중첩된 무선 센서 네트워크 환경에서 동일한 네트워크에 속한 구성요소 간의 상호인증 방법[1]

민호근○ 임상섭 예홍진
아주대학교 정보통신 대학원○, 아주대학교 정보통신 전문대학원
hackytoss@ajou.ac.kr, leemss@ajou.ac.kr, hjyeh@ajou.ac.kr

A Mutual Authentication Method Between Entities of the Same Network in Multiple Wireless Sensor Networks

Min ho kun○ Leem sang seob Yeh hong jin
Ajou University Graduate School of Information&Communication

요 약

가까운 미래에는 저가의 센서노드가 대량으로 보급되어, 같은 공간에 서로 다른 다양한 무선 센서 네트워크(WSN)들이 동시에 존재하는 상황이 보편적일 것으로 예상된다. 본 논문에서는 이러한 환경에서 센서노드나 베이스스테이션이 서로 동일한 네트워크에 속한 것인지 여부를 확인하기 위한 상호인증 문제를 다루고자 한다. 모든 네트워크 구성요소가 동일한 형식의 식별자(Verifier)를 갖는다고 가정할 때, 식별자를 이용하여 각자 자기가 속한 네트워크를 구별하는 방법을 제안한다. 또한 식별자가 갖추어야 할 요건을 제시하고, 이와 같은 요건을 만족하는 식별자의 예를 보인다.

1. 서 론

최근 무선 센서 네트워크에 대한 관심이 높아지고 있는 가운데, 저전력의 무선통신과 고성능을 가진 마이크로 센서 제작 기술의 발달로 인하여 다양한 무선 센서 네트워크의 구축이 가능하게 되었다. 무선 센서 네트워크는 다양한 분야에 적용되어 유용한 서비스를 제공할 수 있기 때문에 앞으로 관련 분야의 시장 또한 매우 커질 것으로 예상되고 있다.[1, 2]

센서 제작 기술이 비약적으로 발전하면서 무선 센서 네트워크 구성요소들의 저가 공급 및 대량 생산이 가능해짐에 따라, 동일한 공간에 동질의 센서노드로 이루어진 다수의 개별적인 무선 센서 네트워크가 존재하는 환경이 발생하게 될 것이다.

이러한 환경에서 센서노드의 안전한 통신보다 우선적으로 해결해야 할 문제는 네트워크 구성요소들을 구별하는 방법이다. 예를 들어, 홈 네트워크 환경에서 동질의 센서노드들을 이용하여 개인화 서비스를 제공할 때, 각 센서노드는 다른 네트워크에 속한 센서노드와 혼동되어서는 안 되기 때문에 이들을 서로 구별해야 할 필요가 있다.

1 본 연구는 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업의 일환으로 수행하였음. [2008-S-027-01, IP 기반 센서네트워크 기술개발]

센서 네트워크 보안을 위해 초기에 제안된 대표적인 인증 메커니즘으로 A. Perrig, R. Szewczyk, V. Wen, D. Culler, 그리고 J.D. Tygar는 SPINS(Security Protocols for Sensor Networks)를 제안하였다.[3] SPINS는 데이터의 기밀성, 인증, 무결성을 제공하기 위한 SNEP와 데이터 브로드캐스트 인증을 보장하기위한 μTESLA로 구성된다. 안전한 통신을 위하여 베이스스테이션과 센서노드는 하나의 마스터키를 사전 분배받는다. 각 센서노드는 카운터 값과 마스터키로부터 유도된 암호화키를 이용하여 데이터를 암호화하고, 암호문에 카운터 값을 포함하여 MAC 키로 MAC값을 만들어 전송하는 방식을 사용한다.

SPINS는 동일한 공간에 동질의 센서노드를 사용하여 다수의 무선 센서 네트워크를 구성하는 경우를 고려하지 않고 있다. 즉, 공격자가 동일한 프로토콜을 이용하면서 네트워크에 침입했을 때 마스터키가 단 한번이라도 노출된다면, 전체 네트워크가 치명적인 위험에 빠질 수 있다.

