WSN에서 3차원 노드 배치에 따른 효율적인 키관리

이경효*, 오병균*

*목포대학교 정보공학부 정보보호전공

The Efficiency Key management for three dimensional node deployment in WSN

*Kyeong hyo Lee, *Byeong-Kyun Oh

*Department of information Security, Mokpo National University

요 약

WSN에서 센서 노드는 저전력을 필요로 함으로 에너지 소비를 최소화할 수 있어야 하고 기존의 키관리 방식에서 암호키 검색시간의 절약과 키의 위치정보 추출 방법에 따른 효과적인 암호 키 관리가 필요하다. 따라서 본 논문에서는 키의 배분 및 저장을 3차원 적인 위치기반 키관리 방식을 적용하여 키관리에 있어서 기존의 위치기반의 형식보다 경로키 수를 줄여 센서 노드의 에너지 소비를 줄여 가용성 보장을 할 수 있게 하였다.

I. 서론

WSN(Wirelesss Sensor Networks)에서 노드들의 암호키는 전체 센서네트워크의 데이터 기밀성을 유지하기 위해 센서노드 하나에 대한 암호키 공격이 전체 센서네트워크로 확산되지 않도록 세밀한 제어가 필요하다. WSN을 구성하는 가장 기본적인 요소인 센서노드는 주위 환경을 모니터링 하면서 최적의 네트워크의 구성 및 기존의 유무선 통신 기술을 이용하여 사용자가 원하는 네트워크 구성을 가능하게 한다. 이러한 센서노드는 다수의 노드를 광범위한 환경에서 분산 배치하여 이용되므로 저전력, 소형화, 경량화가 필수적이다.

또한 센서 노드 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.

따라서 본 논문에서는 이러한 암호키의 효과적 관리를 위하여 키의 배분 및 저장을 3차원 적인 위치기반 키관리 방식을 적용하여 키관리에 있어서 기존의 위치기반의 형식보다 경로키 수를 줄여 센서 노드의 에너지 소비를 줄여 가용성 보장을 할 수 있게 하였다.

2. 관련연구

2.1 클러스터링 / 계층 구조 방식

센서네트워크에서 클러스터링 / 계층 구조 방식은 본질적으로 데이터 집중/ 융합에 유리한 장점이 있으며, 클러스터 헤드 노드의 관리에 의해서 하위 노드들을 조정하여 전력 소모도 낮출 수 있다. 그러나 최적의 클러스터를 만드는 것은 NP- Hard에 해당하는 문제로써 이루기 상당히 어렵다. 따라서 많은 프로토콜들이 제안 되었으며, 그 중 Low-Energy Adative Clustring Hierarchy (LEACH)가 대표적인 프로토콜이다. 기존의 위치기반 기법은 센서노드가 위치하는 셀과 인접한 셀들은 직접키를 생성할 수 있고 클러스터기반은 하나의 클러스터내에 클러스터 헤더를 중심으로 노드들이 배치되어 있다.

2.1 USN 환경에서 키분배 기법 및 문제점

유·무선 네트워크 환경에서 사용하는 기존의 공유 비밀키(secret key) 교환 방식 과 공개키(public key) 교환 방식은 저 전력, 낮은 메모리 용량 및 소량의 게이트웨이 수, 낮은 컴퓨팅 파워로 인한 느린 처리 시간 등의 한계를 가진 센서 네트워크 환경에는 적합하지 않다.

그룹키(group key)를 공유하는 방법은 하나의 센서노드라도 공격자에게 포획되면 전체 그룹키가 유출되어 전체 센서노드 사이의 통신이 안전하지 않게 된다. 또한 모든 센서노드 쌍마다 유일한 키들을 할당하는 방식은 각각의 센서노드가 전체 센서노드의 수만큼 키들을 저장해야하므로 센서노드의 메모리 제약조건 때문에 비현실적인 방법이다.

SPINS(security protocols for sensor networks)는 각 노드들이 키 교환을 위해 베이스 스테이션과 통신을 해야 하기 때문에 베이스 스테이션 주위의 노드들의 급격한 에너지 소모가 발생하므로 대규모 센서 네트워크 환경에 적합하지 않다.

