논문 2006-43TC-7-2

정적 무선 센서 네트워크를 위한 강한 연결성을 가진 계층적 그리드 기반의 키 선분배 기법

(Strongly-Connected Hierarchical Grid-Based Pairwise Key Predistribution Scheme for Static Wireless Sensor Networks)

양 대 헌*, 모하이센 아브델아지즈**

(DaeHun Nyang and Mohaisen Abedelaziz)

요 약

무선 센서 네트워크(Wireless Sensor Network, WSN)는 작고 값이 싸지만 매우 제한된 자원을 가진 많은 수의 센서로 구성된다. 이러한 자원의 부족으로 인하여 공개키 암호화방식은 WSN에 사용하기 적합하지 않으며, 비밀키 암호화방식을 적용사키기 위하여는 키 관리와 선분배 기법이 필요하다. 많은 키 선분배 기법이 제안되었지만 대부분의 이러한 기법은 실제 WSN의 환경을 충분히 고려하지 않고 있다. 이 논문에서는 적당한 통신량과 연결을 고려한 WSN을 위하여 계층적 그리드(Grid)를 기반으로 하는 보안 프레임워크를 제안한다. 프레임워크의 보안성을 검증하기 위하여 간단한 키 개체 분배 기법을 적용하였으며, WSN에서 가능한 보안 위협에 대하여 분석하였다.

Abstract

Wireless Sensor Network(WSN) consists of huge number of sensor nodes which are small and inexpensive with very limited resources. The public key cryptography is undesirable to be used in WSN because of the limitations of the resources. A key management and predistribution techniques are required to apply the symmetric key cryptography in such a big network. Many key predistribution techniques and approaches have been proposed, but most of them didn't consider the real WSN assumptions. In this paper, we propose a security framework that is based on a hierarchical grid for WSN considering the proper assumptions of the communication traffic and required connectivity. We apply simple keying material distribution scheme to measure the value of our framework. Finally, we provide security analysis for possible security threats in WSN.

Keywords : Wireless Sensor Networks, Pair-wise Key, Hierarchical Grid

Ⅰ. 서 론

센서는 제한된 자원을 가지고 있는 값싸며 낮은 연산 능력을 가진 장치로 작은 사이즈와 짧은 거리의 제한된 무선 통신 능력을 가지고 있다.[1] 일반적인 센서 노드는 전원부(power unit)와 감지부(sensing unit), 그리고 연산부(processing unit), 저장부(storage unit), 무선 통신 장치(wireless transceiver)를 가지고 있다. WSN는 제한된 저장 공간과 이동성을 가진 많은 수의 센서 노드를 포함한다. 마이크로 센싱과 센서 노드들의 무선 연결은 군사적 이용이나, 환경, 건강과 관련한 많은 여러 상업적 영역을 가능하게 한다.[1] WSN의 자원에 대한 특성으로 인하여 Deffie-Hellman 키 교환[6]이나 RSA 서명[17]과 같은 공개키 암호화 알고리즘은 WSN에서 사용하기 힘들다. 또한 사용한다고 하더라도 수십 초에서 수분이 소요되기 때문에 서비스 거부 공격(Denial of Service attacks)의 위험성에 노출되어 있다.[19] 하지만 그렇다고 하더라도, 이를 WSN에 사용하기 위하여 현

* 정회원, ** 비회원, 인하대학교 정보통신대학원
(Graduate School of Information Technology and Telecommunication, Inha University)
접수일자: 수정완료일:

재의 공개키 암호화 알고리즘을 수정하려는 노력이 진행 중에 있다.

위와 같은 이유로, WSN에서의 보안에는 주로 비밀키 암호화 방식이 사용되고 있다. WSN의 제한된 자원으로 말미암아, 보안과 관련된 연구의 주된 내용은 비밀키 암호화 방식에서 어떻게 키를 분배할 것이냐 하는 것에 모아지고 있다.[8] 때때로 센서 노드들은 연결이 끊어지거나 키가 뿌려진 뒤에는 이를 바꾸지 않기 때문에, 오프라인 상에서 비밀키를 할당하거나 분배하는 키 선분배 기법들이 많이 제안되었다.

WSN과 관련하여 이미 여러 키 선분배 기법이 존재하지만, 이 논문과 관련한 기법은 초기에 제시된 Eschenauer-Gligor(EG) 기법[8]과 Blom 기법[2], 이 둘에 기반 하는 다중 공간(multi-space) 기법[7], 그리고 다항식을 이용하는 Blundo 기법[3] 등이 있다. [16]에서는 SPINS라는 불리는 특별히 설계된 센서 네트워크 보안 구조를 제시하였으며 [18]에서는 [3]을 바탕으로 하는 보안 구조가 제시되었다.

이 논문에서는 프레임워크로써 계층적 그리드(Hierarchical Grid)를 사용하고 키 생성 방법으로 Blundo의 기법에 바탕 하는 새로운 기법을 제안한다. 이 논문에서 우리는 1) 키를 설정하기 위한 완벽한 연결성을 제공하는 확장 가능하고(scalable) 견고한 특성을 갖는 참신한 키 분배 프레임워크를 제시하고 2) 다른 WSN 자원, 특히 통신량과 메모리사용량, 그리고 연상 능력에 대한 최적화에 관한 내용과 3) 제안하는 기법에 대한 이론적으로 계산적인 증명에 대한 분석을 보일 것이다. 그리고 4) 제안하는 기법에 대한 모든 가능한 보안 위협의 대응 수단과 이와 관련한 토의를 수행할 것이다.

