무선 센서 네트워크에 적용되는 방송형 인증 기법의 조사 분석*

윤성준, 이현록, 김광조
한국정보통신대학교

Survey and Comparison of Broadcast Authentication Protocols for Wireless Sensor Networks

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

요 약

무선 센서 네트워크 (WSN)에서 방송형 (broadcast) 인증 기법은 네트워크 전역에 걸친 안전한 메시지 전파 (소프트웨어의 갱신, 네트워크 질의 등)를 위한 보안 기법이다. WSN은 수백에서 수천 개의 자원 제약적인 소형의 센서 노드들로 이루어진 Ad-hoc 네트워크로써, 기존의 모바일 Ad-hoc 네트워크와 많은 유사점을 가진다. 하지만 기존의 유/무선 인터넷 또는 Ad-hoc 네트워크를 위해 제안된 방송형 인증 기법들은 극심한 자원 제약 및 대규모의 네트워크 특성을 가진 WSN에 그대로 적용될 수 없다. 본 논문에서는 현제까지 제안된 WSN을 위한 방송형 인증 기법을 조사하고, 앞으로의 연구 방향을 제시하고자 한다.

ABSTRACT

In wireless sensor networks (WSNs), broadcast authentication is one of the most important security protocols for secure network-wide software updates, queries, commands, and messages dissemination. However, existing broadcast authentication protocols widely used in wired Internet or mobile ad-hoc networks are impractical due to the very limited resources and the large-scale deployment of sensor nodes. To cope with these problems, many researchers have heavily investigated how to minimize the computation, communication and storage overheads of sensor nodes. In this paper, we provide an overview of broadcast authentication and present new research direction toward broadcast authentication especially for WSNs.

Keywords : 무선 센서 네트워크, 방송형 인증

Ⅰ. 서 론

무선 센서 네트워크 (Wireless Sensor Network, WSN)는 유비쿼터스 시대를 앞당길 가장 핵심적인 기술 중 하나이다. WSN은 수백에서 수천 개의 자원 제약적인 소형의 센서 노드들과 소수의 안전하고 자원이 풍부한 기지국으로 구성된 무선 Ad-hoc

* 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]

네트워크로써 각각의 센서 노드들은 자신의 주변 환경 데이터를 획득하고 정제하여 이를 기지국에 제공한다. 기지국은 센서 노드들로부터 획득한 데이터를 보다 유용한 정보로 가공하여 이를 필요로 하는 사용자들에게 제공한다. 기존의 유/무선 네트워크 (인터넷, 모바일 Ad-hoc 네트워크)와는 다르게, WSN은 자동화된 원격 데이터 획득을 위해, 전장 감시에서 빌딩 관리 응용에 이르기까지 다양한 분야에서 연구가 수행되어오고 있다.[1] 그림 1은 기본적인 WSN 구성을 보여준다.

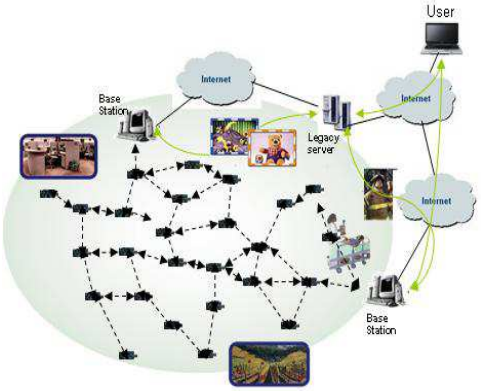

그림 1. 무선 센서 네트워크

WSN은 기존의 Ad-hoc 네트워크와 많은 유사점을 가지고 있지만 센서 노드들이 Ad-hoc 네트워크에서 고려되는 무선 단말에 비해 보다 자원 제약적이며, 네트워크의 규모가 훨씬 크다는 차이점을 가지고 있다. 따라서 무선 Ad-hoc 네트워크를 위해 고안된 보안 기법들을 WSN에 직접 적용되기에는 많은 문제점이 존재한다.[2]

WSN에서 방송형 인증은 네트워크 전체적으로 확산되는 소프트웨어의 갱신, 질의 등의 메시지를 센서 노드가 효율적으로 인증하기 위한 기법이다. 초기에 제안된 방송형 인증 기법들은 주로 비밀키 암호화 시스템 (Secret Key Cryptosystem, SKC)에 기반을 두어 설계되었으며, 소수의 송신자 (주로 기지국)만을 지원한다. 최근에는 다수의 송신자 (모바일 유저)를 지원하기 위해 공개키 암호화 시스템 (Public Key Cryptosystem, PKC)을 이용한 기법들이 제안되고 있다.