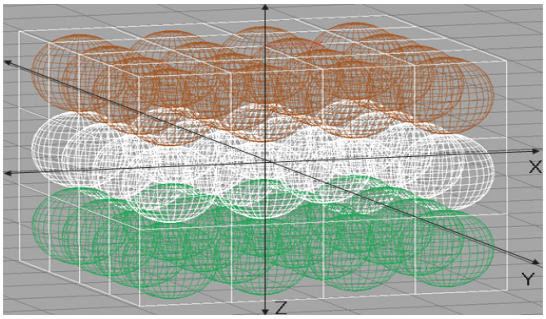
최근에 제안된 소모형 센서 네트워크 환경에 적합한 효율적인 키 분배 방법은 초기 키 설정동안에 공격자는 노드 포획 같은 물리적인 공격을 하지 못하고 초기 키 설정 이후에 모든 공격이 100% 가능하다. 또한, Eschenauer와 Gligor에 의해 제안된 임의의 키 사전 분배방법에서 발전된 방법들은 공격자가 다수의 센서노드를 포획하면 전체 키 집

합을 예측한다.

본 논문과 관련된 위치기반 키 분배 기법은 노드 추가가 용이하지만 인접한 5개의 셀의 다항식 정보만을 공유하기 때문에 네트워크가 커지면 셋업 서버는 더 많은 이변수 다항식을 만들어야 한다. 또한 셀 추가 시 셀에 위치한 노드들이 compromised된 노드의 ID를 가지고 있으므로 다항식이 노출될 수 있다.

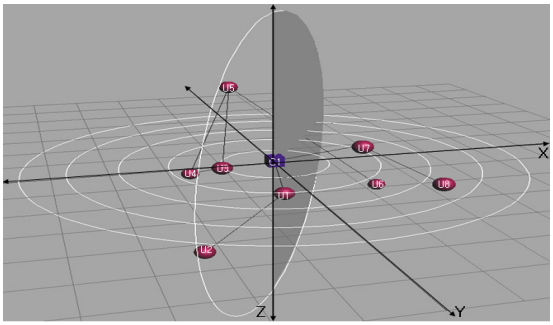
3. 클러스터 기반의 센서 네트워크

3.1 클러스터 영역 분할과 노드 배치



[그림 1] 클러스터 영역분할.

센서네트워크의 영역을 클러스터 단위로 키 분배를 하기 위하여 그림1과 같이 전체 센서 네트워크의 영역을 구의 형태로 클러스터링 한다. 그림2에서와 같이 구형태의 클러스터 내에서 센서 노드들의 위치를 3차원 분포로 모델링한다. 즉 $u1(x_i,y_j,z_k)$,$u2(x_i,y_j,z_k)$,..., $un(x_i,y_j,z_k)$는 센서의 좌표이며 배치중심 노드인 클러스터 헤더의 좌표는 $c1(x_i,y_i,z_k)$이다.

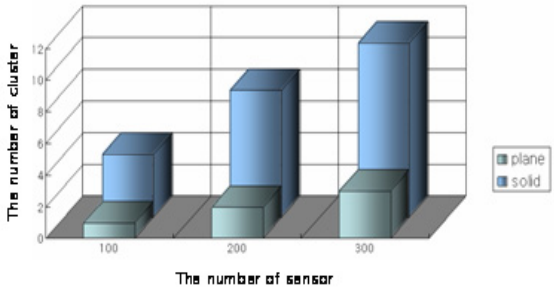


[그림 2] 클러스터$c1$ 내 센서 노드 배치.

전체 네트워크를 평면대신 입체형으로 클러스터링함으로써 동일 클러스터 내에 위치하는 센서노드의 수를 늘릴 수 있다. 그림3은 평면 클러스터링에서의 센서 노드 수와 입체형으로 클러스터링 했을 때의 센서 노드 수 차이를 나타내었다.

따라서 제안한 논문에서는 평면배치에서보다 하나의 클러스터내의 노드 수를 더 많이 배치하여 기존의 평면의 클러스터링에 비해 전체 경로키 수를 줄일 수 있어 센서노드의 불필요한 키 관리 동작을 지양하여 에너지 소비를 최소화하였다. 또한 그림 4에서와 같이 센서수에 적합한 클러스터의 수도 평면 배치에 비해 입체형으로 배치할 때 줄어들었음을 알 수 있다.

