경량화 데이터 Origin 인증을 통한 효율적인 센서 네트워크 보안에 관한 연구

정회원 박 민 호*, 이 충 근*, 손 주 형*, 종신회원 서 승 우**

Efficient Security Mechanism using Light-weight Data Origin Authentication in Sensor Networks

Min-Ho Park*, Chung-Keun Lee*, Ju-Hyung Son* ***Regular Members***,
Seung-Woo Seo* ***Lifelong Menber***

요 약

센서 네트워크는 무선 채널의 근본적인 보안상의 취약점 이외에도 센서 노드 자체의 하드웨어적인 제약 사항을 가진다. 따라서 보안성을 보장해 주기 위해 기존의 무선통신 네트워크와는 다른 접근이 필요하다. 즉 인증 방법의 경량화를 통해서 저 사양의 센서 노드에서 동작 가능하고 보안체계 작동 시에 네트워크의 성능을 유지 할 수 있도록 해야 한다. 본 논문에서는 이러한 센서 네트워크가 가지는 특징들을 고려하여 네트워크 성능과 보안성 사이에서의 절충점을 만족시킬 수 있는 데이터 origin인증 방법에 대해 논의하였다. 이것은 각 센서 노드들이 클러스터 헤드와 스타 토폴로지 형태로 연결된 센서 네트워크에서 메시지에 특수한 인증코드의 첨부로 네트워크 성능은 유지하면서 주고받는 메시지의 origin인증을 가능하게 하는 challenge-response 방식의 인증방법이다. 이때 사용되는 특수한 코드는 질의코드와 응답코드의 순서쌍이 오직 하나만 존재하는 특징을 가진 유일순차코드로서, 본 논문에서는 이를 생성하는 방법과 생성된 코드의 인증 적용 방법에 대해서 설명하고 공격에 대한 안전성에 대해서 논의 한다.

Key Words : Sensor network, Security, Authentication, Random sequence code

ABSTRACT

There are many weaknesses in sensor networks due to hardware limitation of sensor nodes besides the vulnerabilities of a wireless channel. In order to provide sensor networks with security, we should find out the approaches different from ones in existing wireless networks; the security mechanism in sensor network should be light-weighted and not degrade network performance. Sowe proposed a novel data origin authentication satisfying both of being light-weighted and maintaining network performance by using Unique Random Sequence Code. This scheme uses a challenge-response authentication consisting of a query code and a response code. In this paper, we show how to make a Unique Random Sequence Code and how to use it for data origin authentication.

Ⅰ. 서 론

센서 네트워크(sensor network)는 물리공간의 상태인 빛, 소리, 온도, 움직임 같은 물리적 데이터를 센서노드에서 감지하고 측정하여 중앙의 베이스스테이션 (Base Station) 또는 싱크 (Sink) 로 전달하는

※ 본 연구는 대학정보통신연구센터(ITRC)와 서울시 산학연 협력사업의 지원으로 수행되었습니다.
* 서울대학교 전기.컴퓨터공학부 컴퓨터네트워크 및 보안연구실 (minopak@cnslab.snu.ac.kr)
논문번호 : KICS2006-05-249, 접수일자 : 2006년 5월 30일, 최종논문접수일자 : 2007년 5월 8일

센서 노드들로 구성되는 무선 네트워크이다. 그런데 센서 네트워크는 무선통신이 가지는 보안상의 취약점 외에도 센서 노드 자체의 하드웨어적인 제약(마이크로 프로세서, 메모리)에서 기인하는 취약성 때문에, 보안성을 보장해 주기 위해 기존의 무선통신 네트워크와는 다른 접근이 필요하다. 즉 네트워크 성능을 유지하면서 매우 경량화된 보안체계를 갖추고 있어야 한다.

네트워크 관리자는 네트워크 성능 향상과 보안체계 강화 사이에서 발생하는 tradeoff에서 대부분 네트워크 성능 향상을 선택하게 된다. 즉 네트워크 성능향상을 위해서 보안에 필요한 선택사항들을 off 상태로 동작시키게 되는데, 이런 경우 만약에 발생할지 모르는 공격에 대해서 피해가 상당할 수 밖에 없다. 따라서 센서 네트워크에서는 네트워크 성능과 보안레벨(Security Level)사이에서의 적절한 절충점을 찾아야 한다.