Ⅱ. 배경 기법들

키 선분배(Key Predistribution) 메커니즘은 현재 진행 중인 연구들의 중요 토픽이거나 과거 몇 년 동안 연구되어 여러 기법이 존재한다. 그러한 기법에 대한 자세한 조사는 Camtep와 Yener에 의해서 [4]에 기술되어 있다. WSN의 초기 키 선분배 기법은 Eschenauer-Gligor(EG) 기법이다.[8] 이 기법에서 각각의 노드는 키의 집합 S_k를 커다란 키 저장소 P로부터 무작위로 선택되어 주어진다. 그리고 센서 노드가 뿌려진 후, 다른 노드들의 다른 S_k는 두 노드 간에 하나의 비밀키를 공유할 확률적 연결성 값(probabilistic connectivity value) p_c가 주어지게 된다. 노드 i, j가 키를 만들 필요가 있을 때, 공유키 $k \in S_{k_i} \cap S_{k_j}$를 사용할 수 있을 것이다. 만약 공유키가 존재하지 않는다면, 중간의 노드를 통한 경로 키 설정(path key establishment)이 실행된다. EG 기법의 탄력성을 높이기 위해서는 Chan은 키 저장소를 다시 디자인하고 키 링 S_k를 q-composite를 사용하는 저장소에서 꺼내는 방식으로 EG 기법을 업그레이드한 기법을 제시하였다.[5]

키가 필요하고, q개의 공유된 키 $k_1, k_2, \cdots, k_q \in S_{k_i} \cap S_{k_j}$가 있을 때, $hash(k_1 \| k_2 \| \cdots \| k_q)$가 비밀키가 된다. 만약 q개보다 작은 n개의 키가 공유되었을 때에는, 두 노드는 한 개 이상의 중간 노드를 통한 키 설정을 실행한다.

다른 기법으로는 Blom 기법이 있다.[2] 이 기법에서는 어떠한 두 노드 $(i, j) \in N$가 그들의 고유한 공유된 비밀키를 갖도록 한다. 사이즈가 N인 네트워크에서 가장 높은 연결성을 가질 때는 노드 자신으로부터 각각 다른 외부 패스(outgoing path)에 다른 비밀키를 사용할 때이고, 구현 가능한 모든 키는 $N \times N$ 크기의 대칭 행렬(symmetric matrix)에서 찾을 수 있다. [2]에서 저자는 이러한 행렬을 생성하는 $(\lambda+1) \times N$ 크기의 공개 행렬 G 와 $(\lambda+1) \times (\lambda+1)$ 크기의 무작위로 생성되는 비밀 대칭 행렬 D 를 소개하였다. A 를 $N \times (\lambda+1)$ 크기의 행렬로 $(DG)^T$ 라고 정의할 때, 네트워크에서 각각의 노드는 행렬 A의 열에 해당하는 행을 행렬 G에서 찾을 수 있다. 만약 노드 i와 j 사이에서 비밀키가 필요하다면 공유된 비밀키를 생성하기 위하여 행렬 A의 i번째 열과 행렬 G의 j번째 행이 선택되어 곱해진다.

EG 기법과 Blom 기법에 기반하여, Du는 각각의 노드가 저장해야하는 데이터는 해당하는 열과 행을(각각 A_{R_j}와 G_{C_j}) 저장하는 기법을 제안하였다.[7] 다중 공간(multi- space) 기법은 ω개의 미리 계산된 행렬로부터 무작위로 선택된 τ개의 비밀 행렬 D를 고려하는 기법으로 제안되었으며, 다른 A들은 다른 D에서 생성된다. 다른 A의 τ개의 열들은 선택되고 각각의 노드에게 나눠진다. 두 노드 (i, j)사이에 비밀키가 필요할 때, 우선 키 협상 과정(key agreement phase)이 사용되고 있는 공간에서 수행된다. 만약 어떠한 공간 $\tau_{i,j} \in \tau_i \cap \tau_j$가 존재한다면 Blom 기법의 나머지 부분을 계속한다. 그렇지 않다면 하나나 그 이상의 중간 공간을 이용하는 경로 키 설정 과정을 수행한다. 이 기법에서 필요한 메모

리양과 키를 복원하기 위한 계산량 및 공간 ID를 알리기 위해 이루어지는 통신양은 다름 기법들 보다 큰 편이다. 이 기법의 연결성은 EG 기법에 비해서는 상대적으로 낮은 편이지만 탄성력은 EG 기법보다 좋다.

Blundo는 다항식을 이용한 동적인 협의 환경(dynamic conference environment)에서의 비밀키 분배 방법을 제시하였다.[3] 이 기법에서는 파티 사이에서 t차 대칭 이변 다항식(symmetric bivariate polynomial)이 공유하고 분배된다. 이 다항식은 네트워크에서 안전한 연결을 위해서 필요한 비밀키를 생성하기 위해 각각의 파티를 위한 어떠한 고유한 시드(seed)를 사용한다.

$$f(x,y)=\sum_{i,j=0}^{t} a_{ij}x^{i}y^{j} \ (a_{ij}=a_{ji}) \tag{1}$$

$$g_{ID}(x)=f(x,ID) \tag{2}$$

아직 필드에 노드들이 뿌려지기 전, 각각의 노드는 계산된 대칭 이변 다항식 $g_{ID}(x)$를 갖는다. 어떠한 노드는 다른 노드의 ID를 이 다항식에 입력하여 나온 결과 값을 취한다. 연산량을 줄인 Blundo 기법의 효율적인 구현은 S. Schmit가 기술하였다.[18]

Liu-Ning 기법에서, 다른 노드들이 격자(grid)의 다른 교차점에 위치한다는 가정 하에 2차원 환경을 사용하는 방법이 제안되었다.[12] 앞서 언급되었던 Blundo 기법을 다른 대칭 이변 다항식을 갖는 격자 형태에 적용시킨 것이다. 같은 열이나 행에 속하는 어떠한 두 노드는 같은 대칭 이변 다항식을 갖기 때문에 Blundo 기법에서는 공유 비밀키를 곧바로 구할 수 있다. 그러나 곧바로 구할 수 없을 때(즉, $R_i \neq R_j$이고 $C_i \neq C_j$일 때) 중간 노드를 이용한 경로 키 설정 단계를 거쳐야 한다. 이 기법은 단순해보이지만 보안 채널을 만들기 위하여 높은 확률로 좋은 연결성을 지원한다. 어떠한 노드들이 공격자의 손에 넘어갔을 때에도 네트워크는 다른 노드들을 이용한 경로를 선택함으로써 안전하게 비밀키를 생성해낼 수 있다. 한편, 노드는 통신량을 줄이는 다른 노드들을 통하여 비밀키를 설정할 수 있는지 없는지 결정할 수 있다. 그러나 이 기법에서 요구하는 연산능력은 $t+1$개의 대칭 이변 다항식을 계산하여야 하기 때문에 상대적으로 높은 편이다. 키 경로에서 중간 노드를 이용하는 방법은 연산이나 통신량에서 효율적이지 않다.