M. Younis, M. Youssef 그리고 K. Arisha는 무선 센서 네트워크에서 각 센서노드에 키를 분배하는 방법 중 하나인 Identity Based Symmetric Keying(IBSK)[4]을 확장한 키 관리 프로토콜을 제안하였다.[5] 각 센서노드에 유일한 ID를 부여하고, 베이스스테이션이 ID별로 키를 유지 및 분배하는 방법을 사용한다.

이 프로토콜은 각 센서노드에 유일한 ID를 사전에 분배하여 베이스스테이션이 이러한 ID 정보를 모두 유지해

야 한다. 이를 이용하여 자신의 네트워크 내의 센서노드들을 구별하는 방식을 취하고 있다.

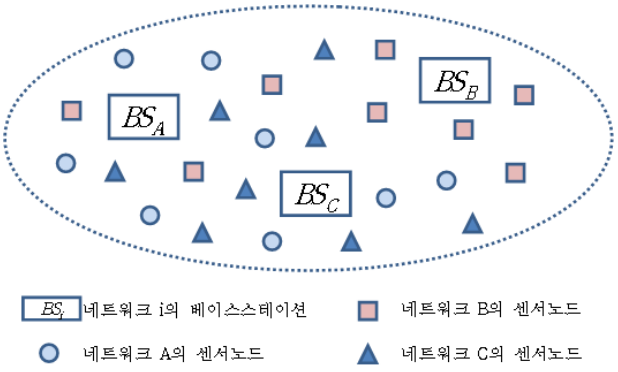
본 논문에서는 동일한 공간에 동질의 센서노드들을 이용하여 다수의 개별적인 무선 센서 네트워크가 설치되어 있는 환경에서, 베이스스테이션과 센서노드가 각자 가지고 있는 정보만을 유지하면서 다른 네트워크 요소들이 자신과 같은 네트워크에 속하는지를 구별할 수 있는 새로운 식별자 및 구별방법을 제안하였다.

이와 같은 접근은 사용자 중심의 네트워크 환경으로서 사용자가 처한 상황이나 환경을 네트워크가 지능적으로 파악하여 언제 어디에서나 네트워크에 편리하게 연결될 수 있도록 할 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 문제정의를 기술하며, 3장에서는 본 논문에서 제안한 구별방법의 자세한 소개 및 분석을 다루며, 4장에서는 식별자가 갖추어야 할 요건에 대해서 생각하고, 5장에서는 결론을 맺는다.

2. 문제정의

본 논문에서는 Ad-hoc WSN(Wireless Sensor Network)을 가정한다. 이러한 가정 하에 동일 공간에 여러 네트워크가 존재하게 되면, 각 네트워크 구성 요소들은 전송거리 내에 존재하는 다른 네트워크 구성 요소들의 신호를 감지할 수 있게 된다.



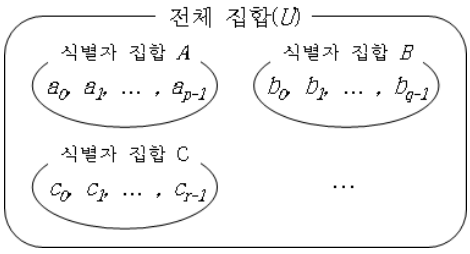
[그림 1] 동일 공간에 설치된 다수의 네트워크 예

예를 들어, [그림 1]과 같이 동일한 공간에 세 개의 네트워크가 존재할 때, 네트워크 A에 속하는 센서노드나 베이스스테이션이 주고받는 메시지를 네트워크 B 또는 C에 속하는 센서노드나 베이스스테이션이 수신할 수 있게 된다. 그러므로 네트워크 구성 요소들 사이의 상호인증 방법이 필요하다.