클러스터 헤드가 각 센서 노드들과의 통신을 통해서 주변 상황의 데이터를 수집하고 이를 클러스터 헤드 사이의 통신을 통해서 BS까지 전달되는 전형적인 센서 네트워크를 가정하자. 이 경우, 보안성을 제공하는 메시지 인증을 위해서 네트워크 성능 저하를 피할 수 있고 완벽한 보안 제공은 어렵더라도 오버헤드 없이 언제나 동작할 수 있는 just-enough security가 요구된다.

본 논문에서는 보안성 유지에 필요한 just-enough security를 제공하기 위하여 특수한 성질을 가지는 유일순차코드(Unique Sequence Code)를 사용하였다. 각 노드는 자신만이 사용하는 특수한 코드를 할당 받고, 이 코드를 이용하여 클러스터 헤드와 노드간의 메시지 전달에 있어서 네트워크 성능을 떨어뜨리지 않고 메시지마다 데이터의 origin인증을 할 수 있다. 유일순차코드 중 하나인 Prime Sequence Code (PSC)[2]는 생성방법이 쉽다는 장점과 노드가 알고 있어야 하는 정보가 적다는 장점이 있으나, 코드의 패턴이 쉽게 추측 가능하다는 약점 때문에 보다 높은 보안성을 제공하는 코드생성 방법이 필요하다.

따라서 PSC가 간단한 패턴을 가지는 취약점을 보완한 Unique Random Sequence Code (URSC)를 이용한 데이터origin인증방법을 제안하였다. 이 방법을 이용하여 주고 받는 메시지에 수 비트의 간단한 코드를 첨부하고 challenge-response방식으로 질의코드와 응답코드의 매칭을 통해서 메시지의 origin인증과 freshness를 동시에 검증할 수 있다. 본 논문에서 제안한 인증방법은 다른 인증방법에 비해 상대적으로 작은 크기의 URSC로 origin인증과 freshness를 동시에 보장해 줄 수 있고, 기존의 경량화된 인증방법에서 요구 되었던 양단간의 인증비트의 동기화가 필요 없다는 장점을 가지고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 여러 인증 방법에 관한 연구에 대해서 알아보고, 3장에서는 두 가지 유일순차코드의 생성법과 인증에의 적용에 대해서 살펴본다. 그리고 4장에서는 URSC를 사용한 인증방법의 공격 가능성 등에 대해서 논의하며 5장에서는 제시한 인증 방법을 실제 IEEE 802.15.4 MAC 계층에의 적용에 대해서 논의한다.

Ⅱ. 관련연구

데이터의 무결성과 데이터origin인증을 모두 제공해 주는 전자서명(Digital Signature)[6]과 Hashed Message Authentication Code (HMAC)[7]에 대한 많은 연구가 있었다. 그러나 센서 네트워크에서는 센서 노드의 하드웨어적인 제약 때문에, 많은 계산량이 요구되는 전자서명은 부적합하다. 비교적 계산이 단순한 HMAC의 경우에 데이터 무결성과 origin 인증을 제공하기 위해서 20바이트를 사용하는데, 데이터의 크기가 작거나 ACK메시지처럼 데이터의 무결성이 중요하지 않은 상황에서는 HMAC자체가 오버헤드가 될 수 있다.

[3]에서는 IEEE 802.11네트워크에서 데이터와 독립적인 1비트만을 첨부하여 네트워크의 성능저하 없는 사용자 인증을 제공하기 위한 인증 방법으로 Statistical One-bit Lightweight Authentication (SOLA)을 제안하였다. Access Point (AP)는 각 노드들과의 통신에 사용되는 인증 비트 스트림(Authentication Bit Stream)을 각 노드에 대해서 가지고 있고, 각 노드들과의 패킷 전달과정에 1비트의 사용자 인증 비트를 메시지에 포함시킨다. 이 경우 공격자가 연속적으로 n번의 메시지 인증 비트를 맞출 확률은 2-n보다 작게 된다. n=6정도만 되더라도 약98% 이상의 시큐리티를 보장할 수 있게 된다. 하지만 여러 번의 메시지 전송이 이루어져야만 사용자 인증이 보장되고, 따라서 공격자를 알아내기 전에 전송되는 메시지의 불법성에 대해서 알아낼 수 없다. 또한 AP와 노드는 각자가 가지고 있는 비트 스트림에서 현재의 위치를 나타내는 비트 인디케이터(Bit Indicator)의 동기를 유지해야 하는데 채널 에러 확률이 높기 때문에 패킷손실이 발생하기 쉬