Ⅲ. 계층적 그리드 기반의 키 선분배 기법

제안하는 기법에서는 WSN에 더 적합하고 높은 연결성을 보장하는 분배 영역(deployment zone)을 사용하였다. 이 네트워크 영역은 그리드(Grid) 형태로 이루어지며 계층적 구조를 가지고 있다. 제안하는 기법은 Blundo 기법에서 다른 네트워크 영역에 다른 다항식을 사용하여 키 요소를 생성하는 부분이 수정 및 첨가되었다. 이렇게 함으로써 $(t+1)$개의 노드들이 공격당한다고 해도 이러한 공격은 관련된 다항식 영역에만 영향을 주게 되며, 서로 다른 t차 다항식을 사용하는 것은 공격으로부터의 보안 레벨과 사용하는 다항식에 따라 더 많은 연산을 수행하는 것으로 통신을 여전히 유지할 수 있게 한다.

1. 용어의 정의

다음의 용어 및 정의는 이 논문의 나머지 부분에서 사용되는 것들이다.

- 네트워크 수위(Network Order) n: 네트워크의 크기와 각각의 센서 노드에서 사용되는 대칭 이변 다항식의 수를 결정하는 정수 파라미터
- 기본 영역(Base Grid, 또는 Base Zone): t_0차의 동일한 다항식을 사용하는 지리적 영역(geographical area)에 존재하는 센서 노드의 집합
- 다항식 수위(Polynomial Order) O: 비밀키를 설정하는데 사용하는 다항식의 범위, $O \in \{1,2,\cdots,n\}$, 각각의 노드는 어떠한 n의 최소 수위와 최고 수위를 갖는다.
- 다항식 차수(Polynomial Degree) t_0: 다항식의 강도와 이 다항식을 공유하고 있는 각각의 노드들이 다항식을 복구하기 위하여 얼마나 많이 필요한지 나타내는 파라미터. 0부터 n까지 다항식의 수위를 표현한다.

이 논문의 나머지 부분에서 주로 사용하는 영어 약자는 표 1에 설명되어 있다.

표 1. 논문에서 사용하는 영어 약자에 대한 설명
Table 1. Notations.

영어 약자	설 명
n	네트워크 수위
N	WSN 내의 센서 노드의 수
m	기본 네트워크 영역에 있는 센서 노드의 수
k	네트워크를 통한 센서 노드 분배 단위
d	노드 수위
B_z	기본 영역(기본 그리드)
O_x	x번째 네트워크 그리드의 수위
t_0	기본 그리드에서 기본 다항식의 차수
t_n	수위가 n인 그리드에서 다항식의 차수
i,j	센서 노드
ID_i	센서 노드 i의 식별자
G_n	네트워크에서 기본 영역의 수

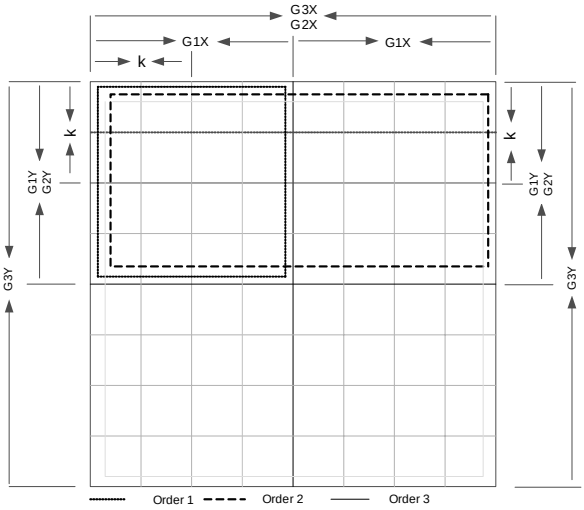

그림 1. 계층적 그리드 네트워크에서의 센서 노드의 분배

Fig. 1. Node deployment in Hierarchical grid structure.

2. HGB(Hierarchical Grid-Based) 기법 개요

제안하는 기법은 두 노드를 위한 비밀키를 생성하는 방법으로써 Blundo 기법을 사용한다. 키 요소 분배 방법은 그림 1처럼 계층적 그리드(Hierarchical Grid)를 사용한다. 여기서 이 계층적 그리드는 Ad hoc 네트워크에서 사용되는 견고한 라우팅 기법을 사용하고 있다고 가정한다. 그리드는 최대한 정사각형을 유지하며, 크기를 두 배씩 증가하며 수위를 증가시킨다. 만약 동일한 센서 노드에서 다른 다항식들을 사용하면 매우 많은 수의 노드가 공격자의 손에 떨어졌다고 하더라도 비밀키를 설정하고 다른 노드들과 통신할 수 있는 기회를 얻을 수 있다.

N개의 노드가 존재하는 네트워크는 그림 1처럼 노드들이 분포하고 네트워크가 n개의 계층 수위로 나누어진다고 가정한다. 각각의 l 수위의 계층은 2^{l-1}개의 기본 영역 B_z로 이루어져 있고, B_z는 $[2k, 2k]$의 크기를 갖는다. 따라서 하나의 B_z에 속하는 센서 노드의 수 m은 $(2k)^2$개가 된다.

가장 높은 수위의 O_n는 $G_n = 2^{n-1}$개의 B_z를 가지고 있으며, 모든 노드의 수 N은 $m \times G_n = (2k)^2 \times 2^{n-1}$와 같다. 그림 1에서 보이는 것처럼 B_z는 O_1를 갖는 [G1X, G1Y]의 크기를 갖는 어떠한 그리드이다. [G2X, G2Y]는 수위 2의 그리드(즉, O_2)가 될 것이며 [G3X, G3Y]는 O_3이 된다.

