센서 네트워크에서 이동성이 있는 센서 노드의 효율적인 인증 방안

정회원 손 태 식*, 한 규 석**°

Efficient Mobile Node Authentication in WSN

Taeshik Shon*, Kyusuk Han**° *Regular Members*

요 약

최근 무선 센서 네트워크 (Wireless Sensor Network)에서 Actor Network 등의 이동성이 있는 센서에 대한 연구가 매우 활발하게 진행되고 있다. 그러나 기존의 대부분의 센서 간의 인증 및 키 교환 기술에 대한 연구는 고정된 센서만 있는 환경만을 고려하고 있으며, 이동성이 있는 센서 노드가 있는 환경에 적용하는 경우 통신 및 연산 부하가 급증하기 때문에, 자원 제약이 있는 센서 네트워크 환경에서 적용하기 부적합하다. 따라서 본 논문을 통해 최초 인증 이후 재인증 시 자원 이용을 최소화 할 수 있는 이동성이 있는 센서 환경에 적합한 효율적인 센서 인증 및 키 교환 기술을 제안한다.

Key Words : Wireless Sensor Networks, Authentication, Key Exchange, Mobile Sensor

ABSTRACT

Mobility of sensor node is one of the rising issues in Wireless Sensor Networks (WSN). However, current security researches on WSN only consider static environments. Thus they are not sufficient to be deployed in the dynamic environment where the resource is limited. In this paper, we propose the efficient node authentication and key exchange protocol that reduces the overhead in node re-authentication.

Ⅰ. 서 론

무선 센서 네트워크 (Wireless Sensor Network, WSN)는 근거리 무선 통신 기능이 있고, 배터리를 통해 전력 공급을 하는 경량의 센서 간에 구성되어 있는 네트워크이다. 이런 환경에서 보안 기술은 노드의 제한된 자원을 최대한 이용할 수 있도록 하는 것을 중요한 목표로 하고 있으며, 여러 연구가 진행되고 있다.

이와 같은 기존의 센서 네트워크 인증 및 키 교환 기법은 정적 환경의 응용 분야에 치중하고 있으나, 최근 들어 WSN의 발전 및 Wireless Sensor and Actor Network (WSAN) 등의 응용 분야 확대에 따라 같은 이동하는 개체 등을 고려하는 센서 네트워크의 동적 환경에 대한 연구에 대한 필요성이 증가하고 있다.

그러나, 이러한 이동성이 있는 모바일 센서 노드의 등장에도 불구하고, 기존의 센서 네트워크 인증 및 키 교환 기술에서 노드의 이동성은 거의 고려하지 않고 있으며 한번 연결되어 인증 과정을 거친 노드가 다른 싱크에 재연결 및 재인증 과정을 거치는 경우 최초의 인증 절차를 반복하도록 하고 있다. 또한, 극히 일부의 이동성을 고려하는 노드 인증 기술은 노드 자원의 사용량이 민감한 애플리케이션에서는 적합하지 않다.

따라서, 본 논문은 센서 네트워크에서 싱크에 연

* 삼성전자 Digital Media & Communication R&D Center, Convergence S/W Lab (ts.shon@samsung.com)
** 한국과학기술원 정보통신학과 (hankyusuk@kaist.ac.kr) (° : 교신저자)
논문번호 : KICS2010-03-140, 접수일자 : 2010년 3월 31일, 최종논문접수일자 : 2010년 5월 4일

결된 이동성을 가진 노드가 이동하여 다른 싱크에 재연결되는 경우 최초 연결 시 발생하는 인증 과정보다 효율적으로 재인증을 가능하게 하기 위한 기술이다. 본 논문에서 제안한 모바일 노드의 인증 및 키 교환 기법을 이용하여 이동성을 가진 노드의 자원을 절감하면서, 센서 네트워크의 싱크의 효율적인 노드 재인증이 가능하다.

본 논문의 구성은 다음과 같다. 제 2 장에서 기존의 관련 연구를 소개 하며, 제 3 장에서 본 논문에서 제안하는 모바일 노드 인증 및 키 교환 기법에 대해 소개하고, 제 4 장에서 성능 및 안전성에 대한 분석을 기술한다. 마지막으로, 제 5 장에서 결론 및 향후 계획에 대해 기술한다.