3. 제안방법

3.1 네트워크 식별자 부여방법 및 표기법

본 논문에서 제안하는 식별 프로토콜을 사용하기 위해서 각 네트워크에 사전 분배되는 식별자는 다음 그림과 같다.



[그림 2] 식별자 집합 다이어그램

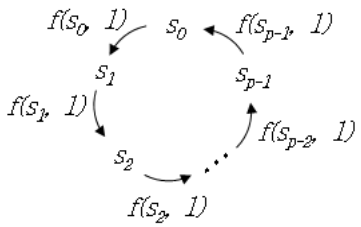
전체 집합을 $k+1$개로 분할하고, 이 중 하나의 구획은 식별자로 사용하지 않으면서 전체 집합에서 상대적으로 큰 비중을 차지한다. 무선 센서 네트워크는 나머지 k개의 집합 중 하나의 식별자 집합을 사전 분배받아야 하며, 다른 네트워크에 중복적으로 분배되지 않아야 한다. 하나의 식별자 집합은 다음과 같이 정의한다.

$$S = \{ s_0, s_1, s_2, \cdots, s_{p-1} \} \quad (n \le p-1)$$

여기서 n은 하나의 네트워크에 속하는 센서노드의 개수이고, p는 식별자의 최대 개수를 지칭한다. s_i는 i번째 센서노드의 식별자이며, 특히 s_0는 베이스스테이션의 식별자로 사용된다. 따라서 하나의 베이스스테이션은 최대 $p-1$개의 센서노드를 가질 수 있다. 이러한 식별자를 구별하기 위하여 다음과 같은 함수 모델을 정의한다.

$$f(s_i, k) = s_{(i+k \bmod p)}$$
$$g(s_{(j+k \bmod p)}, s_j) = k$$

함수 $f()$는 식별자 s_i와 임의의 수 k를 입력받으면, 식별자 $s_{(i+k \bmod p)}$를 결과로 얻을 수 있게 된다. [그림 3]은 함수 $f()$의 동작모습을 보여준다.

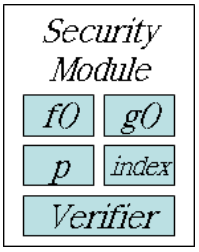


[그림 3] 함수 $f()$의 동작모습

함수 $g()$는 식별자 s_i와 $s_{(i+k \bmod p)}$를 입력받으면, k를 결과로 얻을 수 있다. 만일 입력되는 두 식별자가 서로 다른 네트워크에 속하는 경우, 그 결과는 -1이 된다.

$$g(s_i, t_j) = -1 \quad (s_i \in S, t_j \notin S)$$

네트워크 구성 요소인 베이스스테이션과 센서노드는 다음과 같은 보안 모듈을 포함하고 있다고 가정한다.



[그림 4] 보안 모듈의 구성요소

위의 그림에서 각 항목은 다음과 같다.

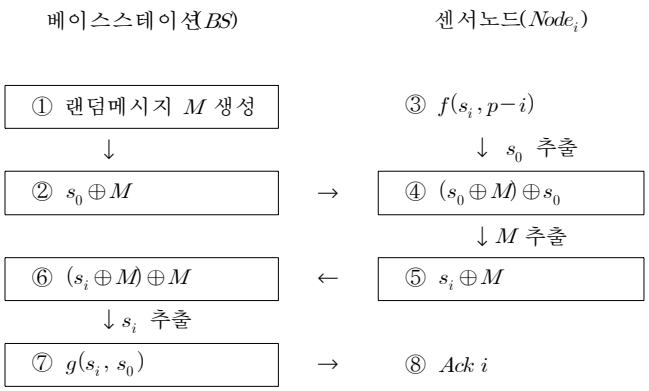
$f()$: 같은 네트워크에 속한 식별자 집합을 생성하기 위한 함수
$g()$: 같은 네트워크에 속한 네트워크 구성요소인지를 알아보기 위한 함수
p : 네트워크 내에서 사용 가능한 식별자의 최대 개수
$index$: 자신의 식별자 번호
$Verifier$: 자신의 식별자

3.2 구별방법

이 절에서는 2장에서의 가정을 기반으로 하여, 베이스스테이션에 의한 센서노드 식별과정, 센서노드에 의한 베이스스테이션 식별과정, 그리고 센서노드 상호 식별과정을 보인다.