그림4는 센서 수에 적합한 클러스터수를 나타낸 것이다. 즉 평면배치에 비해 입체형 클러스터로 배치했을 때 클러스터의 수가 줄어들었음을 알 수있다. 이것은 클러스터의 중앙 센서인 클러스터 헤더가 통신의 중심에 있으므로 센서노드의 에너지 소모를 줄일 수 있다. 클러스터 내부에서 상대시간을 주면 구형 클러스터 내에 위치하는 센서가 기본적으로 많아 가르시안 분포에 따라 클러스터 헤더 부근에 분포하는 센서가 많으므로 센서 수를 제한을 두면 구형 클러스터가 평균 생성 시간이 줄어든다.

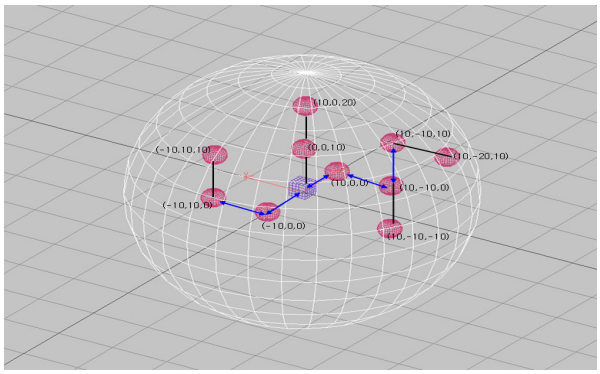


[그림4] 센서수에 적합한 클러스터의 수

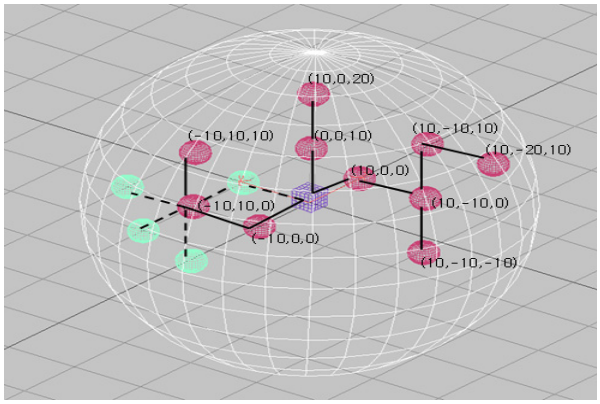
즉 센서노드의 전송반경과 클러스터 헤더의 전송 반경이 일정할 때 한 개의 센서노드의 통신 반경과 이동경로를 나타낸 것이다.

경로의 크기가 커질수록 증가함을 통해 알 수 있다. 그림10은 클러스터 전송 반경 30m일 때 경로시간에 따른 센서수 분포를 나타낸 것이다. 센서의 전송 반경이 10m인 경우 경로키 생성 시간을 상대시간 1을 기준으로 경로수가 1, 2, 3인 경우를 나타낸 것이다. 경로시간이 1인 경우는 센서반경을 10m안에 들어있는 경우 한 번에 통신할 수 있지만 경로시간이 2인 경우는 다른 이웃 노드를 경유하여 클러스터 헤더와 통신하게 된다. 경로시간이 3인 경우는 중간 노드 2개를 경유하여 클러스터 헤더와 통신하게 된다.

경로의 크기가 커질수록 증가함을 통해 알 수 있다. 그림10은 클러스터 전송 반경 30m일 때 경로시간에 따른 센서수 분포를 나타낸 것이다. 센서의 전송 반경이 10m인 경우 경로키 생성 시간을 상대시간 1을 기준으로 경로수가 1, 2, 3인 경우를 나타낸 것이다. 경로시간이 1인 경우는 센서반경을 10m안에 들어있는 경우 한 번에 통신할 수 있지만 경로시간이 2인 경우는 다른 이웃 노드를 경유하여 클러스터 헤더와 통신하게 된다. 경로시간이 3인 경우는 중간 노드 2개를 경유하여 클러스터 헤더와 통신하게 된다.