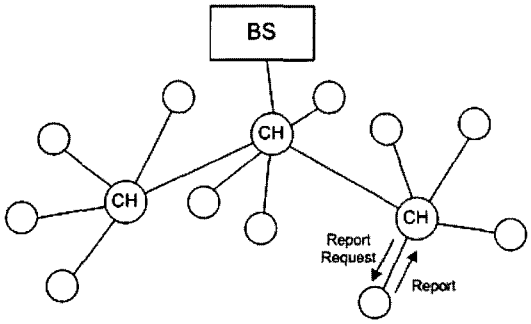


그림 1. 센서 네트워크 모델

운 무선 네트워크 상황에서는 비트 인디케이터의 동기화가 문제가 될 수 있고, 이에 따라 발생하는 false positive 문제도 고려해야 했다. 따라서 메시지의 전달이 양단 간에 지속적으로 발생하지 않는 센서 네트워크에서 채널 에러 때문에 발생하는 비트

스트림 동기화 문제를 해결하는 동시에 메시지의 크기도 최소화 할 수 있는 데이터 origin인증 방법이 필요하다.

Ⅲ. 제안하는 인증기법

본 장에서는 특수한 성질을 가진 순차코드를 제안하고 이 순차코드를 사용하여 사용자 인증을 하는 방법에 대하여, 1절에서는 네트워크 모델을 가정하고 2절과 3절에서는 각각 PSC와 URSC의 생성법, 적용방법과 특징 등에 대해서 살펴본다.

3.1 네트워크 모델

제안한 인증기법을 적용하기 위한 네트워크 모델은 그림1 과 같다. 센서 네트워크의 보편적인 토폴로지로서 주변 상황을 센싱하는 센서, 센서로부터 정보를 수집하고 데이터를 프로세싱하여 BS로의 전달을 수행하는 클러스터 헤드, 데이터의 최종 집결지인 BS로 구성된다. 각 노드와 클러스터 헤드는 challenge-response방식으로 메시지를 주고 받는다고 가정한다. 즉 클러스터 헤드는 자신의 클러스터에 속한 노드에게 'Report Request'를 통해서 자료 요청을 하고, 노드는 클러스터에게 'Report'를 보낸다.

노드는 프로세싱 능력과 메모리 크기의 한계를 가지는 매우 수동적인 장치라고 가정하고, 클러스터 헤드는 노드에 비해서 상대적으로 강력한 성능을 지닌 장치라고 가정한다. 메시지는 클러스터 헤드와 노드 간에 서로 전달이 되고 메시지는 가능한 작은 크기로 전달되어야 한다. 그리고 메시지에는 어떤 형태의 코드를 첨부하여 이 메시지가 불법적인 노드로부터 왔는지의 여부를 판단함으로써 보안성을 제공할 수 있도록 한다. 즉 메시지에는 사용자 인증을 위한 N 비트가 포함되어 있다.

3.2 Prime Sequence Code(PSC)를 사용한 인증 방법

3.2.1 코드 생성

Prime Sequence Code[2] 생성법은 임의의 소수p를 선택하여 서로 중복되지 않는 p-1개의 순차코드를 만드는 방법이다. PSC를 만드는 알고리즘 다음과 같다.

Step1.임의의 소수p를 선택한다.

Step2.다음과 같이 (p-1) 행(p)열의 순차코드 행렬(Sequence Code Matrix) M을 만든다.

Step2.1. 모든 행의 첫 번째 열은 0부터 시작한다.