3.2.1 베이스스테이션에 의한 센서노드 식별

[그림 5]는 하나의 네트워크에 속한 BS가 동일한 네트워크에 속한 $Node_i$를 식별하는 과정을 나타낸 것으로, 주요 흐름은 다음과 같다.



[그림 5] 베이스스테이션에 의한 센서노드 식별과정

① BS가 메시지 M을 랜덤 생성한다.

$$BS: M$$

② BS는 자신의 식별자 s_0와 랜덤메시지 M의 Exclusive-OR 결과 값을 브로드캐스트한다.

$$BS: (s_0 \oplus M) \rightarrow Node_{ALL}$$

③ $Node_i$는 자신의 식별자 s_i와 자신의 $index$ i를 이용하여 BS의 식별자 s_0를 계산한다.

$$Node_i : f(s_i, p-i) = s_{(i+p-i \bmod p)} = s_0$$

④ $Node_i$는 BS로부터 받은 메시지에 BS의 식별자 s_0를 Exclusive-OR하여 M을 계산한다.

$$Node_i : (s_0 \oplus M) \oplus s_0 = M$$

⑤ $Node_i$는 자신의 식별자 s_i와 메시지 M의 Exclusive-OR 결과 값을 BS에게 전송한다.

$$Node_i : (s_i \oplus M) \rightarrow BS$$

⑥ BS는 $Node_i$로부터 받은 메시지와 $Node_i$에게 전송했던 랜덤메시지 M을 Exclusive-OR하여 $Node_i$의 식별자 s_i를 추출한다.

$$BS: (s_i \oplus M) \oplus M = s_i$$

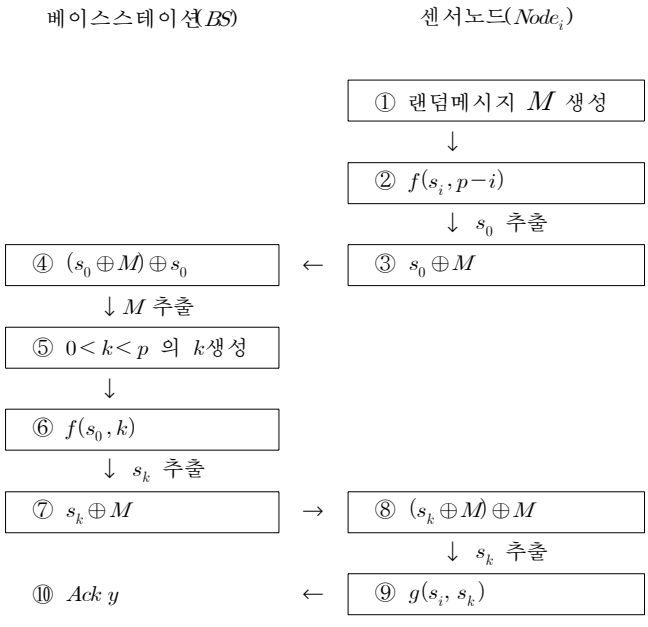
⑦ BS는 추출된 식별자 s_i로부터 i를 추출한다.

$$BS: g(s_i, s_0) = i$$

⑧ 계산 결과 i를 보고 동일한 네트워크에 속하는 $index$ i번째 센서노드라고 판단하고 응답메시지 $Ack\ i$를 $Node_i$에게 전송한다.

3.2.2 센서노드에 의한 베이스스테이션 식별

[그림 6]는 하나의 네트워크에 속한 $Node_i$가 동일한 네트워크에 속한 BS를 식별하는 과정을 나타낸 것으로, 주요 흐름은 다음과 같다.