Ⅱ. 관련 연구

종래 기술에서는 노드의 재인증에 대한 고려가 극히 드물다. 노드가 재인증되는 경우 초기 인증 과정을 동일하게 반복하게 된다.

Ibriq 등[2]은 센서 네트워크의 토폴로지 형성 단계에서 노드를 인증하는 과정의 효율성을 위해 하부 클러스터 헤드(CH)에 인증 기능을 위임하여 노드의 인증 과정에서 overhead를 분산하도록 한 인증 기법을 제안하였다. 각 CH는 사전에 노드에 대한 일부 정보에 대한 목록을 갖고 있으며, 연결되는 노드에 대해서 베이스스테이션에 요청함으로써 나머지 인증 정보를 확인 받는다.

그러나, 노드의 인증을 위해 클러스터 헤드에 노드의 일부 정보를 사전에 배포해야 하므로 네트워크상의 모든 노드에 대해 사전 정보를 저장해야 하는 전제 조건이 있으며, 노드의 신규 참여, 제거, 등을 포함하는 노드의 이동성을 고려한 노드에 대해 사용하기 적합하지 않다. 또한 센서 네트워크 토폴로지의 형성 이후 노드의 토폴로지 변경에 따른 노드 재인증에 대한 고려 역시 미비하다.

LEAP[3]과 같은 방식은 대규모 네트워크에서 효율성을 확보하기 위한 방법으로 일정 지역에 방송하는 경우 발생하는 통신 부하를 절감하기 위해 그림 1과 같이 Cluster key를 사용하는 방식이다.

이동성을 고려한 기술로 그림 2와 같은 분산 인증 기법[1]이 존재하고 있으나, 이는 모든 노드에 노드를 인증할 수 있는 정보를 분산시키고, 인증 과정에서 노드가 참여하는 과정에서 노드의 에너지 소모가 발생할 수 있다.

그림 2의 노드들 (S1, S2, 등)은 모두 동등한 성

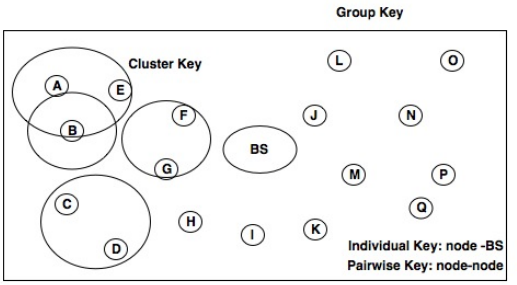

그림 1. LEAP의 키 구조

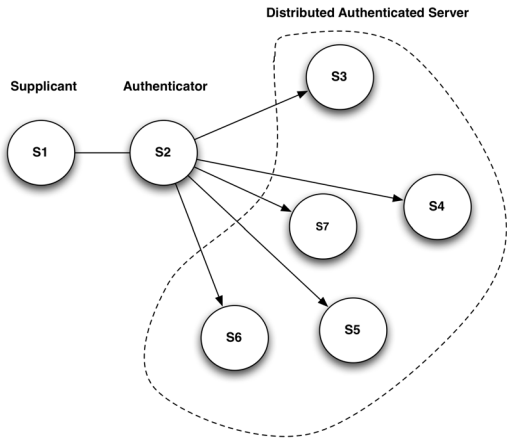

그림 2. Fantacci et al.의 센서 인증 기법[1]

능을 갖고 있으며, 서로에 대해 인증할 수 있는 정보를 일부분씩을 갖고 있다. 센서 네트워크에 참여하는 노드 (S1)은 이미 네트워크에 참여하고 있는 S2에게 인증 요청을 하고, S2는 S1의 인증을 위한 정보를 다른 노드 (S3, S4, 등)으로부터 전달받는다. 그러나 이러한 기법에서는 노드의 인증 과정에서 각 노드가 인증 과정에 참여함으로써 추가적인 overhead가 발생하는 문제점이 있다. 각 노드의 네트워크 배치 상태에 따라 노드의 인증 과정에 참여 횟수가 많은 경우가 발생할 수 있으며, 통신 overhead가 불균형적으로 발생하게 된다.

Ⅲ. 제안 기법

본 논문에서 제안하는 모바일 노드 인증 및 키 교환 기법은 그림 3과 같이 베이스스테이션, 싱크, 노드로 구성된 센서 네트워크를 배경으로 하고 있다.

