DOI: 10.3745/KIPSTC.2010.17C.2.165

# 노드 위치 예측을 통한 클러스터링 기반의 센서네트워크 키설정 메커니즘

도 인 실[†] · 채 기 준[††]


## 요 약

다양한 분야에서 응용될 수 있는 센서 네트워크 통신에 안전성을 제공하기 위해서는 센서 노드 간 pairwise 키설정이 기본이 되어야한다. 본 논문에서는 네트워크 필드를 육각형의 클러스터로 나누고 각 센서 노드마다 예상되는 위치에 따라 세 개의 서로 다른 키 정보를 사전에 나누어 주어 노드 배치 후 갖고 있는 정보를 이용하여 모든 이웃 노드와의 pairwise 키를 설정할 수 있도록 한다. 특히 키스트링 기법을 적용하여 이를 클러스터링 정보와 연계되도록 함으로써 적은 양의 정보를 가지고도 이웃한 모든 노드들 간에 pairwise 키를 설정할 수 있도록 하였다. 제안된 키설정 메커니즘을 통하여 필요한 메모리의 양을 줄이면서도 보안 강도를 높일 수 있음을 증명한다.


**키워드 : 센서 네트워크, 보안, 키관리, 클러스터, 키 스트링**

# Key Establishment Mechanism for Clustered Sensor Networks Through Nodes' Location Estimation

Inshil Doh[†] · Kijoon Chae[††]


## ABSTRACT

Sensor network can be applied in many areas in our life, and security is very important in applying sensor network. For secure sensor communication, pairwise key establishment between sensor nodes is essential. In this paper, we cluster the network field in hexagonal shapes and preassign three different kinds of key information for each sensor according to its expected location. We adopt overlapped key string pool concept for our clustered network architecture and every node uses the part of sub-strings for setting up pairwise keys with all neighboring nodes in its own cluster and from different clusters according to respective position with small amount of information. Our proposal decreases the memory requirement and increases security level efficiently.


**Keywords : Sensor Network, Security, Key Management, Cluster, Key String**

## 1. 서 론

향후 유비쿼터스 통신 환경에서 가장 핵심 기술로 자리 잡을 것으로 예상되는 센서 네트워크는 현재 군통신, 환경 감시, 환자 관찰, 홈 네트워크 등 다양한 분야에서 적용되고 있다. 센서 네트워크 통신에서 가장 중요한 요소 중의 하나로 보안을 들 수 있는데 이는 센서 노드를 배치하는 상황이 일반적으로 사람이 직접 접근하기 힘든 경우가 많고 이는 센서 노드의 직접적인 포획 공격으로 이어지는 경우가 많기 때문이다. 노드가 포획되는 경우, 노드의 키관련 정보가 모두 적에게 노출되어 네트워크 자체가 마비되거나 적에게 오히려 이용될 수 있어 매우 위험한 상황이 될 수 있다. 그러나 센서 노드가 갖는 제약으로 인해 기존의 키설정 방식은 센서 노드에게 직접 적용하기 힘든 경우가 많다.

따라서 센서 네트워크에 적합한 방식의 키관리 기법이 많이 제안되어왔는데 그 중 하나가 키를 노드 배치 이전에 할당하는 방식이다. 그러나 노드의 수가 많은 경우 공중에서 노드를 임의로 뿌리는 형태로 이루어지는 경우가 많아 실제적인 위치를 사전에 정확히 파악하는 어려움이 있다. 특히 클러스터 네트워크인 경우 노드가 위치하게 될 클러스터나 이웃하는 노드에 따라 필요정보가 달라질 수 있는데 기존 연구는 이점을 고려하고 있지 않다. 본 논문에서는 클러스터 기반의 pairwise 키 설정 메커니즘을 제안하여 노드의

※ 이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임. (NO.R01-2009-0083-985).
† 정 회 원 : 이화여자대학교 컴퓨터공학과 연구교수
†† 종신회원 : 이화여자대학교 컴퓨터공학과 교수
논문접수 : 2009년 10월 20일
수 정 일 : 1차 2009년 12월 16일, 2차 2010년 2월 22일
심사완료 : 2010년 2월 24일

배치 후 이웃 노드 정보를 파악하고 갖고 있는 키 정보를 이용하여 키를 설정하는 방법을 제안한다. 제안된 메커니즘은 네트워크의 연결성을 보장하며 오버헤드를 줄이는 효과를 갖는다.