Step2.2. i번째 행은 i만큼씩 증가한다. 즉, i행j열의 값

$$m(i,j) = (i \times (j-1)) \bmod p \text{ for } 1 \le i, j < p$$

p=7 인 경우,

$$M = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 2 & 4 & 6 & 1 & 3 & 5 \\ 0 & 3 & 6 & 2 & 5 & 1 & 4 \\ 0 & 4 & 1 & 5 & 2 & 6 & 3 \\ 0 & 5 & 3 & 1 & 6 & 4 & 2 \\ 0 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$$

$$M = [m(i,j)], m(i,j) = (i \times (j-1)) \bmod 7$$

with $1 \le i \le 6$ and $1 \le j \le 6$

예제 1. PSC 생성 예

예제 1은 p=7일 때, PSC 생성 알고리즘에 의해서 만들어진 순차코드의 예이다. 이렇게 만들어진 PSC에서는 어떤 수와 다음 수로 이어지는 순서쌍은 오직 하나의 행에서 한 개만 존재한다. 예제1에서 '2' 다음에 '5'가 나오는 경우는 3행의 4열과 5열에서 오직 한번만 나타난다. 즉 소수순차코드행렬(Prime Sequence Code Matrix)에서 임의의 순서쌍은 오직 하나의 행에서 한번만 나타난다.

본 논문에서는 이런 특징을 가진 순차코드를 유일순차코드(Unique Sequence Code)라고 명명한다. 다음 절에서는 센서 네트워크와 같이 데이터의 크기가 중요한 요소로 작용하는 경우, 유일순차코드의 특성을 데이터 Origin 인증에 적용하는 방법에 대해서 설명한다.

3.2.2 데이터Origin인증에의 적용

데이터Origin인증에 필요한 필드로 N비트가 할당되어 있다고 할 때, 클러스터 헤드는 $p \leq 2N$을 만족하는 소수 p를 선택하고 PSC생성알고리즘에 의해서 소수순차코드행렬 M을 생성한다. 이때 행렬의 각 행 번호를 시퀀스오더 (Sequence Order)로 정의하여 이것을 자신에게 속한 노드들에게 무작위로 나누어 준다. 즉 각 노드들은 자신이 부여 받은 시퀀스오더만을 알고 있으면 되는데, 이 값은 자신이 사용하게 될 순차코드의 증가분이기 때문에 이 값으로 순차코드를 만들 수 있다.

이해를 돕기 위해 그림2를 예로 들어 설명한다. 클러스터 헤드에 6개의 노드가 속해 있고, 클러스터 헤드는 예제1의 M과 같은 소수순차코드행렬을 가지고 있다. 클러스터 헤드는 각 노드들에게 시퀀스오더(M의 행 번호 1부터 6)까지를 각 노드에게 무작위로 나누어 준다. 노드A가 시퀀스오더 4를 할당받았다고 가정하면, 노드A는 자신의 시퀀스오더 4를 이용하여 M의 4행과 같은 순차코드를 만들어 낼 수 있다. 즉 클러스터 헤드와 노드A는[0, 4, 1, 5, 2, 6, 3]라는 순차코드를 공유하게 되고, 이 순차코드를 클러스터 헤드와 노드A사이에 교환되는 메시지에 첨부하여 클러스터 헤드가 데이터 origin인증을 하는데 사용할 수 있다.

클러스터 헤드가 노드A에게 'Report Request' 메시지를 보낼 때, 클러스터 헤드는 노드A가 할당 받은 4번째 순차코드 중에서 임의로 '2'를 선택하여 메시지를 보낸다. 이때 노드A는 요청에 대한 'Report'를 작성하여 보내는데 '2' 다음에 나와야 하는 응답코드 '6'을 'Report'에 첨부하여 보낸다. 클러스터 헤드는 그 안에 포함된 순차코드가 자신이 요청할 때 보냈던 바로 다음 값인 '6' 인지를 확인한다. 이것이 맞다면 이 메시지는 노드A에게서 온 것이라는 데이터origin인증이 되며, 요청에 대한 응답임을 나타내는 freshness도 검증 할 수 있다.

