WSN에서 클러스터기반의 효율적인 pairwise key 설정 기법

이경효*, 조아앵, 오병균, 이상국**
*목포대학교 정보보호전공, **한국정보통신대학교
*{mediakh, agcho, obk}@mokpo.ac.kr, **sglee@icu.ac.kr

The Cluster based Efficient pairwise key Establishment scheme in WSN

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

요 약

WSN는 초기에 센서 노드들이 배치되었을 때 이웃 센서 노드들 간 보안키를 안전하고 효율적으로 설정해야하고 에너지 소비를 최소화해야하며 네트워크의 생존성을 늘리기 위해 불필요한 키 관리 동작을 지양해야한다. 네트워크 레벨의 중앙 집중적인 키 관리는 센서노드 하나에 대한 취약성 공격이 전체 네트워크의 위협으로 가용성보장이 어렵다. 따라서 본 논문에서는 네트워크를 클러스터링 하여 센서노드 노출로 인한 네트워크 전체에 주는 피해를 줄이고자 구의 형태로 클러스터링 함으로써 동일 클러스터내의 노드수의 증가에도 경로키 수를 줄일 수 있게 하여 센서 노드의 에너지 소모를 감소시켜 가용성을 보장하였다.

1. 서 론

WSN(Wireless Sensor Networks)은 센서를 통한 정보 감지 및 감지된 정보를 베이스스테이션으로 전송하는 구조를 갖는다. WSN은 네트워크가 갖는 근본적인 특성으로 인해 일반 네트워크보다 보안에 취약하다. 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 다양한 센서 네트워크 보안에 관련된 암호, 인증, 키 관리, 안전한 라우팅 프로토콜, DoS 공격에 대한 대응 기술 등을 중심으로 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. 세부적으로 네트워크를 효율적으로 클러스터링하여 센서 노드 노출로 인한 네트워크 전체에 주는 피해를 줄였다. 또한 배치된 센서 네트워크에 베이스스테이션의 오버헤드를 줄이고 pairwise key 설정에서 키 노출에도 안전하게 하였으며, 보안 위협성을 줄여 키관리의 가용성을 보장하고 네트워크의 생존성을 늘리기 위해 불필요한 키 관리 동작을 지양하여 에너지 소비를 최소화하였다.

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

2. 관련연구

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.

$$f(x,y)=\sum_{i,j=0}^{t} a_{ij}x^i y^j \quad \text{.....(식 2.2)}$$

2.2 유한체 위의 다항식

체는 덧셈과 곱셈이 가능한 공집합이 아닌 공집합 F로 구성된 수학적 시스템이며, $\alpha,\beta,\gamma \in F$에 대하여 유일하게 결정된 F의 $\alpha+\beta$ 와 $\alpha\beta(\alpha\cdot\beta)$원소 $\alpha,\beta \in F$ 원소 각 쌍에게 할당된다. 여기에서 $\alpha+\beta \in F$이고 $\alpha\beta \in F$이다. 체 F_q의 원소와 변수 x로 이루어진 한 원소 $f(x)$인 식을 체 F_q위의(x에 관한) 다항식이라 하면 $a_0, a_1, ..., a_n$을 이 다항식의 계수(coefficient)라고 부른다.

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

여기에서 $a_0, a_1, ..., a_n \in F$이다. $a_1=...=a_n=0$ 일 때 다항식 $f(x)=a_0$를 상수 다항식이라 하고, 또 $a_0=a_1=...=a_n=0$ 일 때 $f(x)$를 영 다항식 이라고 한다. $a_n \neq 0$일 때 n을 $f(x)$의 차수(degree)라 하고 $f(x)$를 n차의 다항식이라고 부른다. 특히 0차의 다항식에서 영 다항식의 차수는 $-\infty$로 정의한다.

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

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 한 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)

이 때 0이 아닌 계수 a_{ij}를 갖는 항 중에서 $i+j$의 최대값을 다항식 $f(x,y)$의 차수라 한다.

2.3 WSN 보안 요구사항

WSN환경은 무선 통신을 기본으로 장치들 간에 통신이 이루어지므로 장치의 분실, Rouge 엑세스 포인트, IP 스푸핑, DoS, 웜 바이러스, 배터리 소진공격, 위치정보 노출 등 보안 위협사항이 발생한다. 따라서 이러한 보안 위협사항들에 대처하기위해 고려되어야 하는 보안 요구사항은 다음과 같다.