## 2. 관련 연구

센서 네트워크 키 설정에 관한 초기의 연구로 Eschenauer와 Gligor(EG)[3]는 랜덤 키 사전 분배 스킴을 제안하였다. 즉, 노드 배치 전 각 센서 노드가 키풀에서 키를 선택한 후 배치 이후에 이웃한 노드 간에 공통키를 찾아 둘 간의 pairwise 키로 사용하는 방법이다. 이 방식은 후에 Chan, Perrig, Song[4]에 의해 개선되어 두 노드 간 최소한 $q$개 이상의 키를 공유하게 함으로써 노드포획 공격에의 저항성을 높였으나 일정 이상의 연결성을 제공하기 위해서는 저장장소가 많이 필요하다는 단점을 갖는다. Du 등[5]은 이를 좀 더 발전시켜 [3]의 기본 스킴과 Blom의 키 관리 스킴[2]을 통합한 방식을 제안하였다. 통합된 방안에서 각 노드는 여러 개의 행렬로부터 행을 선택하고 이웃 노드 간에 동일 행렬에서 행을 선택했다면 이를 이용하여 키를 설정하는 방식을 제안하였다. 이 방식은 노드포획 공격에 효과적으로 대응할 수 있으나 노드가 오염되는 경우 빠른 속도로 connection 자체가 오염될 수 있다는 단점을 갖는다. Blundo 등[7]은 $t$개의 멤버를 갖는 그룹을 가정하고 멤버의 일부가 결탁하는 경우에도 안전한 통신을 보장할 수 있는 방식을 제안하였다. 이 방식은 멤버에게 저장 오버헤드를 많이 주지 않으면서도 통신의 비용을 절감할 수 있다는 점에 중점을 두고 있다. Liu 와 Ning[6]은 Blundo의 다항식 기반 키 분배에 기반하여 또 다른 pairwise 키 설정기법을 제안하였는데 다항식 풀을 두고 이 풀에서 임의로 선정된 다항식의 부분정보(share)를 노드에게 할당하는 방식을 취하였다. Du 등[8]은 키 사전분배 스킴에서 노드의 위치정보를 처음으로 사용하여 노드를 그룹으로 나누고 각 그룹은 키 풀에서 부분집합을 할당받도록 하였다. 기본 방식에 비하여 이 스킴은 더 적은 저장공간을 필요로 하는 동시에 높은 연결성을 제공하고 노드 포획 공격에 더 높은 저항성을 나타낸다. Yu 등[9]은 네트워크 필드를 육각형의 그리드로 나눈 후 노드의 배치정보를 이용하는 또 다른 키 사전분배 기법을 제안하였다. 이 스킴은 좀 더 높은 네트워크 연결성과 낮은 저장공간을 요구하면서 동시에 더 강력한 노드 포획공격에의 대응성을 갖는다. B. Lai 등[10]은 각각의 키 대신에 키 스트링 풀(KP)을 이용하여 이 스트링으로부터의 일부분을 키 정보로 사용하여 각 센서 노드에 사전 분배하고 두 노드가 갖고 있는 스트링의 교차부분(overlapped)을 키 계산에 사용하는 방식을 제안하였다. 이 기법은 저장공간은 줄였으나 네트워크 연결성이 낮다는 단점을 갖는다. Huang 등[12]은 배치정보를 이용하지 않고도 기본 기법에 비해 좀더 향상된 결과를 보여주는 기법을 제안하였으나 보안성의 연속적인 특성면에서 단점을 갖는다. 이를 보완한 기법으로 Durresi 등[13]은 노드의 종류를 세가지로 나누고 노드 배치를 여러 단계를 거쳐 수행하며 매 단계별로 다른 키 풀을 사용하도록 하였다. 또한 [14-16] 등에서는 pairwise key와 group key의 문제를 동시에 해결하고자 시도하였다.

## 3. 네트워크 모델

네트워크는 육각형태의 클러스터로 구성되고 각 클러스터 내에 위치할 노드는 배치되기 전 예상되는 클러스터에 따라 필요한 키정보를 분배받는다. 모든 센서 노드는 정적인 센서이며 2차원 가우시안 분배에 따라 배치된다. 키분배 서버는 각 센서 노드가 어느 클러스터에 배치될지 사전에 파악할 수 있으며 각 클러스터의 위치에 따라 각각의 키정보를 분배한다. 노드의 배치와 이웃 노드 파악을 통한 키설정 단계에서 공격은 없다고 가정한다.

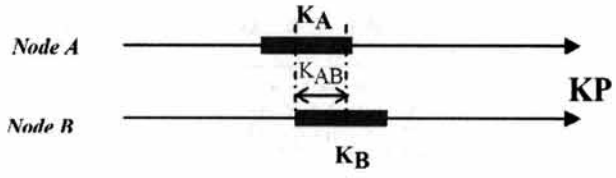
네트워크 필드에 배치될 노드는 다음 식 (1)과 같은 이차원 가우시안 분포에 따라 그 위치가 정해진다. $(x_i, y_i)$는 노드의 배치지점이고 $\sigma$는 표준편차, $\sigma^2$는 공중에서 센서 노드를 뿌리는 위치와 관련되는 값이다.

$$f_i(x,y) = \frac{1}{2\pi\sigma^2} e^{-\left[(x-x_i)^2+(y-y_i)^2\right]/2\sigma^2} \quad (1)$$