[그림 6] 센서노드에 의한 베이스스테이션 식별과정

① $Node_i$가 메시지 M을 랜덤 생성한다.

$$Node_i : M$$

② $Node_i$는 자신의 식별자 s_i와 자신의 $index$ i를 이용하여 BS의 식별자 s_0를 계산한다.

$$Node_i : f(s_i, p-i) = s_{(i+p-i \bmod p)} = s_0$$

③ $Node_i$는 랜덤메시지 M과 BS의 식별자 s_0의 Exclusive-OR 결과값을 BS에게 전송한다.

$$Node_i : (s_0 \oplus M) \rightarrow BS$$

④ BS는 $Node_i$로부터 받은 메시지에 자신의 식별자 s_0를 Exclusive-OR하여 M을 계산한다.

$$BS : (s_0 \oplus M) \oplus s_0 = M$$

⑤ BS는 0과 p사이의 임의의 수 k를 생성한다.

$$BS : k$$

⑥ BS는 자신의 식별자 s_0와 k를 이용하여 다른 센서노드가 가진 식별자 s_k를 추출한다.

$$BS : f(s_0, k) = s_k$$

⑦ BS는 추출한 s_k와 M을 Exclusive-OR하여 $Node_i$로 전송한다.

$$BS : (s_k \oplus M) \rightarrow Node_i$$

⑧ $Node_i$는 BS로부터 받은 메시지와 BS에게 전송했던 랜덤메시지 M을 Exclusive-OR하여 다른 $Node_k$의 식별자 s_k를 추출한다.

$$Node_i : (s_k \oplus M) \oplus M = s_k$$

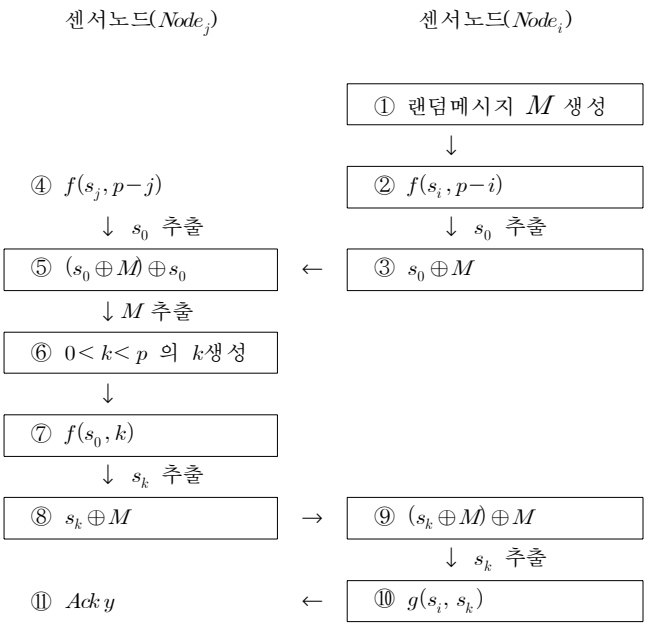
⑨ $Node_i$는 추출된 식별자 s_k로부터 y를 추출한다.

$$Node_i : g(s_i, s_k) = y$$

⑩ 계산 결과 y를 보고 동일한 네트워크에 속하는 BS라고 판단하고 응답메시지 $Ack\ y$를 BS에게 전송한다.

3.2.3 센서노드 상호 식별

[그림 7]은 하나의 네트워크에 속한 $Node_i$가 $Node_j$를 식별하는 과정을 나타낸 것으로, 주요 흐름은 다음과 같다.