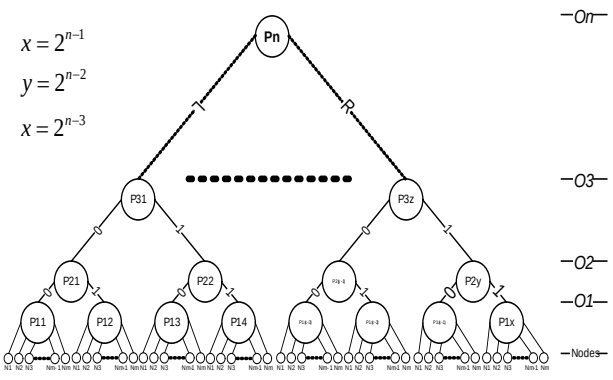

그림 2. WSN에서 노드의 위치로 생성하는 노드 ID

Fig. 2. Node ID allocation based on the location.

3. 노드 식별자

제안하는 기법에서는 네트워크에서 각각의 노드가 고유하게 식별하는 식별자 ID를 사용한다. ID를 생성하는 함수는 그리드 기반의 네트워크에 노드의 위치로 구현할 수 있다. 두 배씩 늘어나는 계층적 그리드의 사용은 그림 2처럼 이진트리의 리프 노드(Leaf Node)들이 다른 B_z의 m개의 노드라고 하고 트리의 높이가 네트워크의 수위라고 한다면 계층적 그리드를 서로 다른 B_z로 표현할 수 있게 한다. 식별자는 트리의 리프를 구별할 수 있는 번호와 리프에 속한 노드들에게 할당된 연속 번호로 구성된다. 리프를 구별할 수 있는 번호는 리프가 위치한 위치에 따라 왼쪽 가지를 거쳤으면 0을, 오른쪽 가지를 거쳤으면 1을 할당하여 최종적으로는 이를 모두 모은 값이 된다. 그리고 리프에 속한 노드들에게 할당된 연속 번호는 1부터 m까지의 수 중 어느 하나가 된다. 그림 3처럼 보이는 이 구조에서 이를 표시하기 위한 비트의 길이는

$$|ID| = n + \log_2 m \tag{3}$$

와 같다. 만약 네트워크의 크기 N이 충분히 크다면 n은 동적으로 확장하는 네트워크에 변하지 않는 값을 사용할 수 있을 것이다.

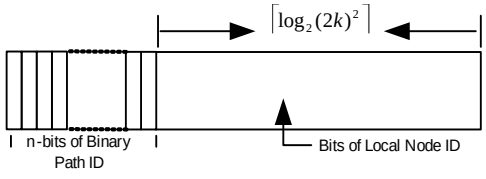

그림 3. 계층적 그리드 기반 기법에서의 센서 노드의 ID 구조

Fig. 3. ID structure in Hierarchical grid.

4. 키 요소(Key Material) 생성

그림 1처럼 WSN에서 HGB(Hierarchical Grid-Based) 분배 구조를 사용하는 것은 네트워크의 각 수위에서 하나 이상의 키 요소가 필요하게 된다. 기본적으로 B_z에 할당된 t_0차 대칭 이변 다항식은 같은 B_z에 속한 노드들이 비밀키를 만들기 위해서 사용된다. 이 다항식을 사용하면 두 노드 사이에서 $(2n-1)^{-1}$의 확률로 직접적으로 키를 설정할 수 있는 기회를 얻을 수 있다. 다른 다항식들은 보다 안전한 연결을 위하여 사용된다. 가장 많은 통신은 B_z에서 일어나게 되고 다른 부분들에서 발생하는 통신량은 확률적으로 매우 작은 값을 갖는다고 가정하면, 낮은 차수의 다항식을 작은 그리드 부분에 사용하고 높은 차수를 큰 수위를 위해서 사용할 수 있을 것이다. 알고리즘 1 다른 수위의 다항식을 생성하며 다항식을 계산하고 각각의 센서 노드에게 할당되는 과정을 보여준다.

5. 비밀 키 생성

두 노드 i와 j가 통신을 하기 위하여 키를 생성하려고 할 때, 각각의 노드는 자신의 ID를 알고 있고 키 설정 단계에서 교환한 다른 노드의 ID를 알 수 있다. 우선, 두 노드에서 공유하고 있는 다항식 중에서 적당한 다항식 $f^*(x,y)$가 선택된다. 선택된 다항식은 노드 i, j의 영역에서 최소한 t차 이상의 두 노드가 공유하고 있는 것이어야 한다. 비밀키를 만들기 위해서는 알고리즘 2를 실행한다. 이 알고리즘은 두 노드에서 동시에 실행된다.

알고리즘 1. 다항식 생성

```
Input: Network Order n, Path ID for node i (d), Node ID
Output: 2^(n-1) Polynomials sorted in P[n][2^(n-1)],
        n SBP for each node x in Px[n] evaluated in one  variable

Loop 1: for i=1 to n
    Loop2:  for j=1 to 2^(i-1)
        p[i][j]= SBP of degree t_0 and belonging to order i
        \\ Generated with coefficients belong to GF(q)
        next j
    end Loop2
    Loop 3: For x=1 to N
        Set Px[i]=P[i][d*(1/(2^(i-1)](ID,y)
        next x
    end Loop 3
    next i
end Loop1
```

6. 변수의 할당

제안하는 기법에서 다항식의 차수 t_0와 다른 다항식들의 차수와 t_0와의 관계는 동적으로 변화한다. B_z안의 노드의 수 m 또한 변수이다. B_z의 수 그 자체는 수위 n의 값에 따라 결정된다. [18]에서 저자는 t_0를 20으로 했지만, 이 가정은 WSN 크기의 변화와 함께 관련된 동적인 보안 강도를 제공하지 못한다. [9]에서와 같은 메모리 값을 사용하여 t_0는 $0.6\times m$으로 할당할 수 있고, 다른 $(n-1)$개의 다항식들의 차수 $t_1,t_2,\cdots,t_{n-1}$는 다음과 같은 접근 방법 중 하나를 따른다. 1) t_0의 값과 네트워크 수위의 크기 값을 할당하는 데에 다항식의 값과 동일한 값을 갖게 한다. 2) 다항식들이 서로 무관한 차수를 갖는다. 제안하는 기법에서는 다른 수위에 독립적인 값 t를 사용하였다.