본 논문에서는 현재까지 제안된 WSN에 특화된 방송형 인증 기법을 알아보고, 앞으로의 연구 방향을 제시하고자 한다. Ⅱ에서는 여러 기법들에서 사용된 기본적인 기술에 대해 알아보고, Ⅲ에서 현재까지 제안된 기법 중 10가지 주요 기법에 대해 간략히 살펴보겠다. Ⅳ에서는 이를 통합적으로 비교 분석하고, Ⅴ에서 결론 및 앞으로의 연구 방향을 제시한다.

Ⅱ. 기초 지식

본 단원에서는 여러 방송형 인증 기법들에서 사용된 기본 기술에 대해 설명한다.

1. 일방향 해쉬 체인

일방향 해쉬 체인 (One-way Hash Chain, OHC)은 일방향 해쉬, $H()$,를 반복 적용하여 생성한 체인이다.[5] 즉, 임의의 값 K_m을 생성한 후, $K_i = H(K_{i+1})$, $i = m-1,...,0$ 을 이용하여 완전한 해쉬 체인을 구성한다. 체인을 생성한 주체를 제외하고는 $H(K_x), 0 \le x \le i$로부터 K_i를 구하는 것이 해쉬 함수의 일방향성으로 인해 산술적으로 불가능하다. OHC는 메시지 인증 코드 (Message Authentication Code, MAC) 계산에 키로 사용되며, 방송형 인증을 시작하기 위해 송신자는 초기 키 K_0를 모든 수신자에게 안전하게 전송한다. 메시지를 전파하기 이전에 송신자는 아직 노출되지 않은 체인의 키 $K_i(i > 0)$ 를 사용하여 MAC을 생성하고 해당 메시지를 MAC과 함께 전파하게 된다. 이후 송신자는 K_0에 의해 인증될 키를 전파하게 되는데, 3.1.1절에서 상세히 기술할 것이다. 대부분의 OHC 기반의 방송형 인증 방식은 한 메시지 당 하나 혹은 두 개의 해쉬 값이나 MAC 값을 가지게 되어 통신량이 적다. 하지만 해당하는 키들이 노출되기 전까지 메시지 인증은 지체되게 된다.

2. 머클 해쉬 트리 (Merkle Hash Tree, MHT)

MHT는 데이터 블록의 해쉬 값들로 구성된 말단 노드들을 순차적으로 해쉬하여 생성된

이진트리이다.[9] 트리의 중간 노드들은 자신들의 자식노드들을 해쉬한 값으로 이루어지며, 데이터 블록을 전파하기 전에 송신자는 MHT의 정점 노드 값을 모든 잠재적인 수신자들에게 안전하게 전송하여야 한다. 다른 데이터 블록을 알지 못하더라도 해당 데이터 블록으로부터 정점 노드 값을 다시 생성할 수 있도록 해주는 부가적인 인증 정보 (Auxiliary Authentication Information, AAI)를 첨부하여 송신자는 데이터 블록을 전파하게 된다. 그림 2는 MHT의 예제를 보여준다. $< n_1,...,n_4 >$ 중 한 값을 전송하기 위해 송신자는 사전에 h_{1-4}를 모든 수신자에게 안전하게 분배한다. n_1을 전파 할 때, 송신자는 h_2와 h_{3-4}를 동시에 보내게 되는데 이는 n_1의 AAI이다. 모든 수신자들은 값을 수신한 즉시 h_{1-4}가 $H(H(H(n_1)||h_2)||h_{3-4})$와 동일한지 여부를 검사하여 n_1을 인증하게 된다. 따라서 MHT는 적은 메모리양으로 즉각적인 메시지 인증을 제공할 수 있지만, MHT의 깊이에 따라 통신량이 점점 커지는 단점이 존재한다.