1) 기밀성(Confidentiality)

센서 네트워크의 암호키는 센서 노드 하나에 대한 암호키 공격의 영향이 전체 네트워크로 확산되지 않게 세밀한 키 제어(Fine key granularity)의 특성을 가져야 한다.

2) 인증(Authentication)/ 무결성(Integrity)

통신하고 있는 상대편 송신자가 정당한 송신자인지와 주고받는 데이터의 내용이 공격자의 불법적인 위/변조 과정 없이 원래의 메시지임을 확인할 수 있는 방법을 제공한다.

3) 적시성(Freshnes)

메시지가 현재 세션의 최신 내용이며 순서가 있어 이전에 전송되었던 메시지와 중복되지 않음을 메시지 순서(Ordering)기능과 추측되는 지연시간의 표시를 통해 제공된다. 또한 센서 네트워크는 클러스터 단위로 멤버구성이 가변적으로 이루어지므로 공유되는 암호키에 대한 적시성이 중요하다.

4) 확장성(Scalability)

센서네트워크는 리소스의 제한이나 전송지연 등으로 확장성이 떨어지는 키관리 스킴을 적용하기가 어렵다. 즉 그룹구성원이 커질수록 암호화 횟수, 키길이 등에 따라 리소스 사용이 증가하지 않아 적시성을 보장하고 전송지연이 발생하지 않은 효율적인 키관리 방안이 필요하다.

5) 가용성(Availability)

센서네트워크에서는 네트워크 레벨의 중앙 집중적인 키관리는 센서 노드 하나에 대한 취약성 공격이 전체 네트워크의 위협으로 쉽게 확산 될 수가 있어 선호하기 어렵다. 가용성을 위해 센서노드의 리소스를 보호하고 센싱정보의 이용을 제한하고 정보보호 서비스는 단일 장애 포인트를 발생시키지 말아야 한다.

6) 자가 조직(Self-Oranization)

센서 네트워크는 동적으로 자신의 라우팅 토폴로지나

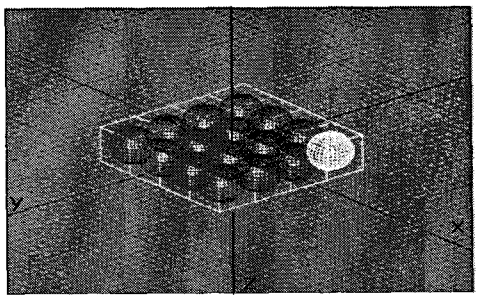
키관리 서비스를 재구성 할 수 있어야한다. 센서네트워크의 구축이전에는 네트워크의 영향범위 인접 네트워크 수나 거리정보, 특정 센서노드의 위치를 알 수 없으므로 네트워크 구축중이나 운영되는 동안 연결이 안 되는 센서노드들을 다룰 수 있어야 한다.

이러한 보안 요구사항들을 만족하기 위하여 본 논문에서는 네트워크를 클러스터링하여 가용성을 보장하고 클러스터 영역분할에 있어서 기존의 평면적인 구조에 비해 클러스터 내 센서노드들의 수를 늘려 경로키 수를 줄임으로써 센서노드의 에너지 소모를 줄일 수 있게 하였다.

3. 클러스터 기반의 센서 네트워크

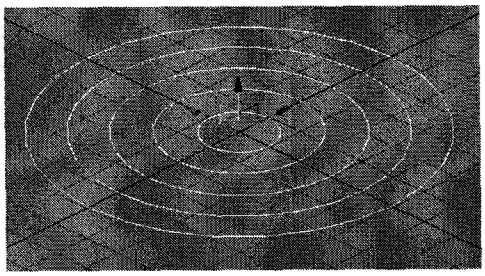
3.1 클러스터 영역 분할과 노드 배치

클러스터 단위의 키 분배를 위해 [그림 1]과 같이 전체 센서 네트워크의 영역을 구의 형태로 클러스터링 한다.