## 4. Pairwise 키 설정

### 4.1 OKS(Overlapped Key Sharing)

센서 노드가 갖는 저장 오버헤드를 줄이기 위해 본 연구에서는 [10]에서 제안된 스트링 키 풀 방식을 응용한다. Overlapped Key Sharing(OKS) 프로토콜은 긴 비트 스트링 key-string-pool(KP)을 생성하여 이 KP의 일부분을 센서 노드에 저장하도록 하고 두 노드가 키를 설정하려할 때 서로 갖고 있는 스트링의 겹치는 부분을 사용하여 키를 계산한다. (그림 1)에서와 같이 노드 A와 노드 B는 각자 갖고 있는 키정보를 이용하여 서로 겹치는 부분을 파악하고 겹치는 영역을 이용하여 둘 사이에 사용할 $K_{AB}$를 계산한다. 키 스트링이 임의로 할당되기 때문에 서로 다른 노드는 서로 다른 공통부분 길이를 갖는다. 일정크기의 키를 설정하기 위해서 패딩비트가 추가되거나 해쉬함수를 이용할 수 있다. 키의 길이에 따라 보안의 정도가 달라지며 노드 배치 전 각 노드는 서브키 스트링 풀을 할당받아 이웃 노드쌍은 상호간에 키 스트링의 교차부분을 찾는다.

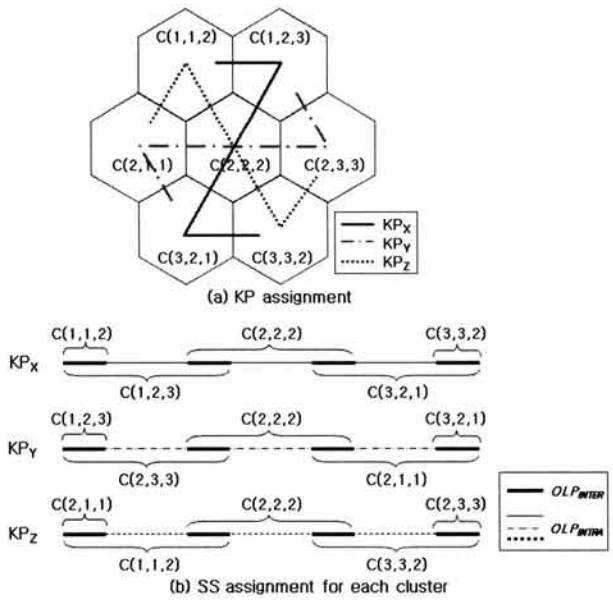



(그림 1) OKS(Overlapped Key Sharing protocol)의 예

### 4.2 서브키 스트링

[11]의 연구에서 우리는 네트워크 필드를 사각의 클러스터로 나누고 서로 다른 키 스트링을 할당하여 이웃 노드 간에 키를 설정하는 방식을 제안한 바 있다. 필드를 사각으로 나누기 때문에 각 클러스터는 수평방향으로 두 개의 클러스터와 접하고 수직방향으로 두 개의 클러스터와 접하며 각 센서 노드는 두 가지 서로 다른 서브키 스트링을 할당 받게 되는 방식이다. 문제는 이 경우 수직 수평방향에 포함되는 클러스터 내의 센서 노드와는 키를 설정할 수 있으나 대각선 방향으로 존재하는 클러스터의 노드와는 키를 직접적으로는 설정할 수 없다는 점이다. 물론 확률적으로 대각선 방향에 존재하는 클러스터에 포함되는 이웃 노드의 수는 가로나 세로에 접하는 클러스터의 경우보다 적지만 노드의 수가 많아지는 경우 비례적으로 그 수도 더 늘어난다. 이러한 문제를 해결하여 네트워크 연결을 100%로 하기 위해 본 연구에서는 네트워크 필드를 육각형태의 클러스터로 나누고 각 센서 노드에 서브키 스트링을 세 개 할당하는 방식을 취하였다.

(그림 2)에서와 같이 세 개의 서로 다른 키스트링 풀을 만들고 각각에 좌표를 할당한다. 즉 $KP_X$(Key string Pool X)의 경우 좌표 (1,1,2), (1,2,3), (2,2,2), (3,2,1), (3,3,2)에 위치하는 클러스터에 배치된다. 각 KP는 $OLP_{INTER}$(OverLapped Part for inter-cluster communication)와 $OLP_{INTRA}$ (OverLapped Part for intra-cluster communication)로 구성된다. C(1,1,2)에 위치할 것으로 예상되는 센서 노드의 경우 $KP_Z$, $KP_X$ 두 개 SS(서브키 스트링)가 할당되는데 $KP_Z$-$SS$는 (그림 2)-(b)에서와 같이 하나의 $OLP_{INTRA}$ 부분과 두 개의 $OLP_{INTER}$ 부분이며 $KP_x$-$SS$는 $OLP_{INTER}$로만 이루어져 있다. 이렇게 받은 키 정보를 이용하여 센서 노드는 키를 설정하게 되는데 클러스터 내의 통신이 필요한 경우 $KP_Z$-$SS$의 $OLP_{INTRA}$부분을 이용하고 클러스터 간의 통신이 필요한 경우 $KP_x$-$SS$의 $OLP_{INTER}$부분과 $KP_Z$-$SS$의 $OLP_{INTER}$부분을 필요에 맞게 이용한다. 필드의 바깥쪽에 위치한 클러스터의 경우 두 개의 SS 정보를 이용하여, 필드의 안쪽에 위치한 노드는 세 개의 SS 정보를 이용하여 클러스터 내, 그리고 클러스터 간 모든 이웃 노드와 pairwise 키를 설정할 수 있다.




