이종망을 고려한 무선센서네트워크에서의 다중 사용자 방송형 인증 기법*

윤성준, 이현록, 김광조
한국정보통신대학교

Multi-user Broadcast Authentication Protocol for Wireless Sensor Network under Mobile Networks

Sungjune Yoon, Hyunrok Lee, and Kwangjo Kim
Information and Communications University

요 약

무선센서네트워크는 유비쿼터스 시대를 주도할 중요한 기술 중 하나로, 네트워크를 구성하는 센서노드들의 자원 제약으로 인해, 기존의 유/무선 네트워크에 적용되는 보안기법을 그대로 적용하기에는 많은 문제점이 존재한다. 방송형 인증은 일대다 통신환경에서 사용되는 메시지 인증기법으로, 무선센서네트워크에서 가장 빈번히 사용될 보안 기법 중 하나이다. 무선센서네트워크에서 사용자는 무선센서네트워크로부터 자신에게 유용한 정보를 획득하고자 하는 사람 또는 장비로써 근래에 들어 이런 사용자는 Wibro와 같은 이종의 무선 인터넷망에 접근할 가능성이 높아지고 있다. 본 논문에서는 이러한 사용자의 이종망의 접근 가능성을 고려하여 센서노드의 자원소모를 줄여줄 수 있는 다중 사용자를 지원하는 방송형 인증 기법을 제안한다.

I. 서론

무선센서네트워크(Wireless Sensor Network, WSN)는 RFID와 함께 다가오는 유비쿼터스 시대를 선도할 중요 기술 중 하나로 많은 연구가 진행되어오고 있다. WSN은 수백에서 수천의 자원 제약적인 센서노드들과 소수의 자원이 풍부한 신뢰받는 기지국(Base Station, *BS*로 표기)으로 이루어진 무선 *Ad-hoc* 네트워크이다. 이러한 WSN은 센서노드들의 자원제약성과 비접근성(한번 배포된 이후에 관리자가 직접적으로 개별적인 센서노드에 접근하여 유지/보수 작업을 하기 어려움)으로 인해 기존에 존재하는 여러 보안기법들을 그대로 적용하기에 문제가 있어, WSN에 특화된 보안기법들을 필요로 한다.

일반적으로 센서노드들은 자신들이 수집한 데이터를 자신들의 *Ad-hoc* 망을 통하여 *BS*에게 전송하고, *BS*는 센서노드들로 전송받은 데이터를 가공하여 이를 유/무선 인터넷망을 통해 사용자(User, *U*로 표기)에게 제공을 한다. 현재까지 제안된 많은 WSN용 보안기법들은 사용자와 *BS*가 정보를 주고받는 인터넷망을 고려하지 않고, WSN의 내부적인 *Ad-hoc*망만을 고려하고 있다. 또한 *U*가 *BS*와 지리적으로 멀리 떨어져있는 경우에도 자신이 위치한 곳의 지역적인 정보를 얻기 위해 반드시 *BS*를 통해서만 이를 획득할 수 있다. 이 경우 *BS*는 *U*가 위치한 지역의 정보를 획득하기 위해 WSN에 질의 메시지를 전파해야 하며, 이 경우 *U*의 지역과 *BS* 사이에 위치한 직접적으로 연관이 없는 센서노드들의 자원을 소모시킬 수 있다.

* This work was supported by the IT R&D program of MIC/IITA. [2005-S-106-02, Development of Sensor Tag and Sensor Node Technologies for RFID/USN]

근래에 들어서 Wibro나 WiFi와 같은 무선망(Mobile Networks, MN로 표기)의 확산으로 인해 U가 위치한 지역에서 MN를 통하여 BS와 직접적인 교신이 가능할 경우가 점점 커지고 있다. 이 경우 U는 BS에게 자신의 위치 정보를 제공함으로써 자신의 주변 환경과 관련된 여러 유용한 정보를 획득할 수 있지만, BS가 보유하고 있는 정보가 최신의 정보가 아닐 경우, 최신 정보를 획득하기 위하여 BS가 추가적인 질의 메시지를 U가 위치한 지역으로 전파하게 되고, 이 경우에도 여전히 중간에 위치한 관련 없는 센서노드들의 자원을 소모하게 된다. 따라서 이런 직접적인 관련이 없는 센서노드들의 자원 소모를 완화하기 위해서, U가 직접적으로 자신의 주변 지역으로 질의를 방송할 수 있는 방법이 필요하다.

