情報保護學會論文誌
第17卷 第3號, 2007. 6

WSN에서의 협력적인 공개키 인증 프로토콜

아 지 즈,[1†] 맹 영 재[1], 양 대 헌[1‡]
[1]인하대학교 정보보호연구실

Efficient Non-Cryptographic Protocols for Public key Authentication in Wireless Sensor Network

Abedelaziz Mohaisen,[1†] YoungJae Maeng[1], DaeHun Nyang[1‡]
[1]Information Security Research Laboratory, INHA University,

요 약

최근의 8비트 무선 센서노드에서 ECC(Elliptic Curve Cryptography)를 포함한 공개키 연구는 긍정적인 결과를 보였다. 하지만 공개키는 대칭키에 비해 더 많은 연산 능력과 메모리를 필요로 하며 공개키 환경에서 각각의 공개키는 사전에 인증을 받아야 하는 단점이 있다. 자원이 제한적인 센서노드에서 공개키 인증의 부담을 줄이고자 이 논문에서는 협력적인 공개키 인증 기법을 소개한다. 이 기법에서 각 노드는 다른 노드의 해시된 키를 저장하고 공개키 인증이 필요할 때 이 키들을 저장하고 있는 노드들은 협력적인 방법으로 인증을 돕는다. 센서노드의 제한된 자원과 보안레벨 은 트레이드오프 관계이다. 이 논문에서는 제안하는 프로토콜에 대한 여러 공격 시나리오를 바탕으로 분석과 평가를 보이고 작은 범위의 인증 오류에도 견딜 수 있도록 확장하여 보인다.

ABSTRACT

We follow the promising recent results of deploying the public key cryptography in sensor networks. Recent results have shown that the public key algorithms are computationally feasible on the typical sensor nodes. However, once the public key cryptography is brought to the sensor network, security services such like key authentication will be critically required. In this paper we investigate the public key authentication problem in the sensor network and provide several authentication protocols. Our protocols are mainly based on the non-solvable overhearing in the wireless environment and a distributed voting mechanism. To show the value of our protocols, we provide an extensive analysis of the used resources and the resulting security level. As well, we compare our work with other existing works. For further benefit of our protocols, we list several additional applications in the sensor network where our protocols provide a sufficient authentication under the constrained resources.

Keywords : *Public key Authentication, Distributed Majority Voting, Wireless Sensor Network*

I. 서 론

WSN은 마이크로 전자 공학, 반도체, 네트워크, 신호처리 등 다양한 기술들의 복합체이며[1] 자원이 제한된 센서노드들은 감지된 데이터를 목적지까지 협력적으

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2006-C1090-0603-0028)
접수일: 2007년 1월 24일; 채택일: 2007년 3월 6일
† 주저자, asm@seclab.inha.ac.kr
‡ 교신저자, nyang@inha.ac.kr

로 전달하는데 그 목적이 있다[2]. 센서들은 MITM (Man In The Middle), Sybil[3], 노드 복제와 같은 공격들이 가능한 공개된 환경에서 peer-to-peer 방법으로 통신한다. 이 안전하지 않은 환경에서 보안의 필요성 때문에 WSN의 보안 연구는 약 5년 동안 센서노드의 제한된 자원을 이유로 제한된 연결성과 탄력성, 키 선분배의 필요성에도 불구하고 적은 자원의 사용과 빠른 속도를 보이는 대칭키를 이용한 기법이 주로 연구되었다.[4]-[9]