그림 3에서 싱크 1과 싱크 2는 각각 네트워크 토폴로지 상에서 베이스 스테이션과 다중 홉으로 연결되어 있고, 싱크 1, 싱크 2는 서로 인접해 있다.

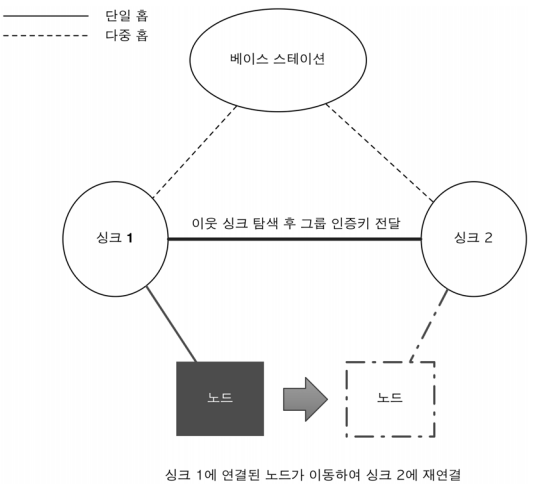

그림 3. 시스템 구성

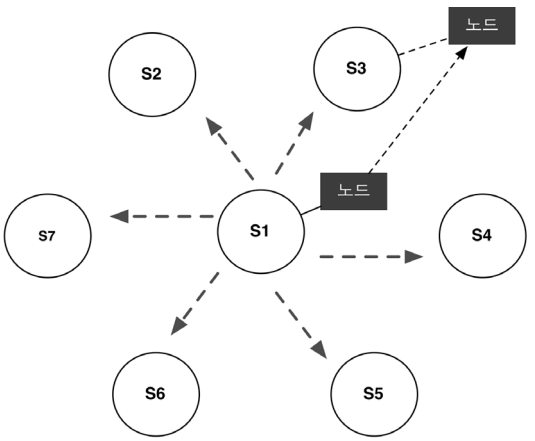

그림 4. S1에 연결된 노드가 S3와 연결되는 경우 재인증

노드는 이동성을 갖고 있으며, 싱크를 통해 센서 네트워크에 연결된다. 싱크는 노드로부터 연결 요청을 받아 노드를 인증 한 후 네트워크에 연결을 한다.

그림 4와 같이 임의의 싱크는 주변에 인접 싱크(S2, S3 등)가 있으며, 싱크에 연결된 노드가 이동하여 다른 장소로 위치가 변경될 때 인접 싱크에게 재연결된다.

각 싱크는 주기적으로 HELLO 메시지를 전송하며 노드가 이동하면서 지속적으로 인접 싱크의 HELLO 메시지를 수신하여 노드의 재인증 요청을 하게 된다.

3.1 프로토콜 세부 내용

각각의 싱크가 주기적으로 HELLO 메시지를 방송하며, 메시지를 수신한 싱크는 사전 단계로서 각

표 1. 제안 기법에 사용된 기호

기 호	설 명
$E_K(m)$	비밀키 K를 사용하여 메시지 m을 대칭키 암호화
$h(m)$	임의의 메시지 m의 해시 값
$MAC_K(m)$	K를 사용하여 m의 메시지 인증 코드(MAC) 생성
TS	타임스탬프
KDF	키 생성 함수
R	임의의 난수

싱크의 이웃 싱크와 키를 공유하고 그룹 키를 전달하게 된다. 네트워크에 추가된 노드는 최초 인증 과정 이후, 이동하여 재인증 과정을 거치게 된다. 아래 표 1은 제안 기법에서 사용한 기호에 대해서 소개하고 있다.

3.1.1 HELLO 메시지 전달

임의의 싱크 S_1은 주기적으로 난수 R_1을 생성하여 타임스탬프 TS_0와 함께 암호화하여 u_0을 생성하고, MAC(메시지 인증 코드) v_0을 생성하여 HELLO 메시지와 함께 방송한다. u_0과 v_0은 아래 식 (1)과 같다.

$$u_0 = E_{K_S}(R_1|\mathrm{TS}_0)$$
$$v_0 = MAC_{K_S}(S_1|\mathrm{HELLO}|u_0), \quad (1)$$