(그림 2) 클러스터 별 SS(서브키 스트링) 할당

### 4.3 Pairwise 키 설정

#### 4.3.1 서브키스트링 할당

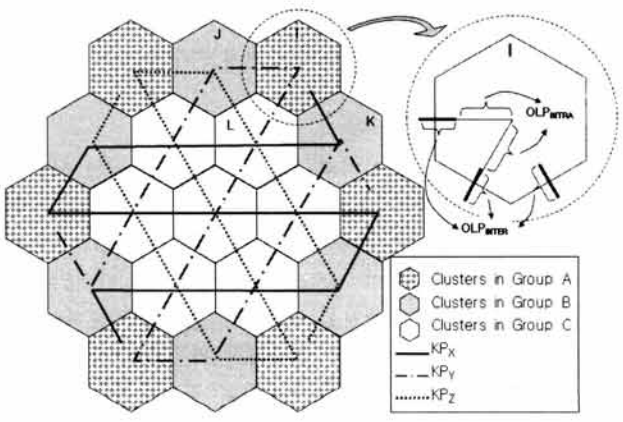
키 서버가 세 개의 서로 다른 KP를 생성하고 나면 모든 노드는 각 노드가 위치할 것으로 예상되는 위치에 따라 각각 세 개의 키 스트링으로부터의 일부분(SS)을 사전분배 받는다. 각 노드는 $KP_X$, $KP_Y$, $KP_Z$로부터 최소 두 개 이상의 SS를 할당받으며 각 SS는 하나의 $OLP_{INTRA}$ 부분과 이를 둘러싼 두 개의 $OLP_{INTER}$ 부분으로 구성된다.

본 연구에서 사용되는 용어는 <표 1>에서와 같다.

사전에 분배된 키정보는 클러스터의 좌표에 따라 다르다. (그림 3)에서 A그룹의 클러스터는 네트워크 필드의 가장자리에 육각형의 각에 해당하는 위치의 클러스터이며 이들은 이웃하는 클러스터의 수가 3이다. 따라서 하나의 SS 전체와 또 다른 SS로부터의 하나의 $OLP_{INTER}$부분을 할당받는다. 예를 들어 클러스터 I의 노드는 $KP_Y$ 의 SS로부터의 $OLP_{INTER}$

〈표 1〉 사용되는 용어

| 용어 | 설 명 |
|---|---|
| KP | 키스트링 풀 |
| SS | 서브키 스트링 |
| $OLP_{INTER}$ | 서로 다른 클러스터에 있는 센서 노드간의 키설정을 위해 사용되는 오버랩 부분 |
| $OLP_{INTRA}$ | 동일 클러스터에 있는 센서 노드간의 키설정을 위해 사용되는 오버랩 부분 |
| OV | 오버랩 threshold |
| R | 센서 노드에게 할당되는 서브키 스트링의 수(본 연구의 경우 R=3) |
| K | 각 SS의 길이 |




(그림 3) 19개 clusters로 구성된 네트워크에서의 스트링 키 풀 할당

〈표 2〉 필요한 서브키 스트링 비교

| Cluster location | Required SS | Number of clusters | | |
|---|---|---|---|---|
| | | 7 | 19 | 37 |
| Group A | $1OLP_{INTRA}$ + $3OLP_{INTER}$ | 6 | 6 | 6 |
| Group B | $2OLP_{INTRA}$ + $4OLP_{INTER}$ | 0 | 6 | 12 |
| Group C | $3OLP_{INTRA}$ + $6OLP_{INTER}$ | 1 | 7 | 19 |

를 사용하여 클러스터 J와 L의 센서 노드와 키를 설정하고 클러스터 K의 노드와는 $KP_X$의 SS로부터의 $OLP_{INTER}$를 사용하여 키를 설정할 수 있다. 클러스터 내 통신만을 필요로 하는 노드 간에는 $KP_Y$의 SS로부터의 $OLP_{INTRA}$를 사용한다. 클러스터 그룹 B의 노드는 가장자리에 위치한 클러스터에 포함되지만 각의 위치에 위치한 것이 아니어서 두 개의 KP로부터 두 개의 SS를 할당받는다. 네트워크 필드의 안쪽에 위치한 클러스터는 세 개의 KP로부터 서로 다른 세 개의 SS를 할당받는다. <표 2>에 이 내용이 정리되어있다.