활발하게 연구가 진행된 대칭키와는 달리 공개키는 필요로 하는 자원이 센서노드에서 부담이 되어 좀처럼 연구가 진행되지 않았지만 기존의 센서노드 플랫폼에서 공개키 프로토콜을 시험한 최근의 연구들은 적절한 연산효율 보여 WSN에서의 공개키 사용 가능성을 보였다.[10]-[11] 만약 WSN에서 공개키(ECC[12], RSA[13])가 사용된다면 대칭키에서 문제시 되었던 확장성과 연결성과 관련한 문제는 더 이상 존재하지 않을 것이다. 공개키 사용에 있어서 가장 문제시 되는 것은 Alice가 요청하여 수신된 Bob의 공개키가 Bob의 것이 옳은가에 대한 것인데 이 문제를 해결하기 위해 각 노드가 자신을 제외한 모든 노드들의 공개키 $(N-1)*P$비트(N: 네트워크 사이즈, P: 공개키의 길이)를 저장하고 수신된 공개키의 인증을 원할 때 키 목록에서 $\log_2(N)$번의 비교로 검색하는 방법이 있다. 공개키의 키 크기를 고려하여 각 노드가 공개키 대신에 공개키의 해시 값 $(N-1)*L$비트(L은 해시된 키의 길이)를 저장하는 방법이 있을 수 있지만 두 방법 모두 메모리 효율 측면에서 좋은 방법은 아니다.

Du[14]등이 연구한 WSN에서의 공개키 인증 기법에서는 Merkle 해시 트리[15]를 이용한다. [14]에서 각각의 노드는 $\log_2(N)+1$ 개의 해시 값(트리의 노드에서부터 루트까지)을 가지고 있다. Alice가 Bob의 키를 인증하려 할 때 Alice는 Bob에게서부터 Bob의 해시 값과 공개키를 받는다. Alice는 받은 것을 SHA1해시한 값과 그녀의 루트와 같은지 비교하는 것으로 수신된 키가 진짜인지 가짜인지 구분해낼 수 있다. 분배 기법을 이용하여 Merkle 트리는 서브트리(Merkle 숲)로 나뉘어 각 노드의 메모리를 줄일 수 있다. 그러므로, 각 나뉨은 요구되는 메모리를 키 하나 정도의 크기로 줄일 수 있다.

이 논문에서, 우리는 WSN의 공개키 인증을 위한 새로운 기법을 보이며 이 기법을 확장하여 다른 보안 레벨의 두 프로토콜을 소개한다. 우리의 프로토콜은 인증 프로세스를 수행하기 위해 분산적이고 협력적인 투표 기술을 이용한다. 또한 키를 인증하기 위해 어떠한 암호학적 연산도 사용하지 않으며 각 센서 노드는 인증에 사용되는 메모리와 자원을 절약하기 위해 몇 개의 다른 노드 집합의 해시키를 저장하고 있다고 가정한다.

2절에서는 3절의 기본 프로토콜에서 사용되는 가정을 소개한다. 3장의 기초 프로토콜의 두 가지 확장된 응용방법은 4절에서 다루고 다른 연구와의 분석, 평가와 비교는 5절에서 소개하며 6절에서는 결론을 담는다.

Ⅱ. 네트워크 모델: 가정

A.1 모든 센서 노드들(또는 같은 클러스터에 속한 노드들)은 같은 주파수 범위를 사용한다. 네트워크의 크기는 물리적 레이어가 아닌 MAC 레이어에 의존하도록 한다.

A.2 네트워크의 노드들(또는 인증에 도움이 될 수 있는 정보를 가진 같은 클러스터에 속한 노드들)은 주어진 시간 내에 노드들의 모든 통신을 도청할 수 있다. 보통의 경우 이 도청은 프레임의 중계 여부를 결정하는데 사용된다. WSN에서의 도청 작업은 애드 혹 네트워크의 것과는 다르므로 정해진 시간에 동작하는 노드가 인증 작업을 도와 유효한 인증 결과를 주는데 충분하다고 가정한다.

A.3 공격자가 지리적으로 같은 영역에 있거나 같은 주파수 범위 안에 있어도 정적 데이터는 한 노드에서부터 다른 노드까지 전송 가능하다.

A.4 공격자는 단일 홉의 전송시간 내에 어떤 노드가 전송할지를 알고 있을 때, 프레임의 차단이나 수정이 가능하다.

A.5 공격자는 인증 작업 동안에 인증 결과에 영향을 줄 수 있는 위조된 프레임을 삽입 할 수 있다.

Ⅲ. 기본 프로토콜

3.1 MAC 프레임 수정

2장에서의 네트워크 가정을 기반으로 두고, 센서 노드에 요구되는 자원을 줄이는 것과 동시에 플러딩 공격을 방지하기 위해 수정한 MAC 프레임을 보인다.