3.1.2 사전 단계

본 단계는 사전에 배포되어 있는 고정된 싱크들 간에 이웃 싱크를 탐색하고 상호 인증 및 키 교환을 하는 과정이다. 싱크 S_1에서 방송한 HELLO 메시지를 처음으로 수신한 S_2는 u_0과 v_0을 검증하기 위해 난수 R_2를 선택하여 메시지를 암호화하여 아래와 같이 u_1과 v_1를 생성하고 S_1의 ID와 함께 u_1, v_1, v_0을 베이스스테이션(BS)에게 전달한다.

$$u_1 = E_{K_S}(R_2|u_0)$$
$$v_1 = MAC_{K_S}(S_2|\mathrm{BS}|S_1|u_1|v_0), \quad (2)$$

BS는 $MAC_{K_S}(S_2|\mathrm{BS}|S_1|u_1|v_0)$을 생성하여 v_1의 유효성을 검사한 후 u_1을 복호화 하여 R_2를 얻고, $MAC_{K_S}(S_1|\mathrm{HELLO}|u_0)$을 생성하여 v_0의 유효성 검사를 한다. 이후 u_0을 복호화 하여 S_1이 생성한 R_1

과 타임스탬프 TS_0를 얻는다. 베이스스테이션이 TS_0의 유효 기간을 확인한 후, S_1과 공유하고 있는 키로 S_2로부터 받은 R_2를 암호화하여 u_3를 생성하고, S_2에게 R_1을 암호화하여 u_4, v_4 를 S_2에게 전달한다.

$$u_3 = E_{K_{S_2}}(S_1|S_2|R_2),\ v_3 = MAC_{K_{S_2}}(\mathrm{BS}|S_1|R_1|u_3)$$
$$u_4 = E_{K_{S_2}}(S_2|S_1|R_1|u_3|v_3),\ v_4 = MAC_{K_{S_2}}(\mathrm{BS}|S_2|R_2|u_4) \quad (3)$$

각 싱크는 생성한 SK를 사용하여 R1과 R2에 대한 MAC을 생성하고, 베이스스테이션에게 받은 암호화된 메시지 (S1과 공유된 키로 암호화된 값)와 함께 S1에게 전달한다.

S_2는 $MAC_{K_{S_2}}(\mathrm{BS}|S_2|R_2|u_4|v_3)$를 생성하여 v_4의 유효성을 검사하고, u_4를 복호화하고 R_1과 u_3, v_3을 얻는다. 이후 S_2는 KDF(키 생성 함수)에 R_1과 R_2를 입력 값으로 하여 pairwise 키 (SK)를 생성한다.

$$SK_{S_1S_2} = \mathrm{KDF}(R_1|R_2) \quad (4)$$

S_2는 이후 아래와 같이 v_5를 생성하여 u_3, v_3, v_5를 S_1에게 전송한다.

$$v_5 = MAC_{SK_{S_1S_2}}(S_2|S_1|R_2|R_1) \quad (5)$$

S_1은 $MAC_{K_{S_2}}(\mathrm{BS}|S_1|R_1|u_3)$을 생성하여 v_3의 유효성을 검사한 후 u_3을 복호화 하여 R_2를 도출한다. S_1은 식 (4)와 같이 pairwise키 $SK_{S_1S_2}$를 생성하여 v_5의 유효성을 검사 후 아래와 같이 v_6을 생성하여 ACK 메시지와 함께 S_2에게 전송한다.

$$v_6 = MAC_{SK_{S_1S_2}}(S_1|S_2|\mathrm{ACK}|R_1|R_2) \quad (6)$$

S_2가 v_6의 유효성 검사를 한 이후 S_1과 S_2 간에 $SK_{S_1S_2}$를 이용하여 보안 통신을 하게 된다.

Pairwise키가 생성된 이후 S_1 (혹은 S_2)는 그룹키(AK)를 생성하여 이웃 싱크에게 전달한다. 그룹키는 LEAP[4]에서의 클러스터 키와 유사하게 생성된다. S_1의 경우 임의의 키 AK_{S_1}와 임의의 난수 R_3를 생성한 이후, 아래와 같이 u_7, v_7을 생성하여 이웃 싱크 (S_2)에게 전송한다.

$$u_7 = E_{SK_{S_1S_2}}(AK_{S_1}|R_3),\ v_7 = MAC_{SK_{S_1S_2}}(S_1|S_2|u_7) \quad (7)$$

S_2는 v_7의 유효성을 검사한 후 u_7을 복호화 하여 AK_{S_1}과 R_3을 도출한다. 그 다음 S_2는 v_8을 생성하고 ACK 메시지와 함께 S_1에게 전송한다.

$$v_8 = MAC_{AK_{S_1}}(S_2|S_1|\mathrm{ACK}|R_3) \quad (8)$$

S_1은 v_8을 검사한 후 프로토콜을 종료한다.