[그림 7] 센서노드 상호 식별과정

① $Node_i$가 메시지 M을 랜덤 생성한다.

$$Node_i : M$$

② $Node_i$는 자신의 식별자 s_i와 자신의 $index\ i$를 이용하여 BS의 식별자 s_0를 계산한다.

$$Node_i : f(s_i, p-i) = s_{(i+p-i \bmod p)} = s_0$$

③ $Node_i$는 랜덤메시지 M과 BS의 식별자 s_0의 Exclusive-OR 결과값을 $Node_j$에게 전송한다.

$$Node_i : (s_0 \oplus M) \rightarrow Node_j$$

④ $Node_j$는 자신의 식별자 s_j와 자신의 $index\ j$를 이용하여 BS의 식별자 s_0를 계산한다.

$$Node_j : f(s_j, p-j) = s_{(j+p-j \bmod p)} = s_0$$

⑤ $Node_j$는 $Node_i$로부터 받은 메시지에 BS의 식별자 s_0를 Exclusive-OR하여 M을 계산한다.

$$Node_j : (s_0 \oplus M) \oplus s_0 = M$$

⑥ $Node_j$는 0과 p사이의 임의의 수 k를 생성한다.

$$Node_j : k$$

⑦ $Node_j$는 BS의 식별자 s_0와 k를 이용하여 다른 센서노드가 가진 식별자 s_k를 추출한다.

$$Node_j : f(s_0, k) = s_k$$

⑧ $Node_j$는 추출한 s_k와 M을 Exclusive-OR하여 $Node_i$로 전송한다.

$$Node_j : (s_k \oplus M) \rightarrow Node_i$$

⑨ $Node_i$는 $Node_j$로부터 받은 메시지와 $Node_j$에게 전송했던 랜덤메시지 M을 Exclusive-OR하여 다른 $Node_k$의 식별자 s_k를 추출한다.

$$Node_i : (s_k \oplus M) \oplus M = s_k$$

⑩ $Node_i$는 추출된 식별자 s_k로부터 y를 추출한다.

$$Node_i : g(s_i, s_k) = y$$

⑪ 계산 결과 y를 보고 동일한 네트워크에 속하는 $Node$라고 판단하고 응답메시지 $Ack\ y$를 $Node_j$에게 전송한다.

3.3 식별자 집합의 예시

이 절에서는 본 논문에서 제안한 식별자 집합의 예를 제시하여, 서로 다른 네트워크에 속하는 네트워크 구성 요소간의 상호인증이 가능함을 보인다.

3.1절에서 가정한 조건들을 만족하는 식별자 집합은 매우 다양한 방법으로 생성될 수 있을 것이다. 우리는 Cellular Automata 기법을 이용하여 아래와 같은 16비트의 길이의 식별자 집합을 생성하였다.

$$S = \{\ 1110101000000000,\\ 1010101000000100,\\ 1010000001000100,\\ 0100010000001110,\\ 0000000010101110,\\ 0100000010101010,\\ 0100010000001010,\\ 1110000001000100\ \}$$

이 식별자 집합의 각각의 비트열을 Rotate시키면 추가적으로 15개의 식별자 집합을 생성할 수 있다. 따라서 전체 집합은 17개의 식별자 집합으로 분할되며, 이 중 하나의 구획은 식별자로 사용하지 않으면서 전체 집합에서 상대적으로 큰 비중을 차지하게 된다.

네트워크 식별과정을 설명하기 위해 두 개의 네트워크에 S와 T가 아래와 같은 식별자 집합을 사전분배 받았다고 가정하자. 여기서 식별자 집합 T는 식별자 집합 S 각각의 비트열을 8비트 Rotate시켜 생성하였다.

S = { 1110101000000000, 1010101000000100, 1010000001000100, 0100010000001110, 0000000010101110, 0100000010101010, 0100010000001010, 1110000001000100 }

T = { 0000000011101010, 0000010010101010, 0100010010100000, 0000111001000100, 1010111000000000, 1010101001000000, 0000101001000100, 0100010011100000 }

식별자 집합 S의 첫 번째 식별자 s_0 : "1110101000000000"는 네트워크 S의 베이스스테이션(BS_S)의 식별자로 사용되며 마찬가지로 식별자 집합 T의 첫 번째 식별자 t_0 : "0000000011101010"는 네트워크 T의 베이스스테이션(BS_T)의 식별자로 사용된다.