전체 클러스터의 수는 클러스터의 수가 c, 네트워크 중심으로부터 클러스터의 레이어의 수가 n일 때 다음 식 (2)와 같이 계산된다.

$$c=3n(n-1)+1 \quad (2)$$

레이어의 수가 많아질수록 전체 클러스터의 수가 많아지게 되는데 실제 상황에서는 클러스터 개수가 지나치게 많아지는 경우, 네트워크의 필드가 너무 넓고 노드의 수가 지나치게 많아 전체를 하나의 키 스트링으로 관리하는 것은 오히려 효율성이나 보안의 측면에서 적절하지 못하므로 전체를 몇 개의 서브필드로 나누고 서브필드별로 별도의 키설정 및 분배를 수행하는 것이 좋다.

4.3.2 노드 배치 및 이웃노드 찾기

모든 센서 노드는 2차원 가우시안 분포에 따라 배치되며 예상 위치에 따라 SS를 사전에 할당받고 배치 후 노드들은 이웃한 노드와 HELLO 메시지를 주고받음으로써 이웃 노드의 클러스터 좌표값을 찾는다. 받은 메시지를 보고 모든 노드는 자신이 각 클러스터의 중심에 위치했는지 가장자리에 위치했는지 판단하여 이에 따른 키설정을 수행한다.

4.3.3 Pairwise 키 설정

모든 이웃노드 쌍은 자신과 상대방이 가지고 있는 서브키 스트링의 교차부분을 이용하여 키를 설정한다. 키를 설정할 때 필요한 교차 길이는 시스템이 정하고 각 센서 노드 쌍은 교차 시작 위치를 정하여 시작 위치로부터 일정 길이만큼을 이용, 키 계산의 기본 정보를 찾고 이 정보를 이용하여 일정 크기의 키를 만들어 낸다. 교차시작 위치가 SS의 뒤쪽인 경우 키 설정을 위해 필요한 최소한의 길이에 못 미칠 수 있어 이 경우 패딩비트가 추가되거나 해쉬함수를 이용하여 일정 길이의 키를 만들어 낸다.

pairwise 키 설정은 SS의 종류와 사용되는 SS의 위치에 따라 세 가지 범주로 분류될 수 있다.

*4.3.3.1 각 클러스터의 중심부분에 배치된 센서 노드간의 키 설정*

노드가 다른 클러스터로부터의 이웃노드를 찾지 못한 경우 $KP_X$, $KP_Y$, $KP_Z$ 의 $OLP_{INTRA}$ 만을 사용한다. 네트워크 필드의 바깥쪽에 각진 위치의 클러스터가 아닌 경우 두개 이상의 $OLP_{INTRA}$를 갖게 된다. 예를 들어 (그림 2)-(a)의 C(2,2,2) 위치는 세 개의 SS를 갖는다. 이 경우, 모든 쌍의 노드는 어떤 서브키 스트링을 사용할 것인지 정하고 나서 서브키 스트링의 시작위치를 교환한다.

*4.3.3.2 서로 이웃한 클러스터의 경계지역에 위치한 센서 노드 쌍의 키 설정*

센서 노드가 다른 클러스터에 속한 노드와 이웃하는 경우 이 노드는 게이트웨이가 된다. 따라서 이웃 노드가 동일한 X,Y,또는 Z좌표값을 갖는지 확인하여 만일 동일한 X좌표값을 갖는 경우 $KP_X$ 를, 동일한 Y나 Z좌표 값을 갖는 경우 $KP_Y$와 $KP_Z$ 를 각각 사용하여 키를 설정한다. C(2,2,2)에 위치한 센서의 경우 $KP_X$, $KP_Y$, $KP_Z$로부터 총 6개의 $OLP_{INTER}$s를 갖게 되며 이 6개의 정보를 이용하여 모든 경계의 모든 이웃노드와 키를 설정할 수 있다. 즉, C(1,2,3), C(3,2,1)와는 $KP_X$-$SS$로부터의 $OLP_{INTER}$를, C(2,1,1)나 C(2,3,3)와는 $KP_Y$-$SS$로부터의 $OLP_{INTER}$를, C(1,1,2)나 C(3,3,2)와는 $KP_Z$-$SS$로부터의 $OLP_{INTER}$를 사용한다.