[그림 1] 클러스터 영역분할

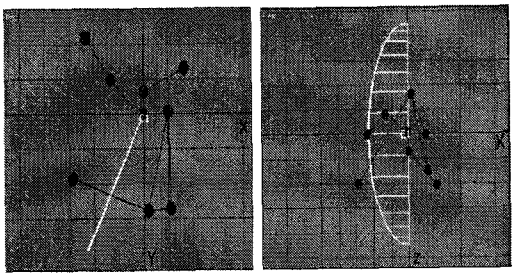
센서 네트워크 영역은 노드 배치 전에 클러스터링 되고 클러스터 내에서는 구형태의 센서 노드들의 위치를 3차원 분포로 모델링한다. 즉 (x,y,z)는 [그림 2]에서와 같이 센서의 좌표이며 배치중심은 (x_i,y_i,z_k)이다.



[그림 2] 센서의 배치중심 좌표

센서네트의 구성 요소로는 다항식을 생성하여 분배하는 셋업 서버와 클러스터 헤더, 클러스터에 존재하는 센서노드들로 구성한다. 베이스 스테이션은 게이트웨이 역할을 하고, 클러스터 헤더는 클러스터의 정중앙에 위치하고 클러스터 당 하나씩 존재한다.

[그림 4]는 동일 클러스터 내 클러스터 헤더를 중심으로 한 센서들의 배치를 나타낸 것으로 위에서와 좌측에서 본 모양은 [그림 3]과 같다.



[그림 3] 클러스터 내 센서들의 배치

[그림 4] 클러스터 내 센서들의 배치

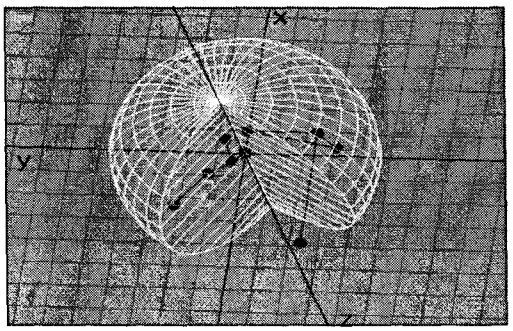
3.2 사전키 분배 방법

센서네트워크의 영역을 $S=n^*n^*n$ 클러스터로 구획을 나누어 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.

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

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

3.2 동일 클러스터 노드 사이의 pairwise key 설정



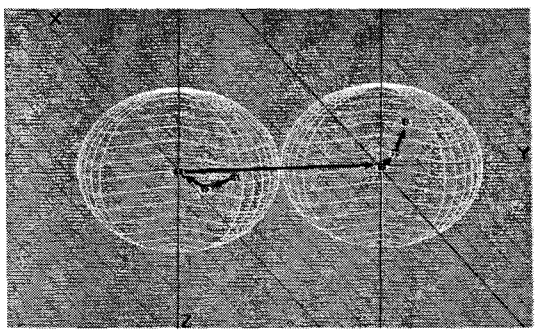
[그림 5] 동일클러스터 pairwise key 설정

클러스터헤더는 $F(r_u u)F(y)$대신에 노드U에게 유한체에서 생성한 난수를 포함한 값 A를 보내고 이를 아래와 같은 값으로 pairwise key를 설정한다.

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

3.3 인접 클러스터의 경로키 설정

통신하고자 하는 센서들이 서로 물리적 전송 범위에 있으나 논리적인 전송영역이 다른 경우 [그림 6]과같이 경로키를 생성한다.



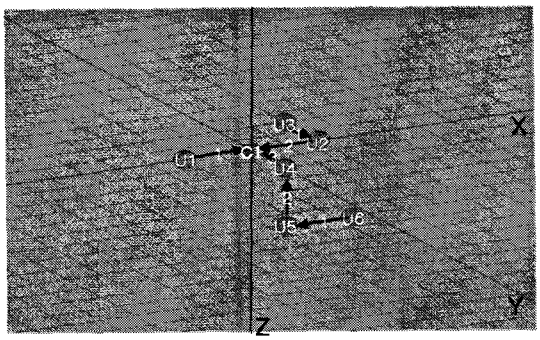
[그림 6] 인접클러스터 경로키 설정

좌표 (i,j,k)와 $(i,j+1,k)$에 위치한 센서노드사이의 pairwise key 생성은 두 좌표에 생성한 다항식을 이용하여 아래와 같이 경로키를 생성한다.

$$G^U_{ijk}(r_c c) = r_{ijk}F_{ijk}(r_u u)F_{ijk}(r_u u)$$
$$= r_{ijk}F_{ijk}(r_c c)F_{ijk}(r_u u) = G^C_{ijk}(r_u u)$$