Ⅳ. 기법 분석

1. 오버헤드 분석

이 절에서는 WSN의 자원이라는 측면에서 분석적이고 수학적인 방법을 이용하여 제안하는 기법에 대한 비용을 측정해본다. 노드 분배 단위 k, 네트워크 사이즈 N 그리고 네트워크 수위 n의 관계는 그림 4에 보이고 있다.

가. 메모리 오버헤드

각각의 노드는 ID를 표현하기 위해서 메모리 크기와 다른 n 다항식을 요구한다. $GF(q)$내의 계수를 갖는 어

알고리즘 2. 키 설정

```
Input: IDi, IDj, Px[n]: array of node's polynomials
Output: Kij = Kji.

set IDi1 = Path ID of IDi
set IDj1 = Path ID of IDj
Loop 1: for d = n to 1
    if (IDi1[d] == IDj1[d])
        Set d = d-1
        next d
        break
    else
        break
end Loop 1

use f*(x,y)=Px[d]
set Kij=f*(IDi,IDj)
```

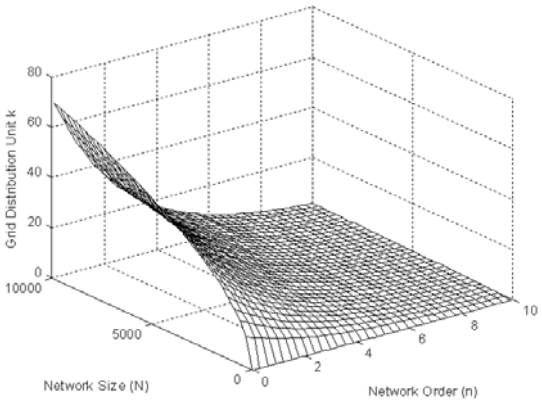

그림 4. 노드 분배 단위 k와 네트워크 사이즈 N, 네트워크 수위 n과의 상호 관계
Fig. 4. Relationship between k, N, and n.

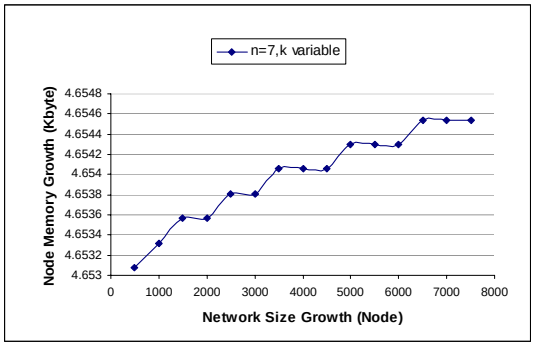

그림 5(A). 네트워크 증가와 메모리 증가
Fig. 5(A). Memory vs. Network size with variable k.

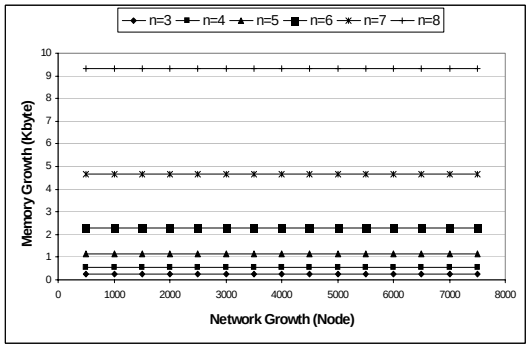

그림 5(B). 네트워크 증가와 메모리 증가
Fig. 5(B). Memory vs. Network size with different n.

떠한 차수 t_0의 SBP $f(x,y)$는 $f(t_0+1)\times\log(q)$의 비트로 표현할 수 있다. 메모리 사용에 대해서 제안한 방식은 두 가지 이점을 가진다. 첫 번째는 서로 독립적인 차수의 다항식을 생성하는 것과 초기 $t_0=0.6\times m$을 부여하는 계산에서 몇몇 무시되는 증분으로 동일한 t_0을 가질 수 있다는 것이다. 아래 수식에서 처음 두 항목은 ID를 표현하기 위한 것이고 마지막 항목은 n 다항식을 표현하기 위한 것이다.

$$Memory_1 = n + \left\lceil \log_2 \frac{N}{2^{n-1}} \right\rceil + n\left(\frac{0.6N}{2^{n-1}}+1\right)\log_2(q) \quad (4)$$

두 번째는 n의 증가를 구성하는 것이 t와 동일하다는 것이다. 그러므로 첫 번째 위수는 t_0차수를 가지고, 모든 i번째 위수는 $2^{i-1}\times t_0$를 가지게 될 것이다. 아래 수식에서의 마지막 항목은 다른 차수의 n 다항식을 표현하기 위해 요구되는 메모리의 합을 보여준다.

$$\begin{aligned} Memory_2 &= n + \left\lceil \log_2 \frac{N}{2^{n-1}} \right\rceil + P_{weight}\sum_{i=1}^{n}(2^{i-1})t_0 \\ &= n + \left\lceil \log_2 \frac{N}{2^{n-1}} \right\rceil + \\ &\left(\frac{0.6\times N}{2^{n-1}}\right)(2^n-1)\left(\frac{0.6N}{2^{n-1}}+1\right)\log(q) \end{aligned} \quad (5)$$

첫 번째 상황의 메모리 증가는 그림 5(A)에서 보이고 있으며, 그림 5(B)는 두 번째 상황을 보여주고 있다. P_{weight}는 t_0차수의 $f(x, ID)$를 표현하는데 필요한 비트수를 보이고 있다.

