⅳ. 결 론

무선 센서 네트워크는 유선 네트워크에 비해 많은 보안 취약성이 존재한다. 노드의 ID를 활용한 데이터 위변조 공격이나 공격자 노드의 라우팅 정보를 이용하여 네트워크의 정상적인 동작을 방해하는 라우팅 공격 등은 노드 인증 메커니즘을 통해 방어할 수 있다.

이를 위해 본 논문에서는 노드의 에너지 값을 이용한 AM-E 메커니즘을 제안하였다. 베이스 스테이션은 인증 요청하는 노드의 메시지를 통해 인증키를 생성한다. 인증키 생성은 노드의 ID와 현재 잔량 에너지 값을 단방향 해시 함수를 이용하여 인증비용을 줄였다. 또한 노드-to-노드 인증은 베이스 스테이션으로부터 상대 노드의 인증 정보를 요청한 후 이를 이용하여 데이터를 전송하도록 하였다. 이렇게 함으로써, 인증 절차에 따른 통신 횟수를 감소시켜 빈번한 송수신에 따른 전체 네트워크의 통신비용을 감소시켰다. 또한 수학적 분석을 이용하여 AM-E 메커니즘의 보안성을 증명하였다.

본 논문은 시간에 따른 변화는 노드의 에너지를 이용하여 안전한 노드 인증이 가능함을 보였으며, 향후 제안한 AM-E 메커니즘을 하드웨어적인 보안기법과 함께 적용함으로써 보안성이 보다 강건한 무선 센서 네트워크 구성이 가능할 것이라 기대한다.

참 고 문 헌

[1] Laurent Eschenauer and Virgil D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” in Proc. of the 9th ACM Conf. on Computer and communications security, pp. 41-47, Washington, DC, USA, Nov 2002.

[2] Haowen Chan, Adrian Perrig and Dawn Song, “Random Key Predistribution Schemes for Sensor Networks,” IEEE Symposium on Security and Privacy, pp. 197-213, May 2003.

[3] Rolf Blom, “An optimal class of symmetric key generation systems,” in Proc. of the EUROCRYPT 84 - a workshop on the Theory and Application of Cryptographic Techniques, pp. 335-338, Paris, France, Apr. 1984.

[4] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen and David E. Culler, “SPINS: Security Protocols for Sensor Networks,” *Wireless Networks Journal*, Vol. 8, no. 5, pp. 521-534, Sept 2002.

[5] Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan and Nirah K. Jha, “Analyzing the Energy Consumption of Security Protocols,” in Proc. of the 2003 international symposium on Low power electronics and design, pp. 30-35, Seoul, Korea, Aug 2003.

[6] David W. Carman, Peter S. Kruus and Brian J. Matt, “Constraints and Approches for Distributed Sensor Network Security,” NAI Labs Technical Report, Sept 2009.

저 자 소 개

김 보 승(정회원)-교신저자
2002년 영동대학교 컴퓨터공학과 공학사.
2004년 숭실대학교 컴퓨터학과 공학석사.
2005년～현재 숭실대학교 컴퓨터학과 박사과정.
<주관심분야 : 멀티캐스트, IPTV, 센서네트워크>

최 종 석(학생회원)
2010년 평생교육진흥원 컴퓨터학과 공학사.
2010년～현재 숭실대학교 컴퓨터학과 석사과정.
<주관심분야 : 네트워크보안, 센서네트워크, IPTV>

임 휘 빈(정회원)
2008년 수원대학교 컴퓨터학과 공학사.
2010년 숭실대학교 컴퓨터학과 공학석사.
2010년～현재 (주)지아이티 시스템서비스팀 연구원.
<주관심분야 : 컴퓨터통신, 센서네트워크, 보안>

신 용 태(정회원)
1985년 한양대학교 산업공학과 공학사.
1990년 Univ. of Iowa 전산학과 공학석사.
1994년 Univ. of Iowa 전산학과 공학박사.
1995년～현재 숭실대학교 컴퓨터학부 교수.
<주관심분야 : 멀티캐스트, 센서네트워크, IPTV, DRM>