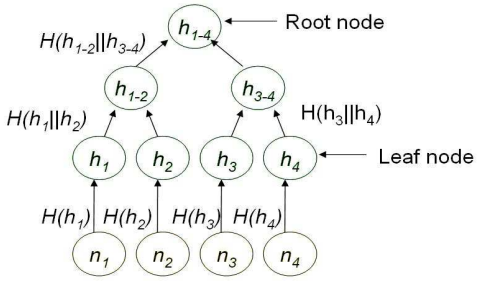

그림 2. 머클 해쉬 트리

3. 블룸 필터 (Bloom Filter, BF)

블룸 필터는 저장 공간의 효율성이 높은 자료 구조로, 집합 $S=< E_1,...,E_m >$상의 개체 E_i를 검사하기 위하여 m-비트 벡터 $V[m]$과 서로 다른 k개의 해쉬 함수 $H_1(),....,H_k()$를 사용한다. 이때 해쉬 함수들의 출력 값은 0에서 $m-1$ 사이의 값을 가지게 된다. 블룸 필터는 $V[H_j(E_i)]$ (이때 $i=1,...,m$ 이고, $j=1,...,k$),를 1로 설정하여 생성된다. 개체 E_x가 S에 속한 개체인지를 검증할 경우에는 $V[H_j(E_x)]$, $(j=1,...,k)$의 값이 1과 동일한지 검사하여 이루어진다. 만약 이 값 중 어느 하나라도 0이면 E_x는 S에 속해 있지 않다는 것을 나타낸다. 그림 3은 블룸 필터의 예를 보여주는데, 해당 필터를 활용 시 적은 메모리와 작은 연산량을 가지는 장점이 있는 반면, 작은 확률이긴 하지만 개체 $E_i^{'}$가 S에 속해있지도 않는데 해당 집합의 원소로 여겨지는 긍정 오류 (False Positive Ratio, FPR)가 나타날 가능성이 존재한다. FPR은 블룸필터의 사용자의 수 (집합 S의 크기)를 제한하거나 m-비트 벡터의 크기를 증가 시킬 수 있다.

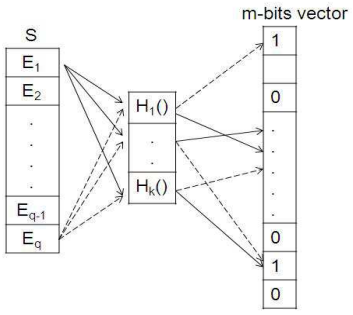

그림 3. 블룸 필터

Ⅲ. 무선 센서 네트워크에 적용 가능한 기존의 방송형 인증 기법

본 단원에서는 현제까지 제안된 WSN에 특화된 방송형 인증기법들에 대해 간략히 소개한다. 일반적으로 보안 기법들은 공개키 기반 기법과 비밀키 기반 보안 기법으로 분류할 수 있다. 이는 방송형 인증기법에서도 마찬가지로 적용될 수 있다.

일반적으로 비밀키 기반 방송형 인증 기법 (Secret Key-based Broadcast Authentication, SKBA)들은 통신량 및 연산량 측면에서 효율적이지만, 다수의 송신자를 지원하기 힘들다. 이는 각 송신자의 방송매개변수들이 모든 센서 노드에 저장되어야하기 때문이다.[1] 공개키 기반 기법 (Public

1) 센서 노드는 일반적으로 매우 작은 공간만을 이러한 매개변수를 저장하는데 사용할 수 있다.

Key-based Broadcast Authentication, PKBA)들은 통신량 및 연산량 측면에서 SKBA 보다 효율성이 떨어지지만, 다수의 송신자를 효율적으로 지원할 수 있다.

1. 비밀키 기반 방송형 인증 (Secret Key-based Broadcast Authentication, SKBA)

1.1. μTESLA

WSN을 위한 최초의 방송형 인증 기법으로 송신자와 수신자간의 시간 동기화를 요구한다.[10] 센서 노드가 응용 영역에 배치되기 전에, 기지국은 네트워크 운용 예상 시간 (t_m)을 균일한 시간 단위 (t_{INT})로 분할한다. (t_m /t_{INT} = m). 이후 임의의 값 K_m을 생성하고 이를 반복적으로 해쉬하여 OHC를 생성하고 ($K_i = H(K_{i+1})$, i는 $m-1$에서 0 사이의 값), 키 공개 스케줄 d (1보다 큰 정수)를 결정한다. 그 후 t_{INT}, d, K_0를 모든 센서노드에게 안전한 통신 채널을 통해 전달하고 센서 노드들을 실제 응용 영역에 배치한다. 이후 기지국은 키 공개 스케줄에 따라 키를 순차적으로 공개하고, 이 키를 이용하여 센서 노드들은 기지국이 보낸 메시지를 검증한다.