3.1.3 노드 최초 인증 단계

본 단계는 임의의 노드 N이 센서 네트워크에 연결되면서 임의의 싱크 S_1에 최초 인증 요청을 하는 단계이다.

S_1이 방송한 HELLO 메시지를 처음 수신한 N은 임의의 난수 R_2를 선택하고 아래와 같이 u_1, v_1을 생성하여 S_1에게 전달한다.

$$u_1 = E_{K_N}(R_2|u_0|v_0)\ \ v_1 = MAC_{K_N}(N|S_1|u_1) \quad (9)$$

S_1은 아래와 같이 v_2를 생성하여 u_1, v_1와 함께 BS에게 전달한다.

$$v_2 = MAC_{K_{S_1}}(S_1|\mathrm{BS}|N|u_1|v_1) \quad (10)$$

BS는 v_2의 유효성을 확인한 후 v_1의 유효성을 검사한다. 이후 BS는 u_1을 복호화 하여 R_2, u_0, v_0을 각각 도출하고, v_0을 검사한 후 u_0을 복호화 하여 R_1과 TS_0을 도출한다.

BS는 아래와 같이 u_3, v_3, u_4, v_4를 각각 생성하고 u_4, v_4를 S_1에게 전송한다.

$$u_3 = E_{K_N}(R_1),\ v_3 = MAC_{K_N}(\mathrm{BS}|N|S_1|u_3)$$
$$u_4 = E_{K_{S_1}}(R_2|h(K_N|R_2)|u_3|v_3),$$
$$v_4 = MAC_{K_S}(\mathrm{BS}|S_1|N|R_1|u_4) \quad (11)$$

S_1은 v_4를 검사 후 u_4를 복호화하여 R_2< $h(K_N|R_2)$, u_3, v_3를 도출하고 $NK_N = \mathrm{KDF}(R_2|R_1)$를 생성하여 아래 식 (12)와 같이 t_1, w_1을 생성한다.

$$t_1 = E_{AK_{S_1}}(\mathrm{TS}_1|R_2|h(K_N|R_2)|NK_N),$$
$$w_1 = MAC_{AK_{S_1}}(N|t_1) \quad (12)$$

t_1, w_1은 인증 티켓으로서 인증 티켓은 노드의

아이디, 유효기간이 포함되어 있다. 이후, S_1은 아래 식 (13)과 같이 u_5, v_5를 생성한 후 u_3, v_3와 함께 N에게 전달한다.

$$u_5 = E_{NK_N}(\mathrm{TS}_1|t_1|w_1),\ v_5 = MAC_{NK_N}(S_1|N|R_2|u_5) \quad (13)$$

노드는 v_3의 유효성 확인 후 u_3를 복호화하여 R_1을 도출한다. 그 후 NK_N을 생성하여 v_5 확인 및 u_5의 복호화를 통해 TS_1, t_1, w_1을 도출한다. N은 아래 식 (14)와 같이 v_6을 생성하여 S_1에게 ACK 메시지와 함께 전달한다.

$$v_6 = MAC_{NK_N}(N|S_1|\mathrm{ACK}|R_2|R_1) \quad (14)$$

S_1은 v_6을 확인 후 N의 인증 과정을 종료한다.

3.1.4 노드 재인증 단계

최초 인증 단계 이후 노드 N이 이동하여 인접한 다른 싱크 S_2의 HELLO 메시지를 수신하고 연결되어 인증 요청하는 경우 본 단계가 시작된다.

