WSN에서 클러스터기반의 효율적인 pairwise key 설정 기법

이경효*, 오병균*, 이상국**
목포대학교 정보공학부 정보보호전공*
한국정보통신대학교 **
e-mail: {mediakh, obk}@mokpo.ac.kr*, sglee@icu.ac.kr**

The Cluster based Efficient pairwise key Establishment scheme in WSN

Kyeong hyo Lee*, Byeong-Kyun Oh*, Sang-Gug Lee**
Department of information Security, Mokpo National University
School of Engineering Information and Communications University

요 약

센서노드들이 배치되었을 때 초기 보안 요구사항은 이웃 노드 사이의 보안키를 안전하고 효율적으로 설정하는 것이다. 이를 위해 본 논문에서는 클러스터 단위로 직접키를 공유함으로써 공유하는 센서 수를 줄임과 동시에 다항식이 노출 되어도 전체 센서 네트워크에 끼치는 영향을 최소화하여 안전성을 보장하게하고 컴퓨팅 오버헤드를 줄일 수 있게 하였다. 또한 가용성 보장을 위해 불필요한 키관리 동작을 지양하고 센서 노드의 에너지 소모를 감소시키기 위하여 근접 클러스터 헤더 노드와의 사전 키 분배를 통해 경로키를 설정하게 함으로써 센서노드간의 안전하고 효율적인 pairwise key 설정을 통해 안전한 통신이 가능하게 하였다.

1. 서론

WSN(Wireless Sensor Networks)은 네트워크를 구성하는 센서의 수가 매우 많고, 각 센서노드들은 제한된 전력과 컴퓨팅 능력을 가지며, 빈번한 센서노드들의 삽입과 제거에 의해 센서 네트워크의 토폴로지가 쉽게 변화될 수 있다는 특성을 갖는다. 이러한 센서 노드의 제약으로 다양한 보안 스킴을 적용하기 힘들고 노드가 배치된 물리적 환경으로 전체 정보의 무결성을 쉽게 무너뜨린다. 또한 가장된 노드의 침입으로 중간 노드의 자원을 소모시켜 네트워크의 수명을 단축시킨다. WSN 보안 관점에서는 이러한 특성들을 반영하여 소형 경량이면서 무선 센서 노드의 보안을 동시에 해결할 수 있는 연구가 진행되어지고 있다.

WSN에 대한 연구 중, 시스템 보안성, 안전성 및 신뢰성은 키에 전적으로 의존하므로 여러 정보보호 메커니즘들을 적용하는데 있어서 키 관리는 중요하다. 또한 네트워크 레벨의 중앙 집중적인 키 관리는 센서노드 하나에 대한 취약성 공격이 전체 네트워크의 위협으로 가용성보장이 어렵다.

따라서 본 논문에서는 센서 배치 후에 센서 노드간의 안전한 통신을 위한 키 관리 문제를 다루고자 한다. 클러스터 기반 이변수 다항식을 이용한 키 분배 기법을 제안하여 위장노드의 공격에 안전하게 하였고 센서 노드간의 pairwise key 설정에 있어 기존의 평면의 클러스터링에 비해 효율성을 높일 수 있었다. 먼저 세부적으로 네트워크 클러스터링으로 센서 노드 노출로 인한 네트워크 전체에 주는 피해를 줄이고 클러스터 헤더를 둠으로써 사전분배 시 셋업서버의 오버헤드를 줄이고 경로키 설정에 있어서 센서 노드의 에너지 소모를 줄일 수 있게 하였다. 또한 클러스터링을 입체형으로 함으로써 하나의 클러스터내의 노드 수를 증가하여 배치하여 기존의 평면의 클러스터링에 비해 전체 경로키수를 줄일 수 있어 센서노드의 불필요한 키 관리 동작을 지양하여 에너지 소비를 최소화하였다.