*. 보통 프레임과 인증 프레임을 구별하기 위해 인증을 위한 1비트의 플래그 AC(Authentication Flag)

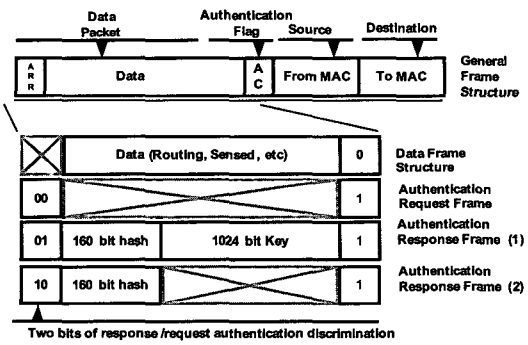
를 기존의 프레임에 추가한다. 이 비트는 k보다 많은 프레임의 수신을 무효화 할 때에도 사용된다.

*. 인증프레임은 노드로부터의 인증 요청, 인증 응답 프레임 또는 도우미 노드로부터의 인증 응답 프레임이 될 수 있다. 그러므로 위와 같은 다른 프레임을 구분하기 위해 2비트의 ARR(Authentication Request Response bits)을 추가한다. 이는 MAC 레이어에서의 플러딩 공격을 방지하기 위함이다.

〔그림 1〕은 비트들이 추가된 MAC 프레임의 실례를 보여주고 〔표 1〕은 AC와 ARR 비트의 의미를 보여준다. 수정된 MAC 프레임은 전체적인 MAC 프로토콜 디자인에 영향을 주지 않고 소프트웨어 구현단계에서 선택적으로 사용될 수 있다. 또한, 수정된 MAC 프레임은 경쟁과 스케줄 기반의 MAC 프로토콜에서도 사용될 수 있다. 이 논문에서의 프로토콜은 크게 초기화와 온라인 프로시저로 구분된다. 다음 장에서 본 프로토콜의 초기화를 보인다.

〔표 1〕 ARR과 AC의 의미

Field value	Stands for (Authentication)
ARR(00)	request frame
ARR(01)	response frame from concerned node
ARR(10)	response frame from an assisting node
ARR(11)	not used
AC(0)	normal frame
AC(1)	authentication frame



〔그림 1〕 MAC 레이어에서 인증을 사용하기 위해 수정된 MAC 프레임.

3.2 프로토콜 초기화

이 프로토콜에서 각 노드는 동전 던지기를 통해 앞면이 선택될 확률 p를 통해 키 인증 과정에 참여할지 여부를 결정한다. 네트워크의 각 센서노드 i는 아래 프로시저를 실행하여 센서노드의 ID로 묶인 공개키 정보를 설치한다.

1. TA(Trusted Authority)는 k개의 노드를 무작위로 선택한다.
2. TA는 노드 i의 공개키 정보인 K_i를 무작위로 선택된 k개의 노드들에게 전송하여 저장시킨다.
   $K_i = hash(\text{Node } i \text{ public key}|\text{Node } i \text{ ID})$.

3.3 온라인 프로시저의 인증 프로토콜

노드 j가 노드i의 공개키 정보인 K_i을 얻으려고 할 때 아래와 같이 실행한다.

1. 노드 j는 노드 i에게 노드 i의 공개키 정보 K_i를 요청하는 프레임을 보낸다. 2절의 가정에서와 같이 모든 노드들은 이를 도청할 수 있다.
2. K_i를 가진 모든 노드(노드i 포함)들은 K_i를 노드i에게 송신한다. 센서 노드i는 자신의 공개키를 함께 보낸다.
3. 노드j는 첫 번째 응답을 받은 후 한계치의 응답을 받을 때까지 응답 프레임의 수를 카운트 한다. 한계치 이상의 응답이 수신되면 노드j는 이후에 도착하는 같은 키에 대한 모든 응답을 무시한다.
4. k'을 노드j에 도착한 응답의 수, e(원래 k의 편차)를 오류 한계치라 한다. 다음이 실행될 것이다.
   a. $|k'-k| \le e$라면:
      i. 노드j는 K_i를 정하기 위해 다수결 투표를 실행한다.
      ii. K_i를 가진 모든 노드는 자신의 메모리에서 K_i를 지운다.
   b. $|k'-k| > e$는 공격을 뜻하므로 센서노드는 요청을 다시하기 위해 수신된 프레임들을 모두 무효화 한다.
5. j를 제외한 모든 노드들은 4단계를 실행하고(가정 A.2만큼의 자원 소모) 4.(a)의 경우는 아래와 같이 실행한다.
   a. 동전 던지기를 실행한다.