나. 연산 오버헤드

공유 비밀 키가 필요할 때마다 t차수의 다항식 $f(x,ID)$가 수행된다. 그러나 $f(x,ID)$의 차수 t는 O_x에 따라 다르다. 수식(4)의 경우, 필요한 계산은 하나의 $f(x,ID)$ 평가식이다. 수식(6)은 수식(5)에 다른 t를 할당함으로써 $GF(q)$의 많은 곱셈 계산이 필요하다는 것을 보여준다. cv는 다항식을 통하여 생성한 ID내의 두 문자열을 비교하기 위해 필요한 계산량이다. p_i는 두 노드가 다른 $(i-1)$번째 그리드에 놓이는 확률을 의미하며, C_{Pt_i}는 i번째 단계의 다항식을 위한 평가에 요구

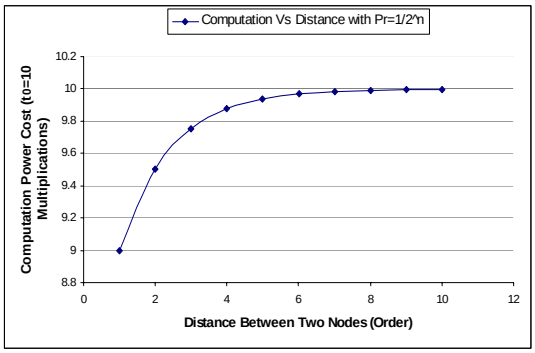

그림 6. $1/2^{n-1}$ 통신 감쇠 트래픽 요소와 O안의 노드사이 거리를 고려한 연산 오버헤드 증가
Fig. 6. Node distance vs. Computational power cost.

되는 연산량을 말한다.

$$CP_{avg} = \sum_{i=1}^{n}(p_i C_{Pt_i}) + cv \quad (6)$$

그림 6은 $GF(q)$의 곱셈으로 인한 성장 곡선을 보여주고 있다.

다. 통신 오버헤드

제안하는 기법을 사용하는 시스템은 통신을 위한 부가적인 일을 필요로 하지 않는다. 서로 다른 다항식들은 이미 선분배 과정에서 노드들에게 분배될 수 있다. 그러므로 추가적으로 필요한 통신 오버헤드는 키를 생성하기 위한 *ID* 교환에 필요하다. 이를 위해서는 크기 N의 네트워크를 표현하기 위한 공간 $\log_2 N$이 필요하다.

2. 보안 분석

가. 연결성

제안 방법은 다른 B_z에 대해서 하나 이상의 다항식을 사용함으로써 연결을 제공하는 계층적 구조를 이용한다. 그러므로 전체 네트워크에서 제공되는 연결성 c는 대략 1이다. B_z에 대한 다항식은 $(2^{n-1})^{-1}$의 연결성을 제공한다. 또한 i번째 수위 그리드에 대한 다항식은 $(2^{n-i})^{-1}$의 연결성을 제공한다. i는 1에서부터 $n-1$까지 증가하므로 연결성은 $c = (2^1)^{-1} + (2^2)^{-1} + \cdots + 2^{(n-1)^{-1}} \simeq 1$이다.

나. 차단된 통신량

Blundo[3] 방법을 적용할 경우 i번째 수위의 다항식 $(1 < i \le n)$이 사용하더라도 다른 네트워크에는 i번째 수위 그리드 내의 통신량보다 많은 통신량의 영향을 미치지 않는다. i번째 수위의 다항식이 노출되었다고 가정하게 되면, 차단된 통신량은 $(2^{n-i})^{-1} \times p_i$ (p_i는 다른 $(i-1)$번째 수위 그리드 안의 노드 사이의 통신량)가 된다. $p_i = (2^{i-1})^{-1}$ 분배를 사용하는 것은 차단된 통신이 항상 i값을 고려하지 않는 상수 값이 되는 것을 보장할 것이다.

다. 타협 영향과 복원력

다음과 같은 네트워크에 대한 공격 시나리오를 생각해보자.

- N_c 노드들에 대한 공격: t_0보다 작은 크기 N_c에 대한 노드들의 집합이 공격자의 손에 떨어진 상황에서, 선택적 공격[9]을 사용하면 동일 B_z에 모든 노드들이 속해있더라도 이로 인해 영향을 받은 노드들은 존재하지 않는다.
- B_z에 대한 공격: 공격자의 손에 떨어진 노드의 집합 $A(t_0 < |A| \le m)$이 있다고 가정한다. 만약 집합 A에 최소한 t_0+1개가 B_z에 속해있다면, 공격자는 B_z의 다항식을 손에 넣을 수 있다. 하지만 네트워크가 2^{n-1}개의 다항식을 포함하고 있고, 동일 다항식 공유가 속하게 되는 t_0노드에 대한 확률 p_r은 $1 - \sum_{i=0}^{t_0-1}\binom{N_c}{i}(\frac{m}{N})^i(\frac{N-m}{N})^{N_c-i}$이 되기 때문에 이로써는 통신을 방해할 수 없다.
- 전체 네트워크에 대한 공격: 전체 네트워크에 대한 공격은 동시에 수행할 수 없다. 하지만 최악의 경우 t_0의 $f(x,y)$ 모두를 하나씩 공격자가 손에 넣음으로써 전체 네트워크를 붕괴시킬 수 있는 가능성을 가지게 된다. B_z를 공격자가 손에 넣기 위해서는 t_0노드들을 공격해야만 한다. 네트워크는 다른 B_z에 대한 G_n으로 구성되었기 때문에 전체 네트워크 크기의 60% 이상 즉, $G_n \times t_0$개의 노드를 공격해야 한다. 이렇게 공격당한 노드들의 중요성을 제외하더라도, 공격당한 노드들은 센서 노드의 50% 미만을 유지해야 한다.
- 선택적 그리고 무작위 노드 공격: 노드들이 무작위로 배포되어졌다 하더라도 노드들의 배치 정보, 각 그룹에 대한 다항식의 할당 그리고 B_z에 기반 하는 다른 노드들의 구분 능력은 선택적 공격을 가능하게 한다. 그림 6은 WSN에서 이러한 공격의 영향을 보여주고 있다. 그리고 무작위 노드 공격은 'B_z에 대한 공격'과 같은 확률 모델을 따르며, $m_1, m_2, \ldots, N$에 대해서 $t_0, t_1, \ldots, t_{(n-1)}$의 간격으로 m에 대한 차이를 가지게 된다.
- Sybil 그리고 노드 응답 공격[14][15]: WSN의 동적인 확장에는 두 가지 문제점이 있다. 동일 노드 j에 대한 하나 이상의 *ID*를 사용함으로써 Sybil 공격이 문제가 된다. 이 방법의 경우 네트워크에는 수차례 동일 *ID*를 사용해서 노드 응답 공격이 수행되어진다. 제안한 방법은 네트워크에서 일정하고 유일한 *ID*구조를 사용하고 있기 때문에 이러한 위협에 대응할 수 있다. 공격자가 이러한 *ID*를 위조하더라도, 제안한 구조를