본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음. [2005-S-106-02, RFID/USN용 센서태그 및 센서노드기술]

2. 다항식 기반의 pairwise key 설정 기법

2.1 다항식 기반 키 분배 기법

Liu, P. Ning은 Blundo가 제안한 다항식 기반 키분배 기법은 센서노드 간 pairwise key를 설정하는 방식에 있어서 실제 키 값을 센서노드들에게 할당하는 것이 아니라 키를 유도할 수 있는 다항식을 이용한 키 분배 방식을 제안하였다[1]. 임의의 두 센서노드가 동일한 t차 이변수 다항식(bivariate polynomial)을 공유하면 두 노드는 그 다항식으로부터 서로 공통되는 키 값을 유도할 수 있다. 다항식 기반 키 사전 분배 방식의 기본 개념은 키 셋업서버가 소수 q에 대한 유한체 Fq상에서 $f(x,y)=f(y,x)$의 성질을 만족하는 임의의 t차 이변수 다항식을 아래와 같이 생성한다.

$$f(x,y)=\sum_{i,j=0}^{t} a_{ij}x^i y^j \quad \text{.....(식 2.1)}$$

2.2 유한체 위의 다항식

체 F_q의 원소와 변수 x로 이루어진 한 원소 $f(x)$인 식을 체 F_q위의 다항식이라 하면 $a_0, a_1, ..., a_n$을 다항식의 계수(coefficient)라고 부른다.

$$f(x)=a_o+a_1x+...+a_nx^n \quad \text{.....(식 2.2)}$$

$a_n \neq 0$일 때 n을 $f(x)$의 차수(degree)라 하고 $f(x)$를 n차의 다항식이라고 부른다.

$$f(x)=a_0+a_1x+...+a_mx^m,$$
$$g(x)=b_0+b_1x+...+b_nx^n \quad \text{.....(식 2.3)}$$

여기서 $f(x)$와 $g(x)$의 차수가 m,n이면 $f(x)g(x)$의 차수는 $m+n$이다. 체 F_q에 대하여 $F_q[x,y]$를 체 F_q에서 계수를 갖는 x와 y에 관한 다항식의 모임이라 정의하자.

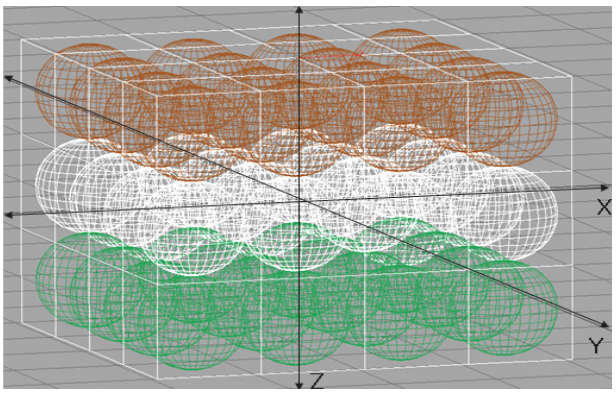
$$F_q[x,y]=\{\sum_{\substack{0\le i\le m\\ 0\le j\le n}} a_{ij}x^i y^j \mid a_{ij}\in F\} \quad \text{.....(식 2.4)}$$

$F_q[x,y]$의 원소 $f(x,y)=\{\sum_{\substack{0\le i\le m\\ 0\le j\le n}} a_{ij}x^i y^j\}$ ..(식 2.5)