그림 4는 기본적인 μTESLA 구조를 보여준다. 시간 단위 i안에서 전파되는 메시지 M_{j+1}과 M_{j+2}는 각각 $MAC(K_i, M_{j+1})$과 $MAC(K_i, M_{j+2})$와 함께 전송되며, 시간 단위 $i+d$에서 기지국은 키 K_i를 공개한다. K_i를 받은 센서 노드들은 이를 이용하여 메시지 M_{j+1}과 M_{j+2}을 검증한다. 키들이 자신들의 생성 방향과 반대로 공개되므로, OHC를 생성한 기지국 이외에는 이 후에 공개될 키 값을 알 수 없으므로, 메시지를 중간에 변조할 수 없다.

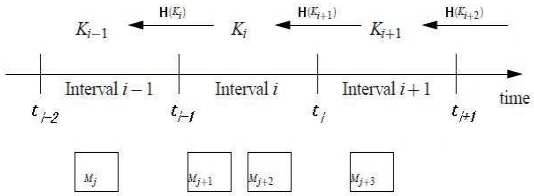

그림 4. μTESLA[10]

1.2. 다중 계층 μTESLA (Multi-level μTESLA, M-TESLA)

M-TESLA는 OHC의 수명을 연장 및 단대단 통신에 기반한 방송매개변수 배포 문제를 해결하기 위하여 μTESLA를 확장한 기법으로, 기본 아이디어는 μTESLA를 다중 계층으로 배치하는 것이다.[6] 상위 계층의 μTESLA는 하위 계층의 μTESLA에서 사용되는 매개변수를 인증하기 위해서만 사용되며, 실제 메시지는 최하위 계층의 μTESLA에 의해서 인증이 이루어진다. 이 기법은 기존의 μTESLA가 가지는 단대단 통신에 기반한 방송매개변수 배포 문제 및 몇 가지 DoS 공격을 해결하였지만, 상위 계층의 μTESLA를 대상으로 한 DoS공격에 취약하다는 단점을 가지고 있다.

1.3. 머클 해쉬 트리 기반 μTESLA (Merkle hash tree-based μTESLA, T-TESLA)

T-TESLA는 μTESLA 방송매개변수의 즉각적인 인증을 위한 기법이다.[7] M-TESLA는 하위 계층의 μTESLA 매개변수들을 인증하기 위해, 센서 노드들이 상위 계층의 μTESLA에서 사용되는 키가 공개되기를 기다려야하며, 이를 겨냥한 DoS 공격에 취약하다는 단점을 가지고 있다. 이러한 공격의 위험성을 제거하기 위해, 센서 노드들은 자신들이 전송받은 방송매개변수를 즉각적으로 인증해야한다. T-TESLA는 MHT를 이용하여 센서 노드들이 제공받은 매개변수들을 즉시에 인증하는 방법을 제공한다. 기지국은 앞으로 사용될 모든 μTESLA 방송매개변수들

을 생성하고, 각 매개변수들의 해쉬 값을 말단 노드로 하는 MHT를 구축한다. 구축된 MHT의 정점 노드는 모든 센서노드들에게 안전한 채널을 이용하여 전송되고, 이를 이용하여 각각의 μTESLA 매개변수들을 즉시에 인증하게 된다.

그림 5는 8개의 μTESLA 매개변수를 가지는 MHT를 보여준다. 정점 노드 K_{18}은 모든 센서 노드들에게 안전한 채널을 이용하여 전송되어 있다고 가정한다. S_3 μTESLA 매개변수를 사용하기 위하여 기지국은 S_3와 함께 AAI (이 경우 K_4, K_{12}, K_{58})를 전파한다. 해당 정보를 수신 받은 센서 노드들은 K_{18}의 값과 $H(H(K_{14}, H(H(S_3), K_4)), K_{58})$를 비교하여 두 값이 같다면 S_3를 올바른 μTESLA 매개변수로 인증하게 된다. T-TESLA는 매개변수의 즉시 인증을 통해, M-TESLA의 문제점을 제거하였지만, 즉시 인증을 위해 추가적인 통신량 (AAI)을 필요로 한다.