b. 앞면이 나왔을 경우에만 K_i를 저장한다. $p(K_i$를 유지하는 것과 같은 확률)를 앞면이 나올 확률, N을 네트워크의 노드의 수, k를 평균적으로 K_i를 가지는 노드의 수라 했을 때 $p=k/N$이다.

인증이 실행된 후에 도우미 그룹은 공격을 힘들게 하기 위해 오래된 그룹은 공개키 정보를 지우고 무작위 동전 던지기를 통해 새로운 그룹을 생성할 것이다. 3.4장에서 위에서 언급한 동전 던지기의 편차에 대해 알아본다.

3.4 Tossing 편차 제어

동전 던지기의 확률을 $p=\frac{k}{N}$라고 할당한다 하여도 노드i의 공개키 정보 K_i를 가지는 노드들의 수는 평균적으로 k개 정도이다. 이와 같은 프로세스의 확률은 이항분포를 가진다. 네트워크 크기를 N이라 하고 k를 평균이라 했을 때 다음과 같은 동전 던지기의 표준 편차를 얻을 수 있다.

$$\sigma=\sqrt{k(1-\frac{k}{N})} \quad (1)$$

편차의 실례는 [그림 2](a)에 있다. 인증 노드들 k의 평균을 줄이더라도 작은 규모의 네트워크에서 표준편차는 크게 나타난다. 따라서 수신자는 그 차이가 공격자에게서부터 왔는지 또는 큰 규모의 동전 던지기 편차와 통신 잡음에서 왔는지 구별하기가 쉽지 않다. [그림 2](b)와 같이 큰 규모의 네트워크(1000 노드들)의 경우 인증을 돕는 그룹 k의 사이즈에 비해 편차가 작게 나타나기 때문에 인증은 성공적으로 이루어질 것이다. 아래에서 작은 규모의 네트워크에서 편차가 크게 나타나는 단점을 보완하기 위한 두 기법을 소개한다.

Ⅳ. 해결책: 효율적인 프로토콜

작은 규모의 네트워크에서 나타나는 큰 편차를 극복하기 위해서는 두 가지 방법이 존재한다.

4.1 c-rounds프로토콜: 제한된 수명과 선택적인 보안

센서 네트워크는 정적으로 동작하므로 분배하기 전에 정확한 공개키 분포 정보를 알 수 있다. 이 프로토콜은 아래와 같이 초기화 단계와 온라인 프로토콜 단계로 나뉜다.

4.1.1 초기화 단계

K_i를 가진 각 노드는 아래와 같이 초기화를 실행한다.

1. TA는 WSN에서 임의로 k사이즈의 c그룹을 선택한다.
2. 키 정보는 $\langle r, K_i\rangle$로 묶인다. r은 시리얼을 뜻하며 $0<r\le c$이다. 다른 쌍들은 해당되는 노드그룹들에 로드된다. 즉, 같은 그룹의 노드들은 똑같은 시리얼을 가지게 된다.

4.1.2 온라인 인증 단계

온라인 인증 단계는 아래와 같다.