먼저 N은 $v_1 = MAC_{NK_N}(N|S_2|t_1|w_1|v_0)$을 생성하고 t_1, w_2와 함께 S_2에게 전송한다. S_2는 AK_{S_1}을 통해 t_1, w_2를 검사하고 R_2, $h(K_N\|R_2)$, NK_N을 도출한다. S_2는 NK_N을 통해 v_1의 유효성을 검사한 후 $NK_{N^*} = \mathrm{KDF}(R_2|R_1)$을 생성하고, 새롭게 t_2와 w_2를 생성한다. $t_2 = E_{AK_{S_2}}(\mathrm{TS}_2|R_2|h(K_N|R_2)|NK_{N^*})$이며 $w_2 = MAC_{AK_{S_2}}(N|t_2)$으로 위의 식 (12)와 동일하다. 그 다음 작업으로 S_2는 $v_2 = h(NK_{N^*}|R_1)$, $u_3 = E_{NK_N}(R_1|\mathrm{TS}_2|v_2|t_2|w_2)$, $v_3 = MAC_{NK_N}(S_2|N|u_3)$을 생성하여 u_3, v_3을 N에게 전송한다. N은 v_3의 유효성을 검사한 후 u_3을 복호화하여 R_1, TS_2, t_2, w_2를 도출하고, NK_{N^*}를 생성하여 v_2의 유효성을 검사한다.

이후 N은 $v_4 = MAC_{NK_{N^*}}(N|S_2|\mathrm{ACK}|R_2|R_1)$을 생성하여 ACK 메시지와 함께 S_2에게 전송한다. S_2는 v_4의 유효성 검사 후 인증 과정을 종료한다.

Ⅳ. 성능 및 안전성 분석

4.1 성능 분석

4.1.1 제안 기법의 재인증 성능 분석

제안 기법의 성능 분석 결과 최초 인증 후 재인증 시 큰 성능 향상이 있었다. 그림 5의 경우 최초

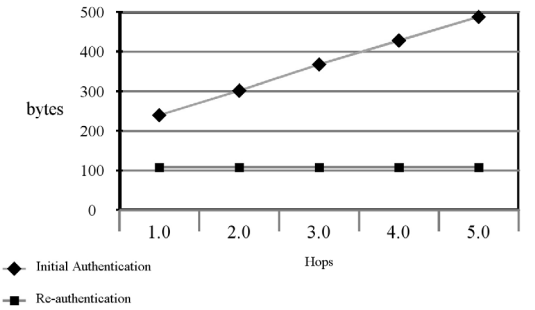

그림 5. 제안 기법의 초기 인증과 재인증 성능 비교

인증 시 노드가 연결되는 싱크와 베이스스테이션 간의 거리에 따라 요구되는 메시지 량의 크기가 크게 증가하는 것에 비해 재인증 시 베이스스테이션 간의 거리와 무관하게 일정량의 메시지 전송량을 보이고 있다. 싱크와 베이스스테이션이 5홉의 경우 약 5배 정도의 차이가 발생하였다.

4.1.2 기존 기술과 비교

표 2는 제안 기법과 기존 연구인 Fantacci et al. (2008) 기법[1]와 Ibriq 기법[2]간의 노드 재인증에 요구되는 통신 횟수를 비교하고 있다. n은 노드 갯수, t는 싱크의 갯수를 의미한다. Fantacci의 기법에서는 노드가 인증 서버 (베이스스테이션)과 인증자 (싱크)의 역할을 담당하며, 표에서는 분리하여 표기한다.

표를 통해 제안한 기법이 재인증의 경우 노드와 싱크 간에 직접 연결되는 경우 통신 횟수는 단지 3회가 되며, 기존의 다른 기법에 비해 매우 효율적임을 알 수 있다.

또한, 그림 6과 같이 기존의 기법이 재인증의 경우 초기 인증과 동일한 과정을 거치면서 싱크와 베이스스테이션 간의 거리 증가에 따라 메시지 량이 증가하는 반면에, 제안 기법은 거리와 상관없이 일정한 메시지 량을 보이고 있다. 그림 6의 결과는 Abraham 기법[4]의 메시지 크기를 기준으로 하여 MAC 크기를 4 byte로 하고, 타임스탬프의 크기를 8 byte로 설정하였다. Nonce의 크기는 8 byte, 키 크기를 16 byte로 하였다. 한편 각 노드의 ID를 1 byte로 설정하여 비교하였다.