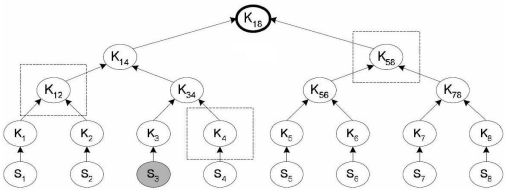

그림 5 T-TESLA[7]

1.4. 지역화 된 μTESLA (Localized μTESLA, L-TESLA)

μTESLA는 네트워크의 규모가 커지면, 인증 지연 시간[2] 역시 증가한다. 이를 해결하기 위해 L-TESLA는 네트워크를 다수의 클러스터 (cluster)로 나누어 방송형 인증이 각 클러스터 내부적으로 수행되도록 하여, 각 센서 노드에서의 인증 지연 시간을 감소 시켰다.[3] 이를 위해서 각 클러스터에는 일반적인 센서 노드보다 안전하고, 연산능력이 뛰어난 클러스터 헤드 노드 (Cluster Head node, CH)가 필요하고, 이 헤드 노드들이 자신의 클러스터 안에서 지역적인 메시지 방송을 수행하게 된다.

2) 각각의 센서 노드가 방송된 메시지를 받은 시간과 이 메시지를 인증한 시간의 차.

1.5. 규칙적이고 예상 가능한 방송 시간을 고려한 μTESLA (Regular and Predictable Time μTESLA, RPT)

RPT는 정기적이고 예측 가능한 시간에 방송되는 메시지를 즉시 인증하기 위하여 μTESLA를 수정한 것으로, 송신자는 어떤 메시지를 언제 보낼지 알고 있고 모든 센서 노드 역시 이를 알고 있다는 가정을 하고 있다.[8] 미리 결정된 시간, 즉 송신자와 수신자들이 매시지를 송수신하기로 예상된 시간, T_r에서 메시지를 방송하기 전에, 송신자는 메시지의 MAC 값을 계산하고, $T_r - D$ (D는 네트워크 전송 지연) 시점에 MAC 값을 방송하게 된다. T_r 시점에 모든 센서 노드들은 MAC을 수신하게 되고, 송신자는 MAC에서 사용될 키와 함께 메시지를 전파하게 된다. $T_r + D$ 시점에서는 모든 센서 노드들이 메시지를 검증할 수 있지만 해당 방식은 DoS 공격에 취약하다.

1.6. 배치 기반 방송형 인증 기법 (Batch-based Broadcast Authentication, BABRA)

인덱스 (index) 값을 통해 시간 동기화의 필요성을 제거한 방식으로, μTESLA와 그 변종에서 필요한 키들의 OHC를 제거하여 무한의 방송 시간을 지원한다.[15] BABRA에서는 메시지들이 패킷들의 집합 (배치)으로 구성되어 일괄적으로 전송되며, 방송형 인증을 시작하기 위해 송신자는 제일 처음 배치작업에 사용되는 키의 해쉬 값을 안전하게 분배해야 한다.

그림 6은 해당 방식의 개요를 보여준다. 한 배치 내의 모든 패킷들은 이전 배치 혹은 시작단계에 분배된 키의 해쉬 값으로 계산된 MAC 값을 가지고 있으며, 다음 배치 작업에 필요한 키의 해쉬 값은 C 시간단위 (Batch Period, BP)내에 보내지게 된다. 해당 시간이 끝나는 시점에서 송신자는 지연 시간 (Delay

Period, DP)을 위한 타이머를 동작시킨다. BP와 DP 중에는 배치키가 송신자에 의해 안전하게 유지된다. DP 타이머가 끝나게 될 때, 송신자는 대응하는 배치키를 노출하는데 이에 해당하는 시간을 KP (Key disclose Period)라 한다. 센서 노드가 배치의 첫 번째 패킷을 받았을 때, 타이머를 C 시간단위로 설정하여 동작시키고 해당 시간동안 받은 패킷들만 정상적으로 처리를 하게 된다. C 시간 단위가 종료되면 센서 노드는 지연 시간을 위한 새로운 타이머인 D를 동작시키고, 해당 시간 후에는 버퍼에 저장된 배치 패킷들의 인증을 위한 키를 받게 된다.