*4.3.3.3 사전에 예상되었던 위치를 벗어나 배치된 노드의 경우*

이러한 노드와 이웃노드 간의 키는 클러스터 경계영역에 배치되지 않았다 하더라도 $OLP_{INTER}$를 사용하여 키를 설정할 수 있다. 예로써 C(1,1,2)에 배치될 것으로 예상되었던 노드가 C(1,2,3)에 배치되었다면 이 노드들은 C(1,2,3)에 배치된 다른 모든 노드들과 $OLP_{INTER}$를 사용하여 키설정이 가능하므로 정상적인 멤버로 활동이 가능하다. 특히 식 (1)의 가우시안 분포에 따라 노드를 배치하므로 $\sigma^2$값에 따라 약간 달라질 수는 있지만 자신의 클러스터를 벗어난다 하더라도 이웃하는 클러스터까지도 벗어나서 그 다음 클러스터에 노드가 배치될 가능성은 매우 낮다. 이러한 방식으로 키설정을 가능성을 높이고 따라서 노드의 사용가능성을 더욱 높일 수 있다.

4.3.4 키정보 삭제

키가 설정되고 난 후, 각 노드는 최소로 필요한 하나의 SS 정보만을 남기고 나머지를 삭제한다. 삭제되지 않은 SS는 새로 이웃이 된 노드와 새롭게 pairwise 키를 설정할 때 사용된다. 만일 사전에 배치된 모든 SS를 유지한다면 노드가 포획되었을 때 좀 더 많은 부분의 키스트링이 노출되어 네트워크 자체에 큰 위협이 될 수 있기 때문이다. 노드 X가

서로 다른 클러스터로부터의 이웃 노드를 발견한 경우 X는 차후에 또 다시 해당 클러스터의 새로운 노드와 키를 설정해야할 가능성이 있기 때문에 해당 SS를 남기고 나머지는 삭제한다.

## 5. 성능 분석

본 연구에서는 다중 키 스트링 풀 방식을 채택함으로써 각 센서 노드의 저장 오버헤드는 줄이고 네트워크 연결성과 예상 클러스터 영역을 벗어난 센서 노드의 사용가능성을 높이는 효과를 기대할 수 있다. 또한 노드의 위치에 따른 서브스트링의 서로 다른 부분을 사용함으로써 설정된 키의 보안강도를 더 높일 수 있는데 이는 노드가 배치된 위치에 따라 서브스트링의 서로 다른 부분을 사용하여 키를 계산할 수 있기 때문이다. 이는 키 스트링 프로토콜을 적용함으로써 전체적인 저장 오버헤드를 매우 낮추었기 때문에 가능하다.

본 장에서는 제안 메커니즘을 통해 노드가 필드에 배치된 후 이웃 노드 간 pairwise 키를 설정할 때 얼마나 효율성을 가질 수 있는 지를 네트워크의 연결성, 차후에 노드가 포획되었을 때 키 정보가 노출될 확률, 키설정에 필요한 에너지의 양, 이를 저장할 때 필요한 오버헤드, 네트워크의 확장에 대처할 수 있는 능력 등으로 분류하여 분석하였다.

### 5.1 네트워크 환경

센서는 제한된 에너지를 갖는 노드로 사전에 키설정에 필요한 키를 분배받고 식 (1)에서 기술한 바와 같이 네트워크 필드에 2차원 가우시안 분포에 따라 배치된다고 가정한다. 즉, 공중의 일정 지점에서 센서 노드를 필드에 뿌리게 되어 해당 지점에 좀 더 많은 노드가 배치되고 배치 중심에서 멀어질수록 노드의 밀집도가 떨어지는 형태이다. 이 때 네트워크 필드는 육각형으로 클러스터링하고 네트워크 규모에 따라 클러스터의 크기와 개수가 달라질 수 있으며 각 클러스터의 중심 위치에서 노드를 뿌린다.

분석에 필요한 기본적인 파라미터 값으로 네트워크 연결성은 0.99999, 센서 노드의 수는 1000~10000개, 키길이는 64 비트, 키의 ID는 14 비트로 가정하였으며 키스트링의 수 R은 3으로 하였다.

### 5.2 연결성

[3]에서 분석한 바와 같이 한 노드의 예상 무선링크의 수 $d$는 $n$이 네트워크의 노드 수일 때 다음과 같이 정의된다.

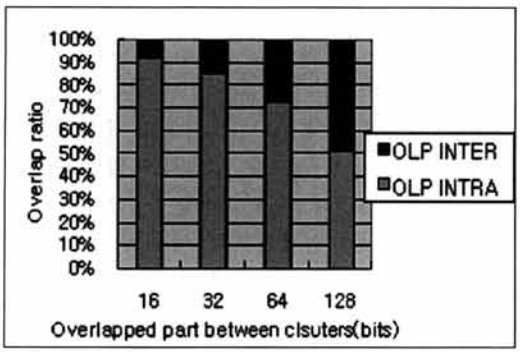
$$d=\left(\frac{n-1}{n}\right)(\ln(n)-\ln(-\ln(p))) \quad (3)$$