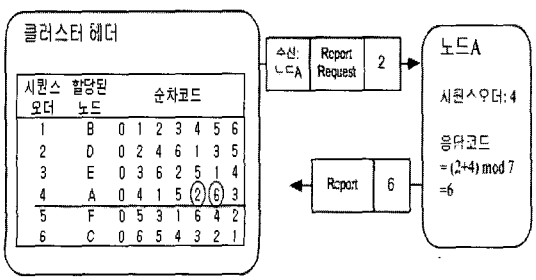


그림 2. PSC를 이용한 데이터origin인증 예

3.2.3 보안 취약성

PSC를 이용한 인증방법은 코드생성 방법이 간단하고 노드가 알아야 할 비밀정보가 자신이 사용하는 시퀀스오더 뿐이라는 장점이 있다. 그러나 패턴 자체가 너무 단순하기 때문에 공격자는 클러스터 헤드와 노드간에 주고 받는 메시지를 한번씩만 훔쳐보게 된다면 그 노드의 시퀀스오더를 알 수 있게 된다. 앞 절의 예에서 클러스터 헤드와 노드간의 메시지 전달과정에서 '2'과 '6'이 교환된 것을 알게 되면 노드의 시퀀스오더인 4가 노출될 수 있고, 이후 에 일어나는 노드와 클러스터 헤드와의 메시지 전달과정에 공격자가 쉽게 침투할 수 있다.

따라서 유일한 순차적 특성은 그대로 유지하면서 패턴을 쉽게 알 수 없는 코드가 필요하다. 이를 위해서 다음 절에서는 보다 강화된 순차코드를 제안하고 자세히 살펴본다.

3.3 Unique Random Sequence Code (URSC)를 사용한 인증방법

3.3.1 코드 생성

PSC에서는 하나의 순차코드가 시퀀스오더 만큼씩 일정하게 증가했지만, URSC에서는 순차코드의 증가 패턴을 다르게 정한다. 즉 길이 L인 순차코드에 대해서 호핑(Hopping) 패턴을 찾는 것이다. 시드(seed)가 되는 순차코드생성자 (Sequence Generating Code)를 찾기 위해서 많은 시도가 필요하지만 일단 만들어진 순차코드생성자는 패턴이 불규칙하기 때문에 PSC에서 발생하는 패턴 노출을 막을 수 있다. 그리고 유일한 순차적 특성은 그대로 유지하므로 보다 안전한 데이터 origin인증을 제공해준다. 코드 생성의 기본적인 알고리즘은 [1]에서 제안한 주파수 도약 광 직교 코드 (Frequency-Hopping Optical Orthogonal Code)에서 공백을 제거하여 메시지의 인증을 위한 필드에 적용할 수 있도록 개선하였다. 알고리즘 1은 URSC의 생성 알고리즘이다. Step3에서 dL-1까지만 더하는 이유는 L열에 dL을 더하면 1열의 값이 다시 반복되기 때문이다.

URSC생성을 예제 2와 같이 예를 들어 살펴보자. q=7, L=4일때, Step2조건에 만족하는 거리호핑패턴 (distance hopping pattern) D 중에서 Case1과 같이 (2,3,4,5)를 선택하였다면 행렬M의 1번째 행은 [0,2,5,2]가 되고 행렬 M의 한 행에 같은 수가 반복적으로 나타나므로 D를 폐기하고 다른 D를 선택한다. Case 2와 같이D가 (2,3,5,4)일 경우, 행렬M의

Step1. 소수p와 code길이 L(<p)을 선택한다.

Step2. Distance Hopping Pattern D를 선택한다.

$$D=[d_1,d_2,d_3,...d_L]$$

$$\forall\ 1\le d_i\le q-1 \text{ and } \sum d_i\equiv 0(\bmod q)$$

Step3. D의 모든 순열에 대해서 다음과 같은 행렬을 만든다.

M=

$$\begin{bmatrix} 0 & 0+d_1 & 0+d_1+d_2 & \cdots & 0+\sum_1^{L-1} d_i \\ 1 & 1+d_1 & 1+d_1+d_2 & \cdots & 1+\sum_1^{L-1} d_i \\ 2 & 2+d_1 & 2+d_1+d_2 & \cdots & 2+\sum_1^{L-1} d_i \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ L' & L'+d_1 & L'+d_1+d_2 & \cdots & L'+\sum_1^{L-1} d_i \end{bmatrix} (\bmod p)$$

where $L'=L-1$

Step4. M의 모든 행과 열에서 같은 수가 반복 되지 않으면 M을 순차코드행렬로 사용한다. 그렇지 않으면 D와M을 폐기, Step2부터 반복한다.