본 논문에서는 이러한 U의 MN으로의 접근 가능성을 전제로 자신의 주변 지역에 위치한 센서노드들에게 메시지를 방송하고 인증할 수 있는 기법을 제안한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 현재까지 제안된 방송형 인증 기법에 대하여 간략히 알아보고, Ⅲ장에서는 제안 기법이 고려하는 네트워크 구성 및 표기법에 대해 설명하고, Ⅳ장에서 제안기법을 설명하겠다. 끝으로 Ⅴ장에서 제안 기법의 장점을 간단히 설명하며 결론을 맺겠다.

II. 관련 연구

현재까지 제안된 방송형 인증기법은 대칭키 기반의 방송형 인증 기법(Symmetric key-based broadcast authentication protocol, SKBA)과 비대칭키 기반의 방송형 인증 기법 (Asymmetric key-based broadcast authentication, AKBA)으로 나눌 수 있다. SKBA 기법들은 소수의 BS가 방송형 인증을 효율적으로 수행하기 위하여 해쉬 기반의 메시지 인증 코드 (Message Authentication Code, MAC)와 같은 대칭키 기반의 암호화 기법만을 사용하여 전파되는 메시지를 인증하는 기법으로, 효율적이지만 다수의 사용자를 지원하기에는 센서노드의 제한적인 메모리로 인해 부적합하다.[1,2] AKBA 기법들은 다수의 사용자들을 지원하지만, 비 대칭키 연산이 센서노드에 적용되기에는 아직 소모되는 에너지 측면에서 부적절하다.[3]

III. 네트워크 가정 및 표기법

본 논문에서 다루는 네트워크는 <그림 1>과 같이 구성되며, WSN은 MN의 영역안에 존재한다. 그러나 센서노드의 자원 제약 및 상이한 무선 주파수로 인해 BS만이 유/무선 인터넷을 통해 MN과 연결되어있다. 즉, U는 Access Point (간단히 AP라고 함)등과 같은 장치를 통해 MN에 접근하여 BS와 직접적인 통신이 가능하며, 자신과 인접한 센서노드들과도 무선으로 통신이 가능하다.

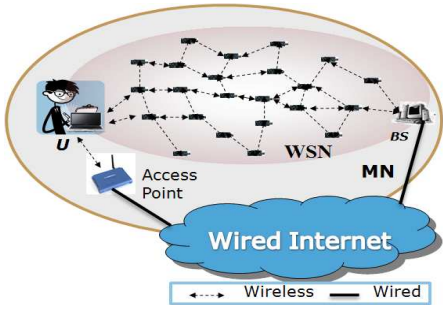

그림 1: 연구 논문에서 다루는 네트워크 구성

<그림 2>는 WSN의 내부 구성을 보여준다. 그림에서와 같이 WSN은 $N \times N$ 클러스터(Cluster, i번째 클러스터는 C_i로 표기)로 나누어지며, 각 C_i에는 이를 관리하는 하나의 관리노드(Manger node of C_i, M_i로 표기)와 다수의 일반적인 센서노드(Sensor node, C_i에서 m번째 센서노드는S_m^i로 표기하며, $|C_i|$는 C_i에 존재하는 S_m^i의 수를 나타냄)들이 존재한다. 모든 M_i는 노드포획 공격을 방지하기 위해 tamper-resistance 장비를 장착하고 있다. M_i는 C_i 내부적으로 메시지를 방송하기 위해 고유한 방송형 인증 기법을 가지고 있다. 제안기법에서는 μTESLA[2]를 사용한다고 가정한다. 즉 각 M_i는 임의 수 HK_q^i를 생성하고 이를 다음과 같이 반복적으로 해쉬하여,$HK_x^i = h(HK_{x+1}^i)$, $x = q-1,...,0$, 해쉬 키 체인을 생성한다. HK_0^i는 모든 S_m^i가 저장하고 있고, M_i가 방송하고자하는 메시지는 HK_x^i $(1 \le x \le q)$를 이용하여 MAC를 생성하여 메시지와 함께 보내고 HK_x^i를 이후 공개한다. 모든 센서노드들은 $HK_0^i = h(HK_x^i)^x$를 이용하여 HK_x^i를 인증하고 이를 다시 MAC를 인증하는데 사용한다. 각 S_m^i는 자신과 인접한 노드들과 대칭

키를 공유하고 있으며, 이를 이용하여 M_i에 메시지를 안전하게 전송할 수 있는 라우팅 알고리즘이 존재한다. WSN에 속하는 모든 노드들은 BS와 자신들과의 고유한 대칭키 $K_{BS,X}$ ($X \in M_i \cup S_m^i, 1 \le i \le N^2$)를 가지고 있다. <표 1>은 앞으로 사용할 추가적인 기호들을 요약하였다.