따라야 하고 동일 B_z에서 통신을 하기 위해서는 특정 영역에 배치되어져야 하므로 이는 어렵다.

- DoM 그리고 DoS 공격 : DoM[13]은 브로드캐스트 메시지를 수신하는 것을 박탈하는 능력을 가진 것을 말한다. 제안하고 있는 방법에서는 노드의 브로드캐스트 수용력을 요구하지 않는다. 만약 브로드캐스트가 사용되면 이것은 동일 그리드 내에서만 이용되어지기 때문에, 이 공격은 전체 네트워크의 일부에만 영향을 미치게 될 것이다. DoS[19]는 키 요소 혹은 공격자의 메시지 흘림(Message Flooding)과 같은 이유로 인한 과도한 통신 혹은 계산의 필요에 기인하여 발생할 수 있다. 그러나 첫 번째 상황에 대해서 우리가 제안한 방법은 계산과 통신이 많이 필요하지 않으며, 짧은 시간을 요구하기 때문에 공격자가 DoS 공격을 수행하는 것은 다소 힘들어 보인다. 두 번째 상황에서 DoS 공격을 수행하기 위해서 노드 응답 공격이 필요할 것이다.
- 공격으로부터의 회복 : $t+1$ 노드가 공격당했을 때, 공격자에게 비밀인 대체 다항식이 사용되어질 것이다. i번째 단계 그리드의 다항식이 노출된 상황에서, $i+1$번째 단계 그리드의 다항식은 시스템이 복구되어질 때까지 사용되며 그 동안 다항식이 노출된 그리드에 다른 다항식을 부여해야 한다. 최상위 단계의 다항식이 노출됐을 때, 공격자에게 노출된 트래픽 양은 단지 $0.5p_i(i=n)$이 될 것이다. (p_i)는 다른 $(i-1)$번째 단계 그리드에 속한 노드들 사이의 통신을 말한다.) 만약 그리드의 단계가 증가할 때마다 트래픽이 반씩 감소된다고 가정한다면 p_n은 $(2^{n-1})^{-1}$이 될 것이다.

Ⅴ. 타 연구와의 비교

이 장에서는 제안한 방법과 비교를 위해서 GBS[12], Multi-space[7], EG[8], Q-Composite와 RPS[5]를 선택하였다. 제안한 방식과 다른 방식에서의 보안을 평가하기 위해서 1680개의 노드를 가진 네트워크를 설정하여 GBS를 기반하여 보안을 비교하였다. 분석에 사용된 파라미터들은 $N=1680$개의 노드, $n=8$ 수위, $m=14$ 노드, $|ID|=12$비트*, $G_n=128B_z$이다. GBS와의 비교를 위해서 동일한 네트워크 크기와 $m=41$을 사용하였다. 또한 선택적 공격을 사용하여 노출된 노드들 사이에서 노출되지 않은 노드들의 영향을 일부 테스트하는 방식을 적용하였다. 그림 7(A)은 이들의 비교를 보여주고 있다. 그림 7(B)는 제안한 방식에 대하여 최악의 경우를 고려한 선택적 공격과 최상의 경우를 고려한 선택적 공격에 대한 측면을 보이고 있다. 제안한 방식

* 실크기 7%의 동적 확장을 제공($\lceil \log_2 m \rceil = 4 \mapsto m_u = 16$, 동적확장 $\frac{(m_u - m) \times G_n}{N} \times 100\%$)

표 2. HGB와 다른 방식들과의 비교
Table 2. Comparison of key establishment schemes.

	통신	계산	메모리
GBS[12]	상수	다항식 계산	$ID+2$ 다항식
EG[8]	$\mathcal{O}\log S_k$	$\frac{(2C+p-p_k)}{2}\log C$	S_k 키
RPS[5]	상수	c	S_k 키
Q-Composite[5]	$\mathcal{O}\log S_k$	$\mathcal{O}\log C$ 비교	S_k 키
Multi-Space[7]	$\mathcal{O}\log(n\times\tau)$	크기 λ의 두 벡터들의 곱	크기 λ벡터의 $\tau+1$
HGBS*	상수	다항식 계산	다항식

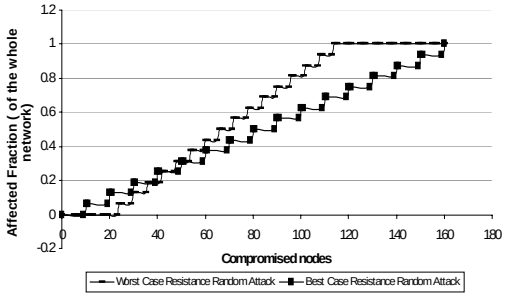

그림 7(A). HGBS에서 선택적 공격에 대한 최악의 경우와 최선의 경우
Fig. 7(A). Worst case and best case analysis for selective attack.