3.2절에서 제안한 방법으로, BS_S가 자신의 네트워크에 속하는 센서노드들을 구별하는 과정을 생각해 보자. 이 경우에는 먼저 BS_S가 $(s_0 \oplus M)$를 주위의 모든 노드에게 브로드캐스트 한다. 이 때, 집합 T를 식별자로 사용하는 네트워크의 t_k를 식별자로 사용하는 센서노드가 응답하는 경우를 생각해보자.

t_k를 식별자로 사용하는 센서노드는 BS_S가 브로드캐스팅 메시지를 수신하고, 다음과 같은 순서로 계산한다.

자신의 p와 $index$를 기반으로 t_0을 계산하여 받은 메시지와 Exclusive-OR 연산을 통하여 랜덤메시지를 추출한다.

$$(s_0 \oplus M) \oplus t_0$$

t_k를 식별자로 사용하는 센서노드는 이와 같은 연산의 결과를 메시지 M으로 잘못 해석하고 자신의 식별자와 Exclusive-OR 결과 $(s_0 \oplus M) \oplus t_0 \oplus t_k$를 BS_S에게 전송하게 된다. BS_S는 전송받은 메시지로부터 센서노드의 식별자를 추출하기 위해 다음과 같이 계산한다.

$$BS_S : (s_0 \oplus M) \oplus t_0 \oplus t_k \oplus M = s_0 \oplus t_0 \oplus t_k$$

이 결과가 $s_0 \sim s_{p-1}$ 사이의 식별자에 존재하게 되면 같은 네트워크의 센서노드로 판단하게 되므로, S 에 존재하지 않아야 한다. 이를 검증하기 위하여 위의 식을 일반화하면 다음과 같다.

$$s_0 \oplus t_0 \oplus t_k \neq s_j$$

양변에 s_0를 Exclusive-OR하면 다음의 식을 얻을 수 있다.

$$t_0 \oplus t_k \neq s_0 \oplus s_j$$

그러므로 각 식별자 집합의 식별자들을 베이스스테이션의 식별자와 Exclusive-OR 연산의 결과들의 집합이 상호 배제되어야 한다. 이는 실험을 통하여 검증하였다.

[표 1]은 식별자의 비트를 늘림으로써 확장할 수 있는 센서노드의 수와 구별할 수 있는 네트워크의 수를 나타낸다.

L	#N	#V	R
16	16	8	2^{-9}
32	256	64	2^{-18}
48	4,096	512	2^{-27}
64	65,536	4,096	2^{-36}

[표 1] 식별자의 확장성

위의 표에서 각 항목은 다음과 같다.

L : 식별자의 길이(비트 수)
#N : 네트워크의 최대 개수
#V : 하나의 네트워크 내 최대 식별자의 개수
R : 전체 비트열 중 식별자로 사용되는 비율

4. 식별자 요건에 대한 논의

이 장에서는 무선 센서 네트워크의 식별자 요건들을 생각해 보고 제안한 식별자가 이러한 요건들을 만족하는지 검토해 본다.

여기서는 베이스스테이션이 센서노드들을 식별하는 과정만을 검증하고, 센서노드에 의한 베이스스테이션 식별과정과 센서노드 상호간 식별과정은 베이스스테이션에 의한 센서노드 식별 과정과 유사하므로, 분석과정은 생략한다.

1) 각 네트워크들을 명확히 구별할 수 있어야 한다.

베이스스테이션은 식별자 집합의 특성을 이용하여 자신의 네트워크에 속한 센서노드들을 자신의 네트워크로 판단함을 앞의 3.2절에서 보였다.

다른 네트워크에 속해있는 센서노드들을 자신의 네트워크에 속하는 센서노드가 아님을 판단하는 것도 중요하다.