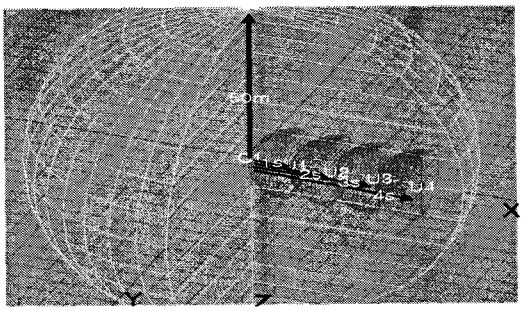
$$G^D_{ij-1k}(r_d d) = r_{ij+1k}F_{ij+1k}(r_c c)F_{ij-1k}(r_d d)$$
$$= r_{ij-1k}F_{ij+1k}(r_d d)F_{ij+1k}(r_c c) = G^D_{ij+1k}(r_c c)$$
$$G^D_{ij-1k}(r_d d) = r_{ij+1k}F_{ij+1k}(r_c c)F_{ij-1k}(r_d d)$$
$$= r_{ij-1k}F_{ij+1k}(r_d d)F_{ij+1k}(r_c c) = G^D_{ij+1k}(r_c c)$$

.....(식 3.3)



[그림 7] 위치에 따른 경로키 설정 과정

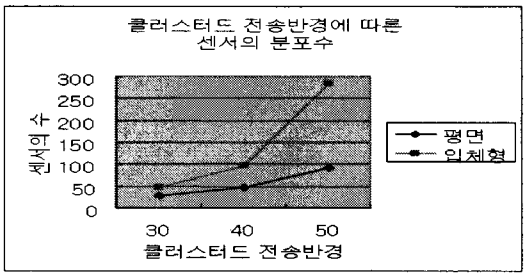
[그림 7]에서와 같이 통신하고자하는 센서들이 클러스터 역이 다르면 두 센서가 소유하는 다항식이 다르기 때문에 경로키를 설정하여 pairwise key로 사용한다. 즉 노드들은 자신이 속한 클러스터 내에서 중간 노드들을 경유하여 클러스터 헤더를 통해 다른 클러스터 영역의 노드들과 통신을 할 수 있다.



[그림 8] 위치에 따른 경로 시간의 변화

[그림 8]에서와 같이 평면의 클러스터의 영역분할에 비해 경로키의 변화로 인한 경로 시간이 줄어들었음을 알 수 있다.

[그림 9]에서는 클러스터 영역을 구형으로 분할함으로써 전송 반경에 다른 센서의 분포수를 늘림으로써 센서 노드의 불필요한에너지 소모를 줄일 수 있게 하여 가용성을 보장하게 할 수 있다.



[그림 9] 클러스터 전송반경에 따른 센서의 분포수

5. 결론

제안한 메커니즘은 다항식이 노출되어도 이 다항식을 사용하여 노출되는 센서 수가 특정 클러스터 영역 내로 한정되므로 기존의 방법보다 좀 더 안전함을 알 수 있었다. 통신하고자 하는 센서들이 서로 이웃해 있으나 다른 클러스터에 존재할 경우 경로키를 각각의 클러스터 헤더를 통해 통신 하고자 하는 상대방 센서에게 전달함으로써 상호간 안전한 통신이 가능하도록 하였다. 또한 클러스터 영역을 구형으로 함으로써 클러스터내의 센서의 수를 늘릴 수 있게 하였고, 인접 클러스터에 위치한 센서노드와는 클러스터헤더를 통한 경로키를 생성함으로써 센서노드의 불필요한 에너지 소모를 줄일 수 있게 하였다. 클러스터 내의 센서노드의 수가 증가하므로 인접클러스터에 위치한 노드들과의 통신 시에 경로키 수를 줄일 수 있게 하였다. 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.

5. 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", *SA SN'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, (Mobohoc) 2004.

[8] L. Eschenauer and V. D. Gilgor, A Key-Management Scheme for Distributed Sensor Proc. of the 9th ACM conference on Computer and communications security, pp.41-47,2002.

[9] D.Liu and P,Ning, Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks, In Proc. of the 10th Annual Network and Distributed System Security Symposium, pp.263-276,2003.