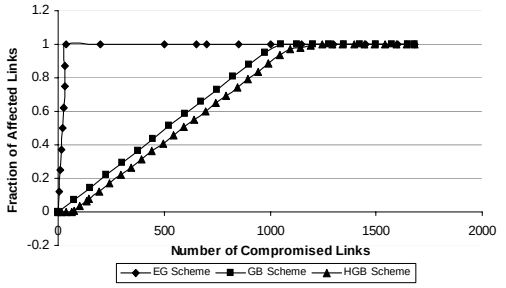

그림 7(B). EG[8] 그리고 GBS[12]에 대한 HGBS 선택적 공격 비교 (EG 방법 $d=40$에 대한 $N=1680$ 노드들, $t_0=0.6m$)
Fig. 7(B). Comparison of EG, GBS, HGBS for selective attack(d = 40 for EG, N = 1680, t0=0.6m).

과 GBS방식에서의 공격자에게 공격당한 노드의 증가에 따른 연결성은 동일하나 제안한 방식의 경우 $n \times t_0$ 만큼의 이동을 보이고 있다.

Ⅵ. 결론 및 향후 연구

이 논문에서 우리는 WSN에서 안전한 키 관리와 선분배를 위한 새로운 프레임워크를 제안하였다. 이 방법에서는 센서 노드들 사이에 계층적 그리드 방식으로 구성하고 있다. 여기에 노드를 구분하기 위한 *ID* 구조를 만들었으며, 위치와 사용된 키 요소를 나타낼 수 있게 하였다. 제안한 방식의 성능을 측정하기 위해서 Blundo[3] 기법을 사용하였으며, 연산능력, 통신 그리고 메모리에 대한 분석을 수행하였다. 또한 생각할 수 있는 여러 공격방법에 대해서 서술하고 그에 대한 비교분석을 통하여 성능을 보여주었다.

이후 제안한 방식에서 사용한 키 요소 할당에 대한 개선과 보안 분석 그리고 안전에 대한 수학적 모델의 유도과정을 수행할 계획이다. 그리고 제공한 프레임워크의 연결성, 통신량 그리고 보안 파라미터들을 고려한 키 설정 알고리즘을 제공할 것이다.

참 고 문 헌

[1] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless Sensor Networks: A Survey, Computer Networks (Elsevier) Journal, Vol. 38, No. 4, pp. 393-422, March 2002.

[2] Blom, R.: An optimal class of symmetric key generation systems, Advances in Cryptography, Proceedings EUROCRYPT 84, LNCS, Springer-Verlag, 209, pp. 335-338, 1985.

[3] Blundo, C., DE Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., and Yung, M.: Perfectly secure key distribution for dynamic conferences, In Advances in Cryptology - CRYPTO '92, LNCS 740, pp. 471-486, 1993.

[4] Camtepe, S. A. Yener, B.: Key Distribution Mechanisms for Wireless Sensor Networks: a Survey, Rensselaer Polytechnic Institute RPI, Technical Report TR-05-07, (March 23, 2005).

[5] Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks, IEEE Symposium on Security and Privacy, pp. 197-213, May 2003.

[6] Diffie, W., Hellman, M. E.: New directions in cryptography, IEEE Trans. Inform. Theory, IT-22, pp. 644-654, November 1976.

[7] Du, W., Deng, J., Han, Y. S., and Varshney, P.: A pairwise key pre-distribution scheme for wireless sensor networks, In Proceedings of 10th ACM Conf. on Computer and Communications Security (CCS'03), pp. 42-51, 2003.

[8] Eschenauer, L., Gligor, V. D.: A key management scheme for distributed sensor networks, In Proceeding of the 9^{th} ACM Conf. on Computer and Communications Security, pp. 41-47, 2002

[9] Huang, D. , Mehta, M., Mehdi, D, Harm, L.: Location-aware Key Management Scheme for Wireless Sensor Networks, Proc. of 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04), pp. 29-42, October 2004.

[10] Hwang, J. M., Kim, Y. D.: Revisiting random key pre-distribution schemes for wireless sensor networks, Workshop on Security of ad hoc and Sensor Networks archive, Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 43 - 52, 2004.

[11] Li, J., Janotti, J., DeCouto, D. S. J. , Karger, D. R., Morris, R.: A Scalable Location Service for Geographic Ad Hoc Routing, The Sixth Annual International Conf. on Mobile Computing and Networking, pp. 120-130, August 2000.

[12] Liu, D., Ning, P.: Establishing Pairwise keys in distributed sensor networks, In Proceedings of 10th ACM Conf. on Computer and Communications Security (CCS'03), pp. 52-61, 2003.

[13] McCune, J., Shi, E., Perrig, A., Reiter, M.: Detection of Denial-of-Message Attacks on Sensor Network Broadcasts, In Proceedings of the IEEE Symposium on Security and Privacy, May 2005.

[14] Newsome, J., Shi, E., Song D., Perrig A.: The Sybil Attack in Sensor Networks: Analysis and Defense., In Proceedings of Information Processing in Sensor Networks (IPSN), April 2004.

[15] Parno, B., Perrig, A., and Gligor V.: Distributed Detection of Node Replication Attacks in Sensor Networks, Proceedings of the 2005 IEEE Symposium on Security and Privacy, May 2005.

[16] Perrig, A., Szewczyk, R., Wen, V., Culler, D. E., Tygar, J. D.: SPINS: security protocols for sensor networks, MOBICOM, pp. 189-199, 2001.

[17] 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.

[18] Schmidt, JS. , Krahn, H., Fischer, S., Watjen, D.: A Security Architecture for Mobile Wireless Sensor Networks, Security in Ad-hoc and Sensor Networks, LNCS 3313, pp 166-177, Springer-Verlag Berlin Heidelberg 2005
[19] Wood, A.,Stankovic, J. A.: Denial of Service in Sensor Networks, IEEE Computer, 35(10): pp. 54-62, October 2002.

저 자 소 개

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

Mohaisen Abedelaziz
2005년 현재 인하대학교 정보통신대학원 석사 과정
<주관심분야 : WSN 보안, 네트워크 보안>