1. 노드j는 노드i의 공개키 정보를 요청한다.
2. 노드i의 공개키 정보를 가지고 있는 다른 노드들은 주어진 키로 인증에 참여할지 여부를 결정하기 위해 현재 인증단계를 나타내는 시리얼 r을 유지한다. 이 단계는 키 정보 쌍의 값과 현재 카운터 값에 대한 키 정보를 단순비교 하는 것으로 수행될 수 있다.
3. 노드i뿐만 아니라 $\langle r, K_i\rangle$를 가진 다른 모든 노드들은 요청에 응답한다(r은 현재 인증 라운드를 뜻한다). 인증에 참여하는 모든 노드들은 네트워크 트래픽을 도청할 수 있으므로 모든 K_i의 복사본을 가질 수 있다.
4. 노드j는 첫 번째 응답을 받자마자 키 정보 프레임 응답의 수를 한계 값까지 카운트 하며 저장한다. 노드j는 한계 값 이후에 도착한 모든 프레임을 버린다.
5. 노드j에 대해서 다수결 투표가 실행되고 그룹 구성원들은 K_i를 승낙할지 여부를 결정한다.
6. 만약 다수결 투표가 K_i를 승낙하면 각각의 노드들은 인증 그룹안의 모든 K_i의 복사본과 현재의 인증 라운드 r를 자신의 메모리에서 삭제한다.
7. 다음 라운드에서 다음 인증 그룹이 K_i를 인증하는 것을 돕기 위해 인증 라운드 카운터는 1증가한다.

수정된 프로토콜은 다음 인증 라운드를 예상하기 위해 동전 던지기를 요구하지 않지만 편차 0에 보증하는

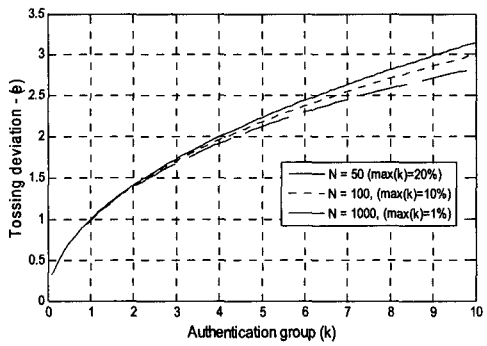
공개키 정보의 선 분배에 의존한다. 게다가 이 프로토콜은 어떤 키 K_i에 대해서도 r인증라운드로 제한되어 있다. 또한 키 인증 프로세스가 시작되면 각 노드는 AC와 ARR 비트 값에 따라 모든 수신중인 프레임을 식별할 수 있어야 하며 인증 프로세스의 현재 상태를 보고 각 노드는 수신된 인증 프레임을 상위 레이어로의 전송 여부 역시 결정할 수 있어야 한다.

4.2 Long Living 프로토콜

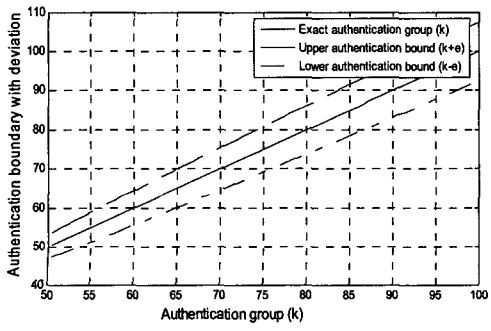
위의 프로토콜에서 주목해야 할 문제점은 제한된 수명이다. 공격자는 프로토콜의 수명을 단축시키기 위해 위조된 프레임을 삽입하는 것이 가능하다. 아래에서, 보안 수준을 약간 낮추는 대신 프로토콜의 수명을 연장시키는 프로토콜을 소개한다.

4.2.1 초기화 단계

1. 노드j는 $\langle r, req\rangle$를 전송하여 K_i인증을 요구한다.



〔그림 2〕 (a) Tossing 편차



〔그림 2〕 (b) 성공적인 인증을 위한 상한치와 하한치

r은 $0 < r \le c$ 랜덤 정수이다.

2. K_i와 r을 가지고 있는 모든 노드는 요청에 응답한다. 예외적으로 노드i는 자신의 공개키도 함께 보낸다.
3. 앞의 프로토콜처럼 노드i는 응답이 한계치만큼 올 때까지 수신된 K_i의 복사본을 카운트한다. 응답의 수가 한계치를 넘으면 j는 K_i인증을 위한 나머지 모든 프레임을 버린다.
4. 다수결 투표를 실행한 후에 인증 라운드에 참여한 노드들의 내용은 지우지 않는다.
5. 같은 키에 대해서 인증이 다시 필요하게 되면 r이 임의로 선택되고 요청이 진행된다.
6. 공격자는 r과 인증 그룹을 r-시간 이전에 알아낼 수 있는 경우에만 공격에 성공할 수 있다.