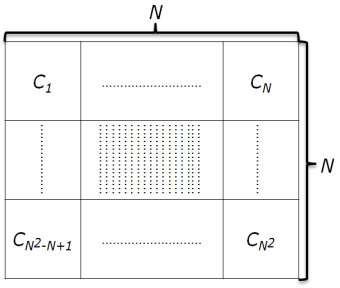

그림 2: $N \times N$ 클러스터로 나눠진 무선센서네트워크

표 1: 표기법

기호	설명
X, Y	$X, Y \in (U \cup S_m^i \cup M_i \cup BS)$, $where 1 \le i \le N^2$ and $1 \le m \le \lvert S_i \rvert$
ID_X	X의 ID
A_U	U의 WSN에서의 통신반경
R_X	X가 생성한 무작위 수
t_X	X의 현재 시간
$K_{X,Y}$	X와 Y가 공유한 대칭키
$T_{X,Y}$1]	BS가 발급한 X와 Y간의 티켓
HK_x^i	x번째 해쉬 값, 메시지 인증코드 생성 시 키로 사용
$E_{K_{XY}}(msg)$	$K_{X,Y}$로 암호화한 msg
$MAC_{HK_x^i}(msg)$	HK_x^i를 이용해 생성된 메시지 인증 코드
$\rightarrow$	일반 통신채널
$\Rightarrow$	보안채널
$X \Leftrightarrow Y$	X와 Y간의 보안채널

Ⅳ. 제안 기법

1] $T_{X,Y} = E_{K_{BSY}}(h(ID_X, R_X), t_E, K_{X,Y})$, 이때 t_E는 티켓의 만료시간을 나타낸다.

제안 기법은 크게 BS와 보안채널 생성, S_m^i와 보안채널 생성, M_i와 보안채널 생성, M_i를 통한 메시지 방송의 4단계로 나누어진다. <그림 3>은 제안기법의 전체적인 흐름을 보여준다.

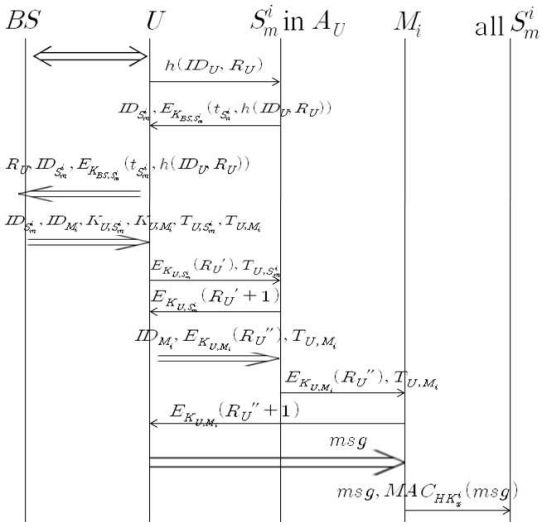

그림 3: 제안기법

1. BS와 보안채널 생성

사용자는 MN을 이용하여 BS와 보안채널을 생성한다.

1) $BS \Leftrightarrow U$

2. S_m^i와 보안채널 생성

사용자는 우선 임의의 수 R_U를 생성하여 ID_U와 함께 해쉬하여 이를 자신의 주변지역으로 전파한다.

2) $U \rightarrow A_U$: $h(ID_U, R_U)$

위의 메시지를 수신한 $S_m^i \in A_U$는 K_{BS,S_m^i}로 자신의 현재시간과 기 수신한 메시지를 암호화하여 $ID_{S_m^i}$와 함께 U에게 전송한다.

3) $S_m^i \rightarrow U$: $ID_{S_m^i}, E_{K_{BS,S_m^i}}(t_{S_m^i}, h(ID_U, R_U))$

U는 3)을 통해 전송받은 메시지 중 가장 수신감도가 좋은 메시지 하나를 선택하여 BS에게 전송한다.

4) $U \Rightarrow BS$: $R_U, ID_{S_m^i}, E_{K_{BS,S_m^i}}(t_{S_m^i}, h(ID_U, R_U))$

BS는 $ID_{S_m^i}$를 이용해 복호화에 사용할 키 K_{BS,S_m^i}를 찾아 $E_{K_{BS,S_m^i}}(t_{S_m^i}, h(ID_U, R_U))$을 복호화한다. 이후 $t_{S_m^i}$가 유효한지를 확인한 후 R_U와 ID_U를 해쉬하여 복호화 된 값과 비교한다. 비교 결과 동일한 경우, K_{U,S_m^i}, K_{U,M_i}, T_{U,S_m^i}, 와 T_{U,M_i}를 생성하여$ID_{S_m^i}$와 ID_{M_i}와 함께 U에 전송한다.