[그림 5] 센서노드의 통신반경내의 경로



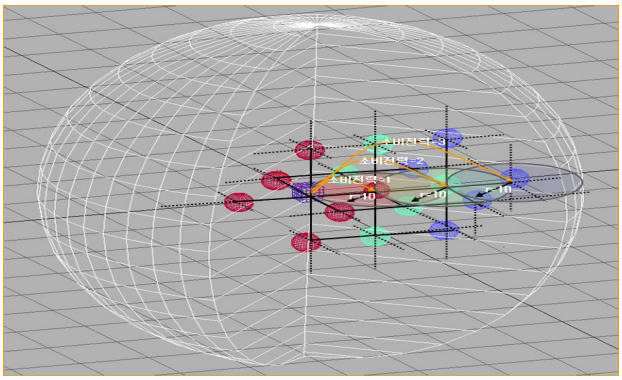
[그림 6] 위치(-10,10,0)인 센서노드의 전송과정

경로의 크기가 커질수록 증가함을 통해 알 수 있다. 그림 10은 클러스터 전송 반경 30m일 때 경로시간에 따른 센서 수 분포를 나타낸 것이다. 센서의 전송 반경이 10m인 경우 경로키 생성 시간을 상대시간 1을 기준으로 경로수가 1, 2, 3인 경우를 나타낸 것이다. 경로시간이 1인 경우는 센서반경을 10m안에 들어있는 경우 한 번에 통신할 수 있지만 경로시간이 2인 경우는 다른 이웃 노드를 경유하여 클러스터 헤더와 통신하게 된다. 경로시간이 3인 경우는 중간 노드 2개를 경유하여 클러스터 헤더와 통신하게 된다.

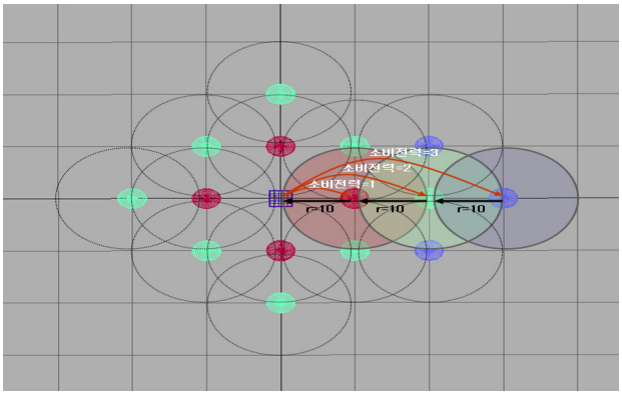
[표 1] 배치에 따른 전력 소모 형태

	평면	구형
전력 1	4	6
전력 2	8	18
전력 3	12	54
전력 4	16	22
전력 5	20	0
전력 6	24	0
전력 7	16	0
합계	100	100
평균소비전력	47.6	29.2

.



[그림 7] 입체형 배치의 소비전력 형태



[그림 8] 입체형 배치의 소비전력과 센서전송반경

즉 생성시간이 길어짐에 따라 입체형으로 클러스터링 할 때 센서의 수가 증가할 수 있음을 알 수 있다. 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 늘림으로써 인접 클러스터에 위치한 센서와의 통신에 있어서 경로키 수를 줄일 수 있고, 제안한 기법의 효율성을 시뮬레이션을 통해 나타내었고 센서노드의 불필요한 에너지 소모를 줄임으로써 가용성을 보장하게 하였다.

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] Liu, P. Ning, "Location-based Pairwise Key Establishments for Static Sensor", *SA SN'03*
[3] Farooq Anjum, Location Dependent Key Management Using Random Key predistribution In Sensor Networks,5th ACM WiSe'06.
[4] Kyeong Hyo Lee, Seok Won Jung, Byeong Kyun Oh, Sang Gug 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.
[5] Kyeong Hyo Lee, Seok Won Jung, Byeong Kyun Oh, Sang Gug 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.
[6] Cherles W. Curitis, Linear algebra: an introductory approach 3d edition.
[7] John Paul Waters, Zhengqiang Liang "Wireless Sensor Network Security: A Survey", Security In Distributed, Grid, And Pervasive Computing, 2006
[8] Pairwise Key Pre-distribution, by Du et al. *in* ACM CCS''03.