V. 평 가

5.1 인증 결정과 트레이드 오프

위의 프로토콜에서는 제한된 수의 위조된 메시지(i.e. 공격자는 인증 시간 안에 위조된 메시지를 전송할 기회가 있다.)가 있을 경우에만 투표의 결정이 가능하다. 〔그림 2〕(a)는 제한된 수의 인증 노드를 사용할 때(i.e. 각 그룹에 10개의 노드까지) 다른 네트워크 크기에서의 편차를 보여준다. 〔그림 2〕(b)는 전체 네트워크 크기의 5%, 10%를 그룹으로 사용했을 때 성공적인 인증을 위한 상한치와 하한치를 보여준다. 반면, c-rounds와 long living 프로토콜은 프로토콜 초기이전에 다른 인증 프로세스의 그룹이 결정되어있기 때문에 어떤 종류의 편차도 생성하지 않는다.

5.2 오버헤드 평가와 다른 연구와의 비교

제안된 프로토콜의 자원 오버헤드는 메모리, 통신, 연산측면으로 분석되었다. 아래에서 요구된 자원의 상세한 명세를 보인다.

5.2.1 메모리 오버헤드

노드들은 각각 k개 노드들의 인증을 도울 수 있다. 또한 각 노드는 r인증 라운드를 가지고 있다. 그러므로 각 노드에 요구되는 메모리는 $k \times r \times L$ bit이다. L은 해시된 키의 비트단위 크기이다. (e.g. SHA1 160비트)

5.2.2 통신 오버헤드 CT_{OH}

키의 인증을 위한 다수결 투표를 실행하기 위해 분산적으로 동작하는 것을 고려하면 통신에 드는 비용은 k개의 해시 키들을 보내고/받는 만큼이다.

5.2.3 연산 오버헤드

8비트 프로세서(i.e. ATmega128L, f = 8 Mhz)에서 160비트의 해시키를 사용하여 하나의 키를 인증하기 위해서는 $(2.5\,k)\,\mu\sec$이 소요된다. 여기서의 연산은 문자열 비교 연산을 나타낸다. 일반적으로 W를 프로세서 워드 사이즈, L을 해시키의 사이즈, f를 Hz단위의 프로세서의 주파수라고 했을 때, 초단위의 연산은 아래와 같다.

$$CM_{OH} = \frac{L}{W} \times \frac{k}{f} \tag{1}$$

〔표 2〕에 인증을 위해 소비된 자원의 상세한 비교가 있다.

5.3 보안분석

제안한 프로토콜의 보안성은 투표의 결정이 공격자의 행동에 영향을 받지 않고 성공적으로 인증을 수행하는데 달렸다. 투표에 참여하는 노드의 수를 k, 오류 허용범위를 e라고 가정 했을 때 인증 결과를 우회하려면 각 노드는 $(k \pm e)/2$만큼의 가짜 키가 필요하다. 수정된 MAC 프레임과 키 K_j의 인증을 승낙하기 위해 $k \pm e$개의 키를 요구하는 것은 k개의 공격자의 가짜 키보다 더 배달하기 힘들게 할 것이다. 〔그림 3〕(c)는 선택적인 공격에 대해 다른 k들에 대한 각 노드의 인증 기회를 나타낸다.

〔표 2〕 RSA[13], ECC[12], Du et al[14]와 제안된 기법의 비교 표. CTOH와 CMOH는 각각 통신과연산 오버헤드를 뜻한다.