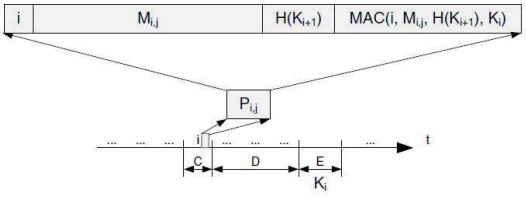

그림 6. BABAR[15]

2. 공개키 기반 방송형 인증 (Public Key-based Broadcast Authentication, PKBA)

센서 노드의 점진적인 성능 향상으로 인해서, PKC가 센서 노드의 중요 보안 기법들에서 사용되는 사례가 증가하고 있다.[4, 11, 14] PKC를 사용함으로써 얻을 수 있는 이점으로써, 단순화된 프로토콜의 설계 및 즉시 인증이 가능 하다는 점을 들 수 있다. 본 소 단원에서는 PKC에 기반을 둔 방송형 인증 기법들에 대해 간략히 소개한다.

2.1. 인증서 기반 PKBA (Certificate-based broadcast Authentication Scheme, CAS)

CAS는 기존의 전자 서명 기법과 거의 모든 점에서 동일하다.[13] 유일한 차이점으로, CAS는 통신량을 감소시키기 위해서 인증서의 크기를 최소화했다.[3] 메지지를 전파하기 위해 각 송신자들은 사전에 기지국으로부터 자신들의 공개/비밀키 쌍 및 인증서를 제공받아야한다. 이를 제공받은 송신자는 전파 할 메시지의 서명을 생성하여, 메시지, 인증서와 함께 전파한다. 방송된 메시지를 수신한 센서 노드들은 먼저 인증서를 검증한 후 송신자의 공개키를 추출하며 이를 이용하여 서명을 검증하게 된다. CAS는 각 센서 노드에서 2번의 서명 검증 연산을 요구하고, 추가적으로 인증서 폐기 리스트 (Certificate Revocation List, CRL)를 저장할 공간을 요구한다. 따라서 CAS는 인증서가 빈번히 폐기되는 환경에서는 적합하지 않다.

2.2. 머클 해쉬 트리 기반 PKBA (Merkle hash tree-based broadcast Authentication Scheme, MAS)

MAS는 CAS에서 요구되는 CRL의 필요성을 제거하고, 인증서 검증에 소요되는 PKC 연산을 MHT를 이용한 소수의 해쉬 연산으로 대체하여 센서 노드에서 요구되는 메모리 및 연산량을 감소시켰다.[13] 그러나 MHT로 인해, 송신자의 수가 증가 할수록 추가적으로 전송해야하는 AAI의 크기가 커져서, 통신량을 증가시키는 단점을 가진다. 한 예로, 송신자의 수가 32이고, 해쉬 값의 크기가 20 바이트 일 때, 요구되는 AAI의 크기는 100 바이트이고, 송신자의 수가 1024일 경우 200 바이트가 요구된다. 또한, 송신자가 추가되거나 제거될 경우 MHT는 다시 구축되어야하는 문제점을 가지고 있다.

2.3 블룸 필터 기반 PKBA (Bloom filter-based broadcast Authentication Scheme, BAS)

BAS는 송신자의 인증서 검증을 블룸 필터에서 요구되는 k번의 해쉬 연산으로 대치시켜 CAS의 통신, 연산, 메모리양을 감소시켰다.[12] 하지만, 블룸 필터는 긍정 오류의 특징을 지니며, 이 긍정 오류의 확률, 즉 FPR, 을 줄이기 위해 총 송신자의 수는 엄격하게 관리되어야 한다. 즉 통신량 측면에서는 CAS나 MAS에 비해 효율적이지만, 메모리 효율성 측면에서는 MAS에 비해 떨어진다.

3.2.4 하이브리드 PKBA (Hybrid broadcast

3) [14]에 따르면, 인증서의 크기는 86바이트 까지 줄일 수 있다.