위의 방정식에 의하면 네트워크 연결 확률 $p$가 0.99999이고 네트워크 내 노드 수가 10,000개일 때 각 노드의 연결정도(degree of connectivity)는 20이다. 만일 안전한 연결을 원하는 경우라면 각 노드는 $d$개의 안전한 링크를 가져야한다는 의미이다. OKS의 경우, 연결정도가 약 0.5, 센서 노드의 수를 10,000개로 가정하였다. 이러한 조건에서 이웃 노드의 수는 적어도 40이상이어야 하는데 밀집도가 지나치게 커진다. 이는 각 노드들이 KP로부터 임의로 서브스트링을 분배받기 때문이다. 본 연구에서는 합리적인 밀집도를 유지하면서 모든 이웃 노드들과 키를 설정할 수 있다는, 즉, 이웃 노드의 수가 많든 적든 언제나 모든 이웃 노드와 키를 설정할 수 있다는 장점을 갖는다. 만일 센서 네트워크 필드가 더 넓어지면 좀 더 많은 클러스터가 존재할 것이고 각 KP는 좀 더 많은 클러스터에 할당될 것이다. 그러나 그러한 경우에도 동일한 규칙이 적용되므로 모든 이웃한 노드쌍 사이에 pairwise키를 설정할 수 있다.

### 5.3 노드포획 공격에 대한 저항성

공격자가 각 클러스터에서 하나씩의 센서 노드를 포획할 수 있다면, 그리고 모든 센서 노드들이 사전에 할당받은 모든 키관련 정보를 계속 가지고 있다면 전체 스트링 키 풀이 공격자에 의해 복원될 수 있다. 그러나 모든 클러스터에서 노드를 하나씩 포획하는 것도 쉽지 않을뿐더러 본 연구에서 제안하는 방식에서는 센서 노드들이 키를 설정한 후 꼭 필요한 하나의 SS만 남기고 나머지는 모두 삭제하는 방식을 취함으로써 많은 센서 노드가 포획되더라도 원래의 KP의 복원은 거의 불가능하다. 또한 각 센서에 할당되는 SS는 임의로 선택되기 때문에 공격자 입장에서 이를 다시 원래의 스트링으로 복원하는 것은 거의 불가능하다고 할 수 있다.

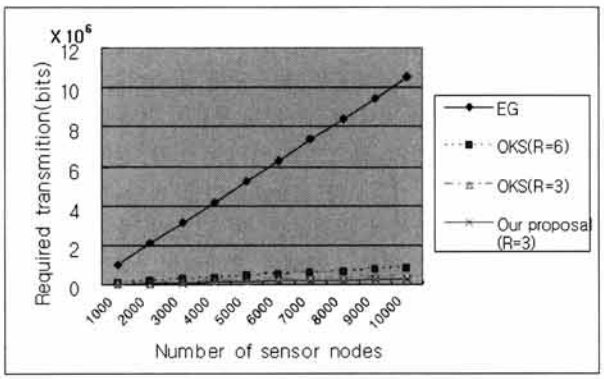
서브키 스트링의 교차율은 노드포획 공격에는 저항성에 있어서 매우 중요한 요소가 된다. 교차율이 높은 경우 키를 생성하기 위한 정보가 많으므로 키의 길이가 길어질 수 있고 결국 공격자가 키정보나 pairwise키를 찾아내기가 쉽지 않다. 또 다른 관점에서 살펴보면, 키 스트링 풀의 정보 중 더 많은 부분이 각 센서 노드에게 할당되어 노드가 포획되는 경우 좀 더 많은 정보가 노출될 수 있다. 이 경우 공격자는 전체 키나 일부 스트링을 복원하기 위해 상대적으로 적은 수의 노드를 포획하면 된다. 이러한 tradeoff는 구현 시 매우 중요한 요소로 작용한다. 또한 $OLP$는 두 부분, 즉, 클러스터 간 통신을 위한 $OLP_{INTER}$ 와 클러스터 내 통신을 위한 $OLP_{INTRA}$로 구성되는데 하나가 길면 다른 하나가 짧아지는 상호관계를 갖게 된다. 그러므로 좀 더 많은 노드가 경계지역에 배치된다면 $OLP_{INTER}$ 가 짧아지고 $OLP_{INTRA}$ 가 길어져야하며 노드가 클러스터의 중심에 집중되는 경우는 반대가 되어야한다. 즉 노드 배치 시에 $\sigma^2$의 값을 고려하여 두 값의 비율이 정해져야 한다. (그림 4)는 두 값의 관계를 나타낸다. 그림에서 보는 바와 같이 클러스터 간의 경계에 좀 더 많은 노드가 배치되는 환경에서는 $OLP_{INTER}$의 비율을 높여 클러스터 간 통신을 위한 키설정에 좀 더 긴 스트링키를 할당하고 경계 부분의 노드 수가 적을 것으로 예상되는 경우에는 $OLP_{INTRA}$의 비율을 높여 클러스터 내 통신에 필요한 키 설정에 사용될 스트링의 비율을 높인다.