5) $BS \Rightarrow U$: $ID_{S_m^i}, ID_{M_i}, K_{U,S_m^i}, K_{U,M_i}, T_{U,S_m^i}, T_{U,M_i}$

U는 임의의 수 $R_U{}'$를 생성K_{U,S_m^i}로 암호화하여 T_{U,S_m^i}와 함께 S_m^i에 전송한다.

6) $U \rightarrow S_m^i : E_{K_{U,S_m^i}}(R_U{}'), T_{U,S_m^i}$

S_m^i는 우선 T_{U,S_m^i}를 복호화하여 키 K_{U,S_m^i}를 추출하여 유효성을 검증 한 후, 이 키를 이용하여 $R_U{}'$를 복원한다. 이후 $R_U{}'$+1을 K_{U,S_m^i}로 암호화하여 U에게 전송한다.

7) $S_m^i \rightarrow U$: $E_{K_{U,S_m^i}}(R_U{}'+1)$

U는 $E_{K_{U,S_m^i}}(R_U{}'+1)$을 복호화하여 $R_U{}'$+1과 같은지 검증하고 S_m^i와 보안채널 생성을 완료한다.

3. M_i와 보안채널 생성

U는 임의의 수 $R_U{}''$를 생성 후 암호화하여 $E_{K_{U,M_i}}(R_U{}'')$을 생성 후 S_m^i과의 보안채널을 통해 ID_{M_i}와 T_{U,M_i} 함께 전송한다.

8) $U \Rightarrow S_m^i : ID_{M_i}, E_{K_{U,M_i}}(R_U{}''), T_{U,M_i}$

S_m^i는 U를 대신하여 $E_{K_{U,M_i}}(R_U{}''), T_{U,M_i}$를 M_i에게 전송한다.

9) $S_m^i \Rightarrow M_i$: $E_{K_{U,M_i}}(R_U{}''), T_{U,M_i}$

M_i는 T_{U,M_i}를 복호화하여 키 K_{U,M_i}를 추출하여 유효성을 검증 한 후, 이 키를 이용하여 $R_U{}''$를 복원한다. 이후 $R_U{}''$+1을 K_{U,M_i}로 암호화하여 S_m^i에게 전송한다.

10) $M_i \Rightarrow S_m^i$: $E_{K_{U,M_i}}(R_U{}''+1)$

S_m^i는 이를 U에게 전달하고, U는 $E_{K_{U,M_i}}(R_U{}''+1)$을 복호화 한 값을 $R_U{}''$+1과 검증하여 M_i과의 보안채널을 생성을 완료한다.

4. M_i를 통한 메시지 방송

이후 M_i와 생성된 보안채널을 통해 방송하고자 하는 메시지를 전송하고, M_i는 자신의 방송형 인증 기법, 즉 μTESLA,을 이용하여 이를 C_i 내의 모든 센서노드에게 전파한다.

11) $U \Rightarrow M_i$: msg

12) $M_i \rightarrow S_m^i$: $msg, MAC_{HK_x^i}(msg)$

Ⅴ. 결론

본 논문에서는 사용자의 이종망 접근가능성을 전제로 WSN에서 사용자가 위치한 지역의 클러스터 내부로 메시지를 효율적으로 전파할 수 있는 기법을 제안하였다. 본 기법에서는 사용자의 실제 ID를 임의의 수와 해쉬하여 그 값을 임시 사용자 ID로 사용함으로 기지국 이외에는 실제 사용자를 확인할 수 없게 하여 사용자의 프라이버시를 보호한다. 또한, 사용자가 위치한 클러스터의 관리노드를 통해 사용자의 메시지를 전파함으로써 기지국과 사용자 영역 이외의 센서노드들의 자원소모를 제거하였다. 추후 연구에서는 제안 기법의 안전성 및 효율성을 면밀히 분석하고 기존의 기법들과 비교 분석을 수행하고자 한다.

참고문헌

[1] J. Drissi and Q. Gu. Localized broadcast authentication in large sensor networks. In Proceedings of International Conference on Networking and Services, July 2006.

[2] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar. Spins: Security protocols for sensor networks. In Proceedings of 7th Annual International Conference on Mobile Computing and Networks, July 2001.

[3] K. Ren, W. Lou, and Y. Zhang. Multi-user broadcast authentication in wireless sensor networks. In Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, June 2007.