Authentication Scheme, HAS)

HAS는 MAS와 BAS를 결합한 기법으로 보다 많은 송신자를 지원하기 위해 약간의 통신량을 증가시킨 기법이다.[12] 본 기법에서는 모든 송신자의 공개키는 다수의 MHT를 구축하는데 말단 노드로 사용되고, 각 MHT의 정점 노드를 이용하여 블룸 필터를 구축한다. 이를 통해 BAS에 비해, 동일한 FPR과 블룸 필터 크기에서 보다 많은 송신자를 지원한다. 하지만, 송신자는 센서 노드에게 자신을 인증하기 위해 자신이 속한 MHT의 정점 노드를 생성하기 위한 AAI를 센서 노드에게 제공하여야 하므로 추가적인 통신량을 필요로 한다.

요한 추가적인 통신/연산/메모리양을 기준으로 비교 분석한다.

⊙ **통신량**: RPT와 BABRA를 제외한 모든 SKBA 기법들은 하나의 메시지 당 하나의 MAC을 추가로 요구하고, PKBA 기법들은 최소 하나의 서명 및 공개키를 추가적으로 전송해야한다.
⊙ **연산량**: 통신량과 비슷하게, 대부분의 SKBA 기법들은 각 센서 노드에서 한번의 MAC 연산을 필요로 하고, PKBS 기법들은 최소한 한 번의 서명 검증 연산을 필요로 한다.
⊙ **메모리양**: M-TESLA를 제외하고, 모든 SKBA 기법들은 한 송신자 당 하나의 방송매개변수 (시간 간격, 초기 키 등) 집합을 모든

표 1. 성능 비교

기법 / 성능	μTESLA	M-TESLA	L-TESLA	T-TESLA	RPT	BABRA	CAS	MAS	BAS	HAS
통신량	MAC				HASH + MAC		SIGN + CERT	SIGN + PK + AAI	SIGN + PK	SIGN + PK + AAI′
연산량	MAC				HASH + MAC		2*SIGN	SIGN + L[4] * HASH	SIGN + k[5] * HASH	SIGN + (L′[6]+k)* HASH
메모리양	PARA[7] * |S|[8]	z[9] * PARA * |S|	PARA * |CH|[10]	PARA * |S| + HASH	PARA*|S|		SIGN + CERT	CERT + HASH	CERT + VEC[11]	CERT + HASH +VEC

Ⅳ. 각 기법의 비교 분석

본 절에서는 앞에서 설명한 각 기법들을 성능과 주요 특징을 기준으로 간략히 비교분석한다.

1. 성능 비교

성능은 각 기법들이 메시지 인증을 위해 필

센서 노드들에 저장시켜야한다. 그러나 PKBA 기법들은 상대적으로 적은 메모리 공간을 요구하는데, 한 예로 MAS의 경우 송신자의 수에 관계없이 하나의 인증서 (기지국의 인증서)와 해쉬 값 (MHT의 정점노드)만 각 센서 노드에 저장하면 된다.

표 1은 각 기법들의 통신, 연산, 메모리양을 보여준다.

2. 주요 특징 비교

표2는 각 기법들의 주요 특징을 보여준다. BABRA를 제외한 모든 기법들은 송/수신자 간의 약하게 결합된 시간 동기화가 요구된다. 모든 PKBA 기법과 RPT는 메시지 즉시 인증

4) MHT의 깊이.
5) 블룸 필터에 사용된 해쉬 함수 수.
6) L' < L, AAI' < AAI.
7) 한 송신자의 방송매개변수 크기.
8) 총 송신자 수.
9) μTESLA의 계층 수.
10) 클러스터 헤드 노드 수.
11) 블룸 필터 크기.

기능을 제공하며, RPT를 제외한 모든 기법은 메시지를 특정 시간에 구애받지 않고 방송 할 수 있다. BAS와 HAS 기법은 긍정 오류 특징을 가지며 이는 소수의 센서노드들이 변조된 방송 메시지를 올바른 메시지로 판단하는 경우가 존재한다. μTESLA와 RPT는 단대단 기반의 매개변수 분배로 인하여 대규모 WSN에 적용하기 부적합하며, 모든 SKBA 기법들은 소수의 송신자만을 지원하지만 대부분의 PKBA 기법들은 다수의 송신자를 지원할 수 있다. L-TESLA의 경우 하나의 클러스터 헤드 노드를 포획함으로써 전체 네트워크에 변조된 메시지를 방송 할 수 있게 되는 취약점을 가지고 있다.