표 2. 메시지 전송 횟수 비교

	Fantacci's	Ibriq's	제안 기법
노드	2	2n	2n
싱크	2t+1	2t	1
BS	-	2	-

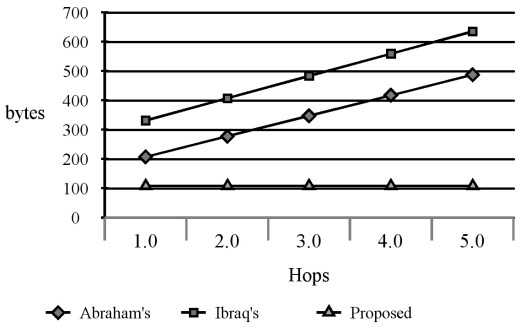

그림 6. 기존 기법과 재인증 성능 비교

4.2 안전성 분석

본 절에서 제안 기법의 안전성에 대해 간략한 분석 결과를 기술한다. 제안 기법에서 싱크와 노드 간의 키 생성은 암호화된 난수를 통해 이루어지므로, 공격자가 통신 내용을 취득하기 위해서는 암호화된 패킷을 해독할 수 있어야 한다. 또한 전송되는 메시지에 대해서는 공격자가 위변조 할 수 없으며, 각 세션 마다 nonce 사용을 통해 key freshness 검사가 가능하다. 각 전송되는 패킷에 대해 상호 인증이 이루어지며, MAC의 검사가 가능하다. 싱크나 노드가 탈취되는 경우 피해 범위는 인접 싱크에 한정되며, 전체 네트워크의 피해를 방지할 수 있다. Replay attack이나 MITM attack 등에 대해서는 공격자가 패킷을 재사용하거나 통신 정보를 변조할 수 없으므로 안전하며, DoS Attack에 대해서는 Ibriq 기법[2] 등의 방법을 통해 대응할 수 있다.

V. 결론 및 향후 계획

본 논문에서는 이동성을 가진 센서의 효율적인 재인증 기법을 제시하였다. 기존 기법의 경우 이동성에 대한 고려가 미비하여, 센서의 반복되는 인증 과정에서 매우 큰 연산 및 통신 부하를 발생시키지만, 본 논문에서 제안한 기법을 통해 최초에 인증 과정을 거친 센서의 경우, 이동 시 사전 정보를 이용하여 효율적으로 인증할 수 있도록 하였다. 제안 기법을 적용하는 경우 싱크와 베이스스테이션 간에 5홉간 거리가 있는 경우에는 5배 정도의 효율성을 얻을 수 있었다. 본 논문의 전체 내용은 [5]에서 발표되었으며 향후 계획으로 제안된 기법의 실제 환경에 적용 시 발생할 수 있는 음영 지역 문제 등에 대한 대응 방안에 대해 연구 중이다.

참 고 문 헌

〔1〕 R. Fantacci, F. Chiti, and L. Maccari, "Fast distributed bi-directional authentication for wireless sensor networks," John Wiley & Sons, Security and Communication Networks, Vol.1, pp.17-24, 2008.

〔2〕 J. Ibriq and Imad Mahgoub, "A Hierarchical Key Establishment Scheme for Wireless Sensor Networks," Proceedings of 21st International Conference on Advanced Networking and applications (AINA'07), pp.210-219, 2007.

〔3〕 S, Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large scale distributed sensor networks," ACM Trans. Sen. Netw. 2006, 2, 500-528.

〔4〕 J. Abraham, and K. S. Ramanatha, "An Efficient Protocol for Authentication and Initial Shared Key Establishment in Clustered Wireless Sensor Networks," Proc. of 3rd IFIP/IEEE International Conference on Wireless and Optical Comm. Networks, 2006.

〔5〕 K. Han, K. Kim, T. Shon, "Untraceable Mobile Node Authentication in WSN," Sensors. 2010; 10(5):4410-4429.

손 태 식 (Taeshik Shon) 정회원

2000년 2월 아주대학교 정보 및 컴퓨터공학부 학사

2002년 2월 아주대학교 정보통신공학 석사

2005년 8월 고려대학교 정보호호학 박사

2004년~2005년 Research Scholar, Univ. of Minnesota

2005년 8월~현재 삼성전자 DMC 연구소 책임연구원

<관심분야> Wireless/Mobile Network Security, Wireless Sensor Network, Anomaly Detection

한 규 석 (Kyusuk Han) 정회원

2001년 2월 홍익대학교 기계공학과 학사

2004년 8월 한국정보통신대학교 공학부 석사

2010년 8월 한국과학기술원 정보통신학과 박사

<관심분야> Wireless/Mobile Network Security, Wireless Sensor Network, Security Policy>