3. 클러스터 기반의 센서 네트워크

3.1 클러스터 영역 분할과 노드 배치

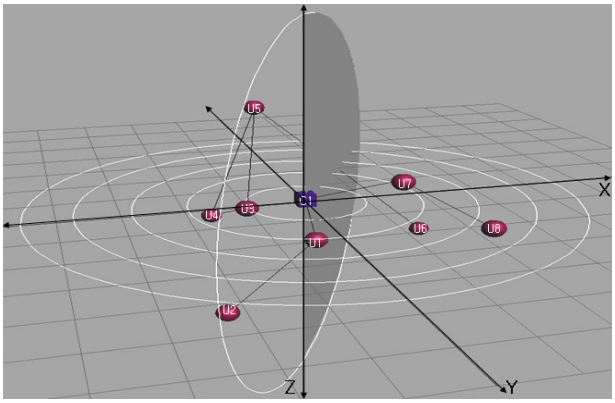
센서네트워크의 영역을 클러스터 단위로 키 분배를 하기 위하여 [그림 1]과 같이 전체 센서 네트워크의 영역을 구의 형태로 클러스터링 한다.



[그림 1] 클러스터 영역분할

입체형으로 클러스터링 함으로써 기존의 평면에서의 클러스터링에 비해 하나의 클러스터내의 노드를 많이 배치함으로써 센서 노드간의 pairwise key 설정 시 인접 클러스터에 위치한 노드간의 경로키 수를 감소시킬 수 있다.

센서네트의 구성 요소로는 다항식을 생성하여 분배하는 셋업 서버와 클러스터 헤더, 클러스터에 존재하는 센서 노드들로 구성한다. 베이스 스테이션은 게이트웨이 역할을 하고, 클러스터 헤더는 클러스터의 정중앙에 위치하고 클러스터 당 하나씩 존재한다. [그림 2]에서와 같이 클러스터 내에서는 구형태의 센서 노드들의 위치를 3차원 분포로 모델링한다. 즉 (x,y,z)는 센서의 좌표이며 배치중심 노드인 클러스터 헤더의 좌표는 (x_i,y_i,z_k)이다.



[그림 2] 클러스터 내 센서 노드 배치

3.2 사전키 분배 방법

센서네트워크의 영역이 $S=n^*n^*n$ 클러스터로 나누어지므로 셋업서버는 임의의 S개의 다항식을 생성한다. 셋업서버는 유한체 F_q상에서 다음 식을 만족하는 t차 이변수다항식 $f(x,y)$과 난수 r을 랜덤하게 선택하여 아래와 같이 생성한 후 클러스터 헤더 C_i에게 분배한다.

$$rf_{ci}(x,y)=r\sum_{i,j,k}^{t} a_{ij,k}x^i y^j z^k = A \quad \text{.....(식 3.1)}$$

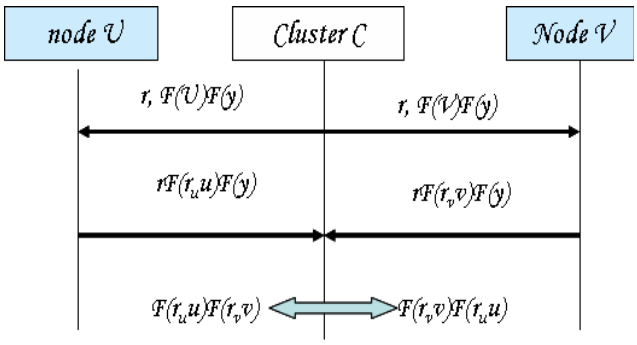
클러스터 영역에 센서들이 배치되면 셋업 서버에서 분배받은 이변수 다항식의 부분 정보와 유한체 Fq상에서 생성한 난수 r을 포함한 (식 3.1)의 A를 생성하여 분배한다. 또한 클러스터헤더는 $f_{ci}(1,y)=F(y)$인 A를 노드 U에게 전송하고 r, $f(x,y)$를 삭제한다.