	Key/Hash size (bit)	CTOH (bit)	CMOH (ms)
RSA〔13〕	1024	1024	430
ECC〔12〕	160	320	1620
Du *et al.*〔14〕	160	$160k$	$7.2k$
Our Scheme	160	$160k$	$2.5\times10^{-3}k$

제안한 프로토콜의 행동을 확률적으로 보이기 위해 P_{pd}를 목적지 노드가 k의 복사본들을 받을 수 있는 충분한 시간 τ안에 인증패킷이 인증노드에 배달될 수 있는 확률이라고 보자. 인증 링의 패킷 배달 이벤트와 공격자 노드는 같다고 볼 수 있다. 그러므로 이 확률은 전체 선택에 영향을 미치지 않는다. τ안에 공격자가 $k/2$와 같거나 더 많은 패킷을 성공적으로 배달할 확률 즉, 인증에 실패할 확률을 P_f라고 하자. m,n,k를 각각 공격자의 패킷, 다른 노드들의 인증 패킷 수, 요구되는 패킷의 한계치라고 보자. 수신된 패킷 k에서부터 $m+n$까지의 수를 $n(S)$라고 하고 다음과 같이 표기한다.

$$n(S) = \binom{m+n}{k} \tag{3}$$

$k/2$ 또는 이 이상의 패킷 이벤트의 결과를 공격자의 것이라 하고 나머지는 인증 노드 $n(B)$의 것이라 하자.

$$n(B) = \sum_{i=0}^{k/2} \binom{m}{\frac{k}{2}+i} \binom{n}{\frac{k}{2}-i} \tag{4}$$

등식4는 성공적으로 받은 공격자의 패킷 $c: k/2 \le c \le k$로 인한 모든 인증 실패 결과를 고려한다. 3과 4로부터 $Pf = n(B)/n(S)$와 같이 얻을 수 있는 P_f는 아래와 같이 나타낼 수 있다.

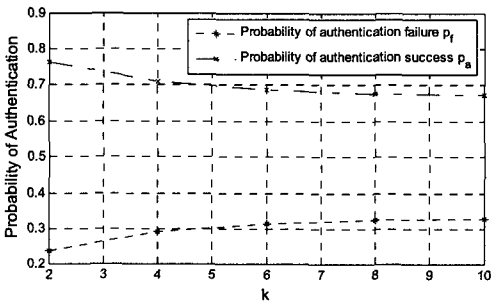
$$P_f = \sum_{i=0}^{k/2} \left(\binom{m}{\frac{k}{2}+i} \binom{n}{\frac{k}{2}-i} \right) \Big/ \binom{m+n}{k} \tag{5}$$

마지막 식에 의해서, 성공적인 인증 확률을 $P_a = 1 - P_f$라고 정의한다. 일정한 n, m과 변하는 k에 대한 결과는 〔그림 3〕(a)에 있다. 추가적으로 〔그림 3〕(b)는 인증 성공확률에 대한 공격자 패킷 수에 따른 영향을 보여준다. 양쪽의 경우 모두 높은 확률($i.e\, P_a > 0.7$)로 성공적으로 인증되었다.

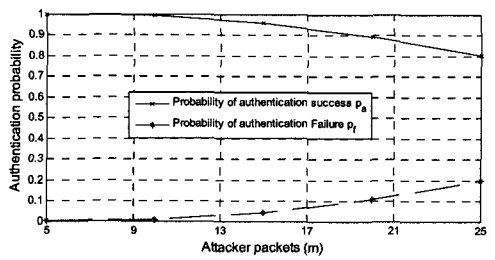
VI. 결 론

이 논문에서는 WSN에서 협력적으로 공개키 인증을 돕는 새로운 프로토콜을 소개했으며 이 프로토콜의 두 가지 응용 방법도 보였다. 센서노드의 제한된 자원을 고려하여 제안된 프로토콜은 어떠한 암호학적 연산도 요

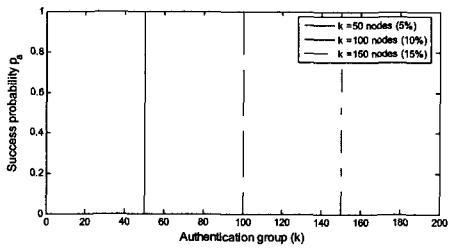
구하지 않고 MAC 프레임의 수정을 극소화하여 기존의 MAC 프로토콜에서도 적용될 수 있도록 하였다. 제안된 기초 프로토콜에서도 인증은 제한적인 편차로 성공적으로 행해진다. 우리의 프로토콜은 단일 홉 인증에 맞게 디자인 되었지만 다중 홉 환경에서도 가능하도록 확장할 연구 계획이 있다. 인증 투표를 수행하기 위한 파라미터의 사용도 연구할 것이다. 다른 프로토콜들이 특정한 분배 지식모델에 맞게 디자인 된 것에 비해 제안한 프로토콜은 일반적인 모델에서 분석되었을 뿐만 아니라 요구되는 셋 사이즈와 통신비용도 줄였다.