알고리즘 1. URSC 생성 알고리즘

모든 행과 열에 같은 수가 반복되지 않으므 로 M을 유일순차코드행렬로 취할 수 있고, M의 1 행 [0,2,5,3]을 순차코드생성자로 둔다.

3.3.2 데이터 Origin 인증에의 적용

기본적인 인증 프로세스는 PSC의 경우와 같은 challenge-response방식이다. 즉 클러스터 헤드가 노드에게 메시지를 보낼 때 origin인증을 위한 질의코드를 첨부해서 보내면, 노드는 다시 그에 대한 응답코드를 메시지에 붙여 보낸다. 그러나 PSC와는 다르게 노드가 자신의 시퀀스오더 이외에 순차코드생성자를 추가로 저장하고 있어야 한다. 순차코드생성자의 크기는 p와 L에 의해서 결정되는데, 그 크기는 $\lceil \log p \rceil \times L$ 비트로 저장해야 할 메모리가 크지 않기 때문에 노드의 메모리 사용에 영향을 미치지 않는다.

기본적으로 노드가 클러스터에 association하는 동안에 비밀정보를 안전하게 전달 받았다고 가정한다. 즉 노드는 클러스터로부터 순차코드생성자와 자신의 시퀀스오더를 안전하게 할당 받아 자신의 순차코드를 만들어 저장하고 있다.

p=7, L=4인 경우,

Case1. D=[2,3,4,5]를 선택했을 때

M=

$$\begin{bmatrix} 0 & 0+2 & 0+2+3 & 0+2+3+4 \\ 1 & 1+2 & 1+2+3 & 1+2+3+4 \\ 2 & 2+2 & 2+2+3 & 2+2+3+4 \\ 3 & 3+2 & 3+2+3 & 3+2+3+4 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 5 & 2 \\ 1 & 3 & 6 & 3 \\ 2 & 4 & 0 & 4 \\ 3 & 5 & 1 & 5 \end{bmatrix}$$

1행과 3행에 같은 수가 반복되므로 D를 폐기

Case2. D=[2,3,5,4]를 선택했을 때

M=

$$\begin{bmatrix} 0 & 0+2 & 0+2+3 & 0+2+3+5 \\ 1 & 1+2 & 1+2+3 & 1+2+3+5 \\ 2 & 2+2 & 2+2+3 & 2+2+3+5 \\ 3 & 3+2 & 3+2+3 & 3+2+3+5 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 5 & 3 \\ 1 & 3 & 6 & 4 \\ 2 & 4 & 0 & 5 \\ 3 & 5 & 1 & 6 \end{bmatrix}$$

모든 행과 열에 같은 수가 없으므로 M을 순차코드행렬로 사용 가능

예제 2. URSC 생성 예

예제 2를 예로 들어 설명한다. 노드B가 시퀀스오더 2(M의 2번째 행)를 할당 받았다고 가정하면 노드B는 자신의 시퀀스오더 2와 순차코드생성자로부터 자신의 순차코드[1, 3, 6, 4]를 만들어 저장하고 있다. 클러스터 헤드가 노드B에게 'Report Request'를 보낼 때 노드B에게 할당된 순차코드 중 '3'을 질의코드로서 붙여 보냈다면, 노드B는 'Report'를 전송할 때 '3' 에 대한 응답코드로 '6'을 메시지에 첨부해서 전송한다. 클러스터 헤드는 전송 받은 응답코드가 '6'인지를 확인하여 이 'Report'가 노드B에게 왔다는 origin인증을 할 수 있고, 방금 보낸 'Report Request'에 대한 응답인지에 대한 freshness를 확인을 할 수 있다.