3.2 동일 클러스터 노드 사이의 pairwise key 설정

클러스터헤더는 노드U와 노드 V에게 $F(r_u u)F(y)$ 대신에 (식 3.1)과 같은 유한체에서 생성한 난수를 포함한 값을 보내면 두 노드는 서로의 아이디 $r_u u$와 $r_v v$를 교환하여 (식 3.2)와 같이 pairwise key를 설정한다.

$$G^u(y)=rF(r_u u)F(y)$$
$$G^v(y)=rF(r_v v)F(y) \quad \text{.....(식 3.2)}$$

$$G^u(r_v v) = rF(r_u u)F(r_v v)$$
$$= rF(r_v v)F(r_u u) = G^V(r_u u) \quad \text{.....(식 3.3)}$$

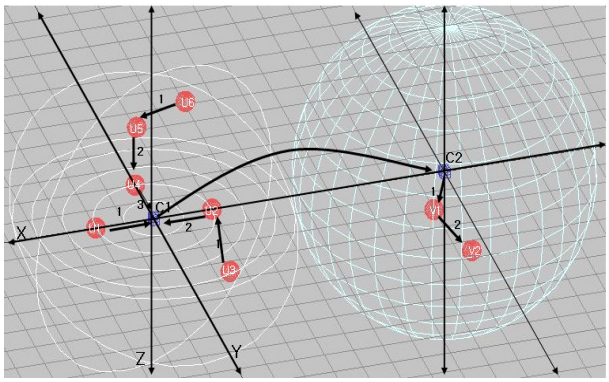


[그림 3] 동일 셀 내의 직접키 설정

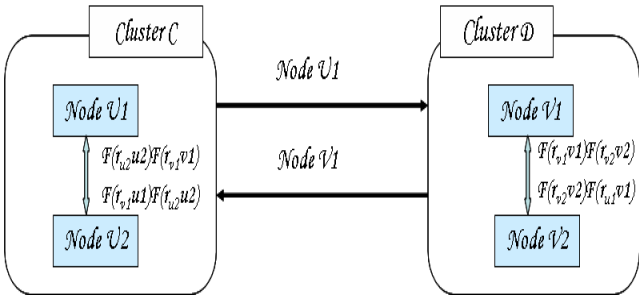
3.3 인접 클러스터의 경로키 설정

통신하고자 하는 센서들이 서로 물리적 전송 범위에 있으나 논리적인 전송영역이 다른 경우 두 센서가 소유하는 다항식이 다르기 때문에 [그림 4]와 같은 과정으로 경로키를 생성할 수 있다. 즉 노드들은 자신이 속한 클러스터 내에서 중간 노드들을 경유하여 클러스터 헤더를 통해 다른 클러스터 영역의 노드들과 통신을 할 수 있다. 좌표 (i,j,k)와 $(i,j+1,k)$에 위치한 센서노드사이의 pairwise key 생성은 아래와 같이 경로키를 생성한다.

$$G^D_{ij+1k}(r_d d) = r_{ij+1k}F_{ij+1k}(r_c c)F_{ij+1k}(r_d d)$$
$$= r_{ij+1k}F_{ij+1k}(r_d d)F_{ij+1k}(r_c c) = G^D_{ij+1k}(r_c c)$$
$$G^U_{ijk}(r_c c) = r_{ijk}F_{ijk}(r_u u)F_{ijk}(r_u u)$$
$$= r_{ijk}F_{ijk}(r_c c)F_{ijk}(r_u u) = G^C_{ijk}(r_u u) \quad \text{.....(식3.4)}$$
$$G^D_{ij+1k}(r_d d) = r_{ij+1k}F_{ij+1k}(r_c c)F_{ij+1k}(r_d d)$$
$$= r_{ij+1k}F_{ij+1k}(r_d d)F_{ij+1k}(r_c c) = G^D_{ij+1k}(r_c c)$$