2) 외부에 노출되지 않아야 한다.

2.1절의 네트워크 모델 가정에서 보안모듈 자체는 물

리적 보안장치가 되어있다고 가정했으며, 또한 식별과정에서 랜덤 문자열과 Exclusive-OR 결과를 전송함으로써 식별자 자체를 직접적으로 노출하지 않는다.

3) 공격자가 위조된 식별자를 사용하기 어려워야 한다.

식별자 집합은 하나의 특정한 규칙을 가지고 순차적으로 생성하는 방식을 취하지 않는다. 다양한 방법을 통해서 식별자 집합을 생성해 낼 수 있으므로, 한 네트워크 내의 베이스스테이션과 모든 센서노드의 식별자를 수집하지 않고서 임의적으로 식별자를 생성해 내기 어렵다.

4) 식별을 위한 계산량이 적어야 한다.

식별자 계산을 위해 베이스스테이션은 두 번의 Exclusive-OR 연산과 한 번의 함수 $g()$를 사용하고, 센서노드는 한 번의 함수 $f()$ 사용과 두 번의 Exclusive-OR 연산을 사용하여 센서노드를 식별하고 있다.

5) 식별을 위한 데이터 전송량이 많지 않아야 한다.

베이스스테이션은 센서노드를 식별하기 위해 단 하나의 메시지를 브로드캐스팅하고 노드별로 하나씩의 메시지를 받음으로써, 동일한 네트워크에 속하는지의 여부를 판단할 수 있다.

6) 한 네트워크 식별자를 이용하여 다른 네트워크의 정보를 알 수 없어야 한다.

한 네트워크의 모든 식별자 집합을 가지고 있는 경우에, 다른 네트워크의 정보를 획득할 수 있다면 문제가 발생한다. 제안한 식별 방법에서 자신의 네트워크에 속하는지 여부만을 판단할 수 있기 때문에 다른 네트워크의 정보를 파악할 수 없다.

5. 결론

지금까지 특정한 식별자 집합을 이용하여 네트워크별로 네트워크 구성요소들을 구별하는 방식의 프로토콜에 대해서 살펴보았다. 이 프로토콜은 제한된 자원을 가진 센서노드의 특징을 고려하여, 어떠한 복잡한 암호학적 연산도 요구하지 않으면서 성공적인 식별을 보장하였다.

이러한 식별자를 이용하여 네트워크를 구별함과 동시에 각 센서노드들을 구별할 수 있으므로 초기화 과정에서 센서노드의 응답여부를 확인할 수 있다. 이러한 속성을 활용하면 네트워크 내부의 식별자를 대체할 수 있을 것을 생각된다.

우리는 3.3절에서 보인 식별자 집합의 예시 이외에도 다른 여러 가지 방법을 통하여 식별자 집합을 생성하는 방법에 대한 연구계획을 가지고 있다. 본 논문에서 제안한 식별자 집합을 이용하여, 보안 목적 이외에도 다양한 분야에서 활용할 수 있을 것으로 기대된다.

6. 참고문헌

[1] M. Horton, et al., “Mica: The commerciatlization of microsensor motes”, Sensors Online Magazine, April 2002.

[2] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, “energy Efficient Communication protocol for Wireless Microsensor Networks”, Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, pp. 3005-3014, Jan. 2000.

[3] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar. “SPINS:Security protocols for sensor networks”, The Seventh Annual International Conference on Mobile Computing and Networking (MobiCom 2001), Rome, Italy, July 16-21, 2001.

[4] D. Carman, P. Kruus, and B. Matt, “Constraints and approaches for distributed sensor network security,” Tech. Rep. 00-010, NAI Labs, September 2000.

[5] M. Younis, M. Youssef, and K. Arisha, “Energy-Aware Routing in Cluster-Based Sensor Networks,” in Proceedings of the 10th IEEE/ACM MASCOTS2002, October, 2002.