3.3.3 URSC를 이용한 인증방법의 장점

URSC는 생성하는데 많은 반복작업이 필요하다는 단점이 있으나, 공격자가 코드패턴을 쉽게 알 수 없다는 것이 가장 큰 장점이라고 할 수 있다. 앞서 언급한 PSC의 경우에는 클러스터 헤드와 노드간의 메시지 전달을 한번만 엿듣게 되면 패턴이 그대로 노출이 되기 때문에 보안성을 보장할 수 없었다. URSC의 경우에는 각 코드간의 거리(distance)가 랜덤하게 정해지므로 공격자가 쉽게 코드의 패턴을 알아 낼 수 없다. 적어도 L(코드길이)번 만큼의 메시지 전달을 엿들어야만 코드의 전체패턴을 알 수 있다. PSC와 같이 공격자가 'Report Request(3)' 과

'Report(6)'를 엿듣는다고 해도 패턴이 쉽게 노출되지 않는다.

그리고 클러스터 헤더와 노드간에 동기화가 필요 없다는 장점이 있다. 클러스터 헤더는 수신 노드에 해당하는 순차코드 중의 하나를 임의로 골라 질의코드로 사용하고, 노드는 질의코드에 대한 유일한 응답코드를 전송하면 되기 때문에 주고 받는 코드에 대해서 동기화를 맞출 필요가 없다.

Ⅳ. 성능 평가

메시지 내에 사용자 인증에 필요한 인증필드를 N 비트를 사용해도 네트워크의 성능에 전혀 영향을 미치지 않고, $p \leq 2N$ 을 만족하는 p와 L을 선택하여 L개의 순차코드를 사용자 인증에 이용한다고 가정하자. 이 경우 공격자는 어떤 메시지에 대한 응답 메시지의 인증비트를 알아 맞출 확률은 2-N이 된다. 만약 인증비트가 5비트만 된다고 하더라도 공격자가 인증비트를 맞출 확률은 약 3%로 매우 희박하기 때문에 안전하다고 볼 수 있다.

따라서 어떤 공격자가 리플레이 공격(replay attack)을 시도할 경우에도 클러스터 헤드가 매 전송 시마다 수신 노드에 해당하는 순차코드 내에서 무작위로 질의코드를 바꾸기 때문에 공격자는 응답 메시지에 포함되어야 응답코드의 패턴을 쉽게 추측할 수 없으며, 또한 이 질의코드-응답코드의 순서쌍이 바로 메시지의 freshness를 제공해 줄 수 있기 때문에 replay attack에 대해서 $1-(1/2^n)$의 보안성을 보장할 수 있다.

Ⅴ. IEEE 802.15.4 MAC 계층에의 적용

IEEE 802.15.4 MAC[5] 계층에서는 ACK 메시지에 대해서는 보안장치가 마련되어 있지 않다. ACK는 단순히 보낸 노드에게 잘 받았다는 응답을 주는 것이기 때문에 메시지의 무결성도 중요하지 않기에 암호화 기법도 적용하지 않는다. 또한 주소필드가 수 바이트를 차지하기 때문에 주소 자체가 오버헤드(overhead)가 될 수 있는 이유로 주소필드도 ACK에 포함되지 않는다. 비록 'Sequence Number' 필드를 사용하기는 하지만 이 것은 ACK가 요구된 메시지에 포함되어 오는 값이기 때문에 공격자가 쉽게 획득할 수 있다. 따라서 공격자는 쉽게 ACK를 위조해서 보낼 수 있기 때문에 메시지의 성공적인 수신확인을 보장할 수 없다. 그림3은 ACK

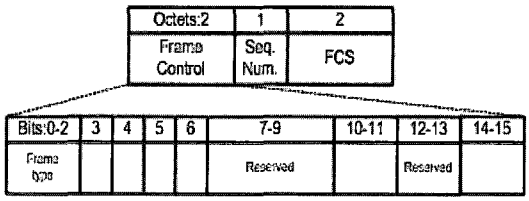


그림 3. IEEE802.15.4 ACK frame format

프레임 형식이다. 전체 5 바이트로 이루어져 있는데 주소필드가 없다. 즉 보내는 이와 받는 이가 전혀 명시되어 있지 않기 때문에 위에서 언급한 문제가 발생할 수 있다. 이 경우 'Frame Control' 필드 내에 Reserved 5 비트가 있는데 본 논문에서 제안한 URSC인증방식을 적용하면 ACK에 대한 origin 인증과 ACK에 대한 freshness를 함께 보장해 줄 수 있다.