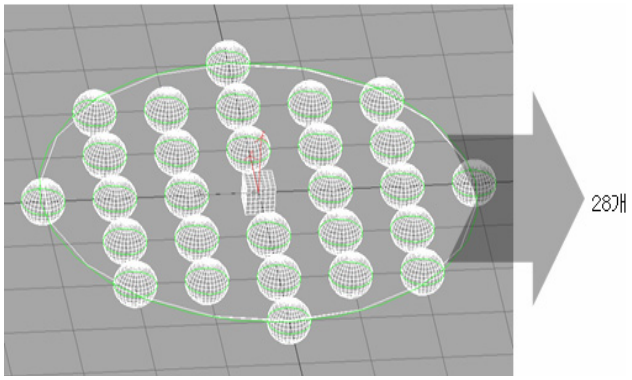
[그림 4] 인접클러스터 간의 경로키 설정



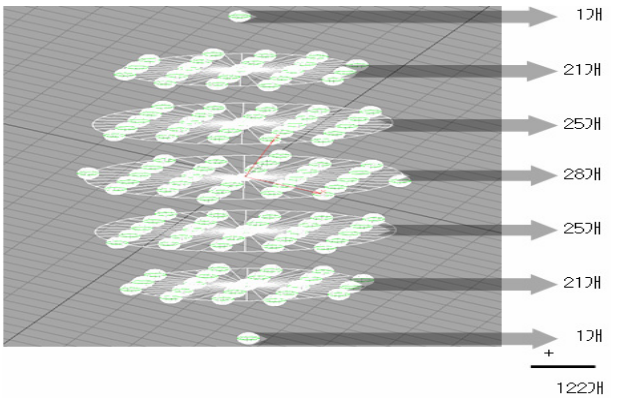
[그림 5] 인접 셀에 위치한 노드들의 경로키 설정

4. 노드 배치에 따른 효율성

제안한 논문에서는 클러스터링을 입체형으로 함으로써 평면배치에서보다 하나의 클러스터내의 노드 수를 더 많이 배치하여 기존의 평면의 클러스터링에 비해 전체 경로키수를 줄일 수 있어 센서노드의 불필요한 키 관리 동작을 지양하여 에너지 소비를 최소화하였다. [그림6]와 [그림 7]에서 평면배치에서의 센서 노드 수와 입체형으로 배치한 센서 노드 수의 차이를 나타내었다.

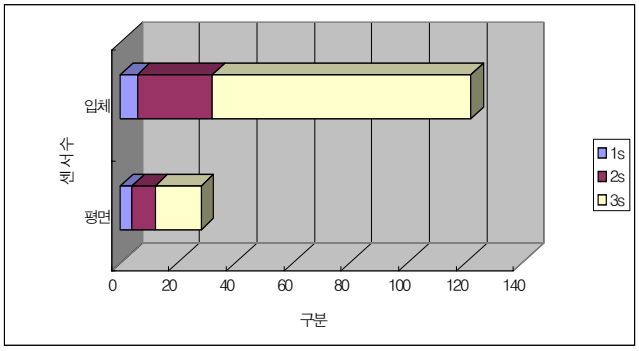


[그림 6] 평면 배치에서의 센서 노드의 수

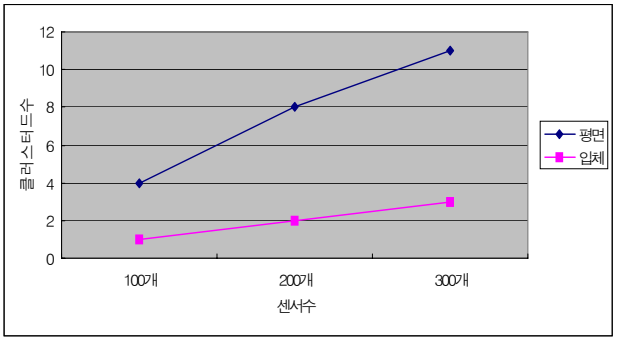


[그림 7] 입체형 배치에서의 센서 노드의 수

센서네트워크 영역을 입체형으로 클러스터링 함으로써 평면의 클러스터의 영역분할에 비해 경로키의 변화로 인한 경로 시간이 줄어들었음 [그림 7]을 통해 나타내었다.