WSN에서 가장 중요한 자원은 각 센서 노드의 한정적인 에너지이다. 기본적으로 소수의 송신자를 지원하는 비밀키 기반의 기법들은 에너지 효율성 측면에서 실제 응용에 적용되기에 충분한 효율성을 제공하지만, 다수의 송신자를 지원하는 공개키 기반의 기법들은 매 방송 메시지마다 모든 센서 노드들이 공개키 연산을 수행해야 하므로 에너지 효율성 측면에서 아직 개선의 여지가 남아있다. 따라서 보다 효율적인 다수의 송신자를 지원하는 방송형 인증 기법에 대한 추가적인 연구가 필요하다.

표 2. 주요 특징 비교

기법 / 특징	μTESLA	M-TESLA	L-TESLA	T-TESLA	RPT	BABRA	CAS	MAS	BAS	HAS
시간 동기화	요구					불필요	요구			
즉시 인증	No			부분적[12]	제공	No	제공			
불규칙성[13]	제공				No	제공				
긍정 오류	No								가능	
확장성	나쁨	좋음			나쁨	좋음		아주 좋음	좋음	아주 좋음
다중 송신자	No		부분적[14]	부분적[15]	No	제공				
노드 포획 공격	강인함		CH 공격에 취약	강인함						

V. 결 론

본 논문에서는 무선 센서 네트워크에 특화되어 제안된 여러 방송형 인증 기법들에 대하여 간략히 살펴보았다. 각 기법들은 서로 자신만의 장점과 단점을 가지고 있어서, 특정 기법을 실제 WSN에 적용하기 전에 응용 어플리케이션의 요구사항을 면밀히 살펴보고, 가장 적합한 기법을 선택 적용해야할 것이다.

12) 방송매개변수만을 즉시 인증할 수 있고 실제 메시지는 즉시 인증 되지 않는다.
13) 메시지를 시간에 구애받지 않고 전파 할 수 있다. No의 경우 특정 시간에만 메시지를 전파 할 수 있다.
14) 모든 클러스터 헤드 노드가 송신자이다.
15) 센서 노드들이 각 송신자의 방송매개변수를 메모리 공간에 저장하고 있어야한다.

참 고 문 헌

[1] C. Chong and S. Kumar. Sensor networks: evolution, opportunities, and challenges. *Proceedings of the IEEE*, 91(8), pp. 1247 - 1256, 2003.

[2] T. Dimitriou and I. Krontiris. Autonomic communication security in sensor networks. In Proceedings of the 2nd International Workshop on Autonomic Communication, Oct. 2005.

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

July 2006.

[4] V. Gupta, M. Millard, S. Fung, Y. Zhu, N. Gura, H. Eberle, and S. C. Shantz. Sizzle: A standards based end-to-end security architecture for the embedded internet. In Proceedings of the 3rd International Conference on Pervasive Computing and Communication, Mar. 2005.

[5] L. Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11), pp. 770 - 772, 1981.

[6] D. Liu and P. Ning. Multi-level μ tesla: Broadcast authentication for distributed sensor networks. *ACM Transactions in Embedded Computing Systems*, 3(4), pp. 800 - 836, Feb. 2004.

[7] D. Liu, P. Ning, S. Zhu, and S. Jajodia. Practical broadcast authentication in sensor networks. In Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, Nov. 2005.

[8] M. Luk, A. Perrig, and B. Whillock. Seven cardinal properties of sensor network broadcast authentication. In Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks, Oct. 2006.

[9] R. Merkle. Protocols for public key cryptosystems. In Proceedings of the IEEE Symposium on Research in Security and Privacy, Apr. 1980.

[10] 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.

[11] K. Piotrowski, P. Langendoerfer, and S. Peter. How public key cryptography influences wireless sensor node lifetime. In Proceedings of the 4th ACM Workshop on Security of Ad hoc and Sensor Networks, 2006.

[12] 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.

[13] K. Ren, K. Zeng,W. Lou, and P. Moran. On 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.

[14] S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz. Energy analysis of public-key cryptography for wireless sensor networks. In Proceedings of the 3rd International Conference on Pervasive Computing and Communication, Mar. 2005.

[15] Y. Zhou and Y. Fang. Babra: Batch-based broadcast authentication in wireless sensor networks. In Proceedings of the 49th Annual IEEE Global Telecommunications Conference, Nov. 2006.