(a) 임의 공격 1



(b) 임의 공격 2



(c) 선택적인 공격

〔그림 3〕 1000개의 노드에서 (a) $n=m=10$ 이고 다른 k값에 대해 임의적으로 공격 했을 때의 인증의 성공과 실패 확률 (b) $n=50, k=10$ 이고 다른 공격 패킷 m (3) 선택적인 공격, 키를 인증하기 위한 다른 한계 값

참고문헌

〔1〕 Culler D., Estrin D, Srivastava M., "Overview of Sensor Networks", IEEE Computer Society, pp. 41-49, August 2004.

〔2〕 Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E., "Wireless Sensor Networks", A Survey, Computer Networks Journal, Vol. 38, No. 4, pp. 393-422, 2002

〔3〕 Zhang Q., Wang P., Reeves D. S., Ning P., "Defending against Sybil Attacks in Sensor Networks", ICDCS Workshops 2005, pp. 185-191, 2005

〔4〕 Eschenauer, L., Gligor, V., "A key management scheme for distributed sensor networks", ACM CCS'02, pp. 41-47, 2002

〔5〕 Blom, R., "An optimal class of symmetric key generation systems", Advances in Cryptography, EUROCRYPT 84, pp. 335-338, 1985

〔6〕 Du, W., Deng, J., Han, Y. S., and Varshney, P., "A pairwise key pre-distribution scheme for wireless sensor networks", 10th ACM CCS'03, pp. 42-51, 2003

〔7〕 Liu, D., Ning, P., "Establishing Pairwise keys in distributed sensor networks", 10th ACM CCS'03, pp. 52-61, 2003

〔8〕 Blundo, C., DE Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., and Yung, M., "Perfectly secure key distribution for dynamic conferences", CRYPTO '92, pp. 471-486, 1993

〔9〕 Mohaisen A, Nyang D., "Hierarchical Grid-Based Pairwise Key Predistribution Scheme for Wireless Sensor Networks". EWSN 2006, LNCS 3868, pp. 83-98, 2006

〔10〕 Gura N., Patel A., Wander A., Eberle A., Shantz S. C., "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs", CHES 2004, pp. 119-132, 2004

〔11〕 Wander A., Gura N., Eberle H., Gupta V., Shantz S.C., "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks",

PerCom'05, pp. 324-328, 2005

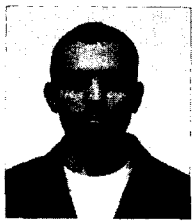
[12] Koblitz N., Menezes A., Vanstone S., "The State of Elliptic Curve Cryptography", Designs, Codes and Cryptography, 19, pp. 173-193, 2000

[13] Rivest, R. L., Shamir, A., Adleman, L. M., "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21(2), pp. 120-126, 1978

[14] Du W., Wang R., and Ning P., "An Efficient Scheme for Authenticating Public Keys in Sensor Networks", 6th ACM MobiHoc, pp. 58-67, 2005

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

〈著者紹介〉



아 지 즈 (Mohaisen Abedelaziz) 정회원
2005년 2월: 가자대학교 컴퓨터 공학과 졸업
2005년 9월~현재: 인하대학교 정보통신대학원 석사
<관심분야> 네트워크 보안, 암호프로토콜

맹 영 재 (YoungJae Maeng) 정회원
2006년 8월 : 인하대학교 컴퓨터 공학과 졸업
2006년 9월~현재 : 인하대학교 정보통신대학원 석사
<관심분야> 인터넷 보안, 네트워크 보안

양 대 헌 (DaeHun Nyang) 정회원
1994년 2월 : 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업
1996년 2월 : 연세대학교 컴퓨터 과학과 석사
2000년 8월 : 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월 : 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재 : 인하대학교 정보통신대학원 조교수
<관심분야> 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안