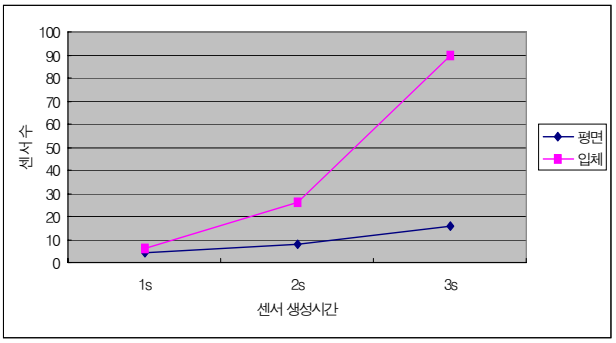


[그림 8] 경로시간에 따른 센서의수



[그림 9] 센서수에 적합한 클러스터의 수

[그림 8]에서는 클러스터 전송 반경 30m일 때 경로시간에 따른 센서 수 분포를 나타낸 것으로 생성시간이 길어짐에 따라 입체형으로 클러스터링할 때 센서의 수가 증가할 수 있음을 알 수 있다.



[그림 10 클러스터 전송 반경에 따른 센서 수 분포

[그림 10]에서는 클러스터 영역을 구형으로 분할함으로써 전송 반경에 다른 센서의 분포수를 늘림으로써 센서 노드의 불필요한에너지 소모를 줄일 수 있게 하여 가용성을 보장하게 할 수 있다.

5. 결론

제안한 메커니즘은 다항식이 노출되어도 이 다항식을 사용하여 노출되는 센서 수가 특정 클러스터 영역 내로 한정되므로 전체 센서네트워크에 미치는 피해를 줄일 수 있다. 통신하고자 하는 센서들이 서로 이웃해 있으나 다른 클러스터에 존재할 경우 경로키를 생성하여 각각의 클러스터 헤더를 통해 통신 하고자 하는 상대방 센서에게 전달함으로써 상호간 안전한 통신이 가능하도록 하였다. 또한 클러스터 영역을 입체형으로 함으로써 클러스터내의 센서의 수를 늘릴 수 있게 하므로 센서노드의 불필요한 에너지 소모를 줄일 수 있게 하였다. 클러스터 내의 센서 노드의 수가 증가로 경로키 수를 줄여 효율성을 높였다. 또한 다항식 분배 시 난수를 사용함으로 키를 유도한 다항식이 공개되지 않기 때문에 노드 노출로 인한 위험에도 안전하게 하였다. 뿐만 아니라 클러스터헤더에게만 키를 사전에 분배하면 되므로 부가적인 작업을 줄일 수 있어 센서네트워크의 오버헤드를 줄일 수 있다.

6. 참고 문헌

[1] D. Liu, P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks", *Proc. of the 10th AC conference on Computer and communications Security*, pp. 52-61. 2003.

[2] K. H Lee, S. W Jung, B. K Oh, S. G Lee, "A pairwise key establishment scheme for USN using polynomial shares derived from bivariate polynomials", The 6th Asia Pacific International Symposium on Information Technology, 2007.

[3] K. H Lee, S. W Jung, B. K Oh, S. G Lee, "New cluster-based key distribution for USNs and its security analysis", The 4th International Conference on Advances in Mobile Computing and Multimedia MOMM06, 2006.

[4] D. Liu, P. Ning, "Location-based Pairwise Key Establishments for Static Sensor", *SASN'03 First Workshop on of Ad Hoc and Sensor*,2003.

[5] Farooq Anjum, Location Dependent Key Management Using Random Key predistribution In Sensor Networks,5th ACM WiSe'06.

[6] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks", IEEE Symposium on Security and Privacy, pp.197-213,2003.

[7] T. Dimitriou, I. Krontiris, and F. Nikakis, Key Establishment in Sensor Networks with resiliency against node Capture and replication , December2003, Submitted to 5th ACM Symposium on Mobile Ad Hoc Networking and Computing, (Mobihoc) 2004.