Ⅵ. 결 론

지금까지 유일순차코드를 이용한 인증방법에 대해서 살펴보았다. 본 논문에서 제안한 인증방법은 네트워크 성능에 영향을 미치지 않고 보안성을 제공해 줄 수 있는 매우 경량화된 challenge-response 방식의 인증방법이다. PSC의 약점을 보완한 URSC를 이용하여 무선 센서 네트워크에서의 데이터 origin 인증과 freshness를 동시에 제공함으로써 여러 공격으로부터의 공격가능성을 줄일 수 있다.

참 고 문 헌

[1] Jinsoo Kim et al., "Frequency-hopping Optical Orthogonal Codes with Arbitrary Time-blank Patterns," *Applied Optics*, vol. 41, no. 20, pp.4070-4077, Jul. 2002.

[2] W. C. Kwong and G. C. Yang, "Construction of 2n Prime-sequence Codes for Optical Code Division Multiple Access," *IEE Proc.-Commun.*, vol.142, no.3, pp.141-150, Jun. 1995.

[3] Henric Hojohnson et al., "SOLA: A One-Bit Identity Authentication Protocol for Access Control in IEEE 802.11," in *IEEE GLOBECOM 2002.*

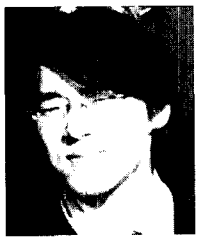
[4] Naveen Sastry and David Wagner, "Security Considerations for IEEE 802.15.4 Networks," in *ACM WiSe 2004.*

[5] Wireless medium access control and physical layer specications for low-rate wireless personal area networks. IEEE Standard, 802.15.4-2003, May 2003. ISBN 0-7381-3677-5.
[6] R. L. Rivest et al., "A method for obtaining digital signatures and public-key cryptosystems," *Comm. of the ACM*, vol. 21, no. 2, pp. 120 - 126, Feb. 1978.
[7] M. Bellare et al., "HMAC: Keyed hashing for message authentication," *RFC 2104*. Feb. 1997.

박 민 호 (Min-ho Park) 정회원

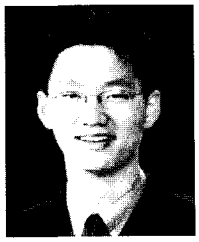
2000년 2월 : 고려대학교 전자공학(학사)
2002년 2월 : 고려대학교 전자공학(석사)
2005년 9월~현재 : 서울대학교 전기공학부 박사과정
<관심분야> 무선 네트워크, 센서 네트워크 보안

이 충 근 (Chung-Keun Lee) 정회원



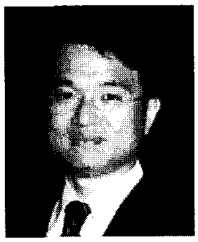
2000년 2월 : 서울대학교 전기공학(학사)
2002년 2월 : 서울대학교 전기공학(석사)
2002년 3월~현재 : 서울대학교 전기공학부 박사과정
<관심분야> 광통신 네트워크, 무선 네트워크

손 주 형 (Ju-Hyung Son) 정회원



2001년 2월 : 연세대학교 전자 공학(학사)
2003년 2월 : 서울대학교 전기 공학(석사)
2002년 3월~현재 : 서울대학교 전기공학부 박사과정
<관심분야> 무선 네트워크 보안, 센서 네트워크

서 승 우 (Seung-Woo Seo) 종신회원



1987년 2월 : 서울대학교 전기 공학(학사)
1989년 2월 : 서울대학교 전기 공학(석사)
1993년 12월 : 미국 펜실베니아 주립대학 전기공학(박사)
1990년~1991년 : 서울대학교 기초전력 주립대학 조교수
1993년~1994년 : 미국 펜실베니아 주립대학 전산기공학과 조교수
1994년~1996년 미국 프린스톤대학 전기공학 poem 연구소
1996년~현재 : 서울대학교 전기.컴퓨터공학부 부교수
<관심분야> 유/무선 네트워크, 네트워크 보안 알고리즘, 무선망 라우팅 및 다중 접속 기술, 센서네트워크