(그림 4) $OLP_{INTER}$와 $OLP_{INTRA}$의 비율

### 5.4 에너지 소비량

네트워크 연결성 0.99999, 키 풀 크기 10,000의 경우 EG 프로토콜은 각 노드에 75개의 키를 저장해야하지만 OKS를 적용한 본 연구의 경우 세 개의 키 스트링을 각 노드가 가지며 각 키는 64비트, 각 키의 ID는 14 비트로 설정한다(키의 ID는 키 풀에서 각 키의 주소이며 키 자체가 아니라 이 주소를 브로드캐스트함으로써 교차부분을 찾는다). 필요한 에너지량은 키를 찾는 단계에서 키의 ID가 이웃 노드에 브로드캐스트될 때 소비되는 에너지로 전송되는 정보의 양에 비례한다. EG 프로토콜은 각 14비트의 ID 75개를 브로드캐스트해야하며 총 1050 비트가 전송된다. OV, 즉 교차부분이 64 비트인 OKS에서는 각 키 스트링의 시작 위치만을 전송함으로써 나머지 부분을 시작 위치를 이용해 계산할 수 있다. 본 연구에서 노드는 어떤 SS가 사용될 것인지의 정보만 브로드캐스트되므로 각 SS의 시작 위치만 전송하여 전체적인 에너지 소모를 더욱 줄일 수 있다. (그림 5)에서는 R이 키스트링의 수일 때 EG, OKS, 제안 기법 각각에서 전송되는 비트의 수를 비교하였다.



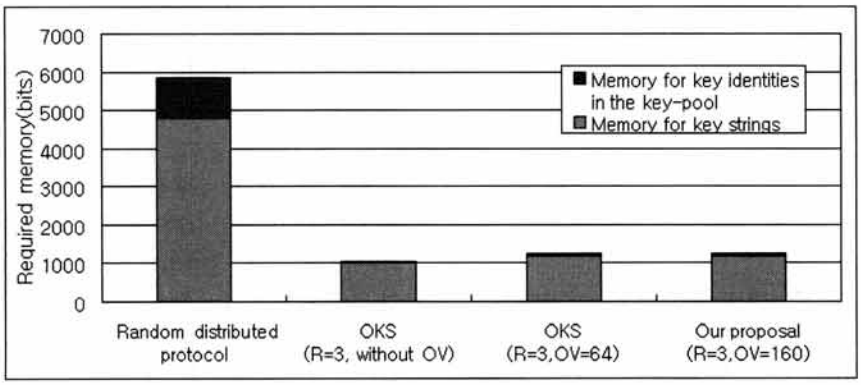

(그림 5) EG, OKS, 제안 기법의 에너지 소비량 비교

### 5.5 저장 오버헤드

(그림 6)에서 EG 프로토콜, OKS 프로토콜, 제안 메커니즘 간의 저장 오버헤드를 분석하였다. EG 프로토콜은 키길이 64, 키의 수 75일 때 각 센서 노드에 필요한 저장 오버헤드가 5850 비트이며, OKS 프로토콜의 경우 각 키 스트링의 길이가 400이고 OV=64(교차부분이 64비트인 경우)일 때 약 1300비트의 오버헤드를 필요로 한다. 제안 기법의 경우 OV=64일 때 OKS와 거의 유사한 정도의 오버헤드를 필요로 하지만 SS의 모든 부분이 오버랩되면서 각 센서 노드가 키 계산 시 OLP의 모든 위치를 사용할 수 있을 뿐 아니라 네트워크 연결성을 100% 보장해준다는 장점을 갖는다.

### 5.6 확장성

노드가 네트워크 필드에 추가되면 이웃한 노드들과 새롭게 pairwise 키를 설정해야 한다. 새롭게 배치되는 노드도 세 개의 서로 다른 서브키 스트링을 할당받은 상태이므로 세 개의 스트링 중 하나를 선택하여 $OLP_{INTRA}$를 이용하여 키를 설정한다. 만일 다른 노드가 하나의 SS만을 갖고 있는 경우 새로 배치된 노드는 이와 동일한 SS를 선택한다. 확률이 높지는 않으나 새로운 노드가 클러스터의 경계지역에 배치되는 경우 다른 클러스터에 속한 노드와 키를 설정해야한다. 이 경우 사용하지 않는 SS를 만일 지운 상태라면 공통키를 설정할 수 없으므로 path key 설정방법에 의해 키를 설정한다. 그러나 이런 경우가 발생할 확률은 매우 낮으므로 효율성을 떨어뜨리는 요인이 되지 않는다.




(그림 6) EG, OKS, 제안기법의 저장 오버헤드 비교

## 6. 결 론

본 연구를 통해 센서 네트워크에서의 키 관리를 위해 클러스터링과 스트링키 오버랩 기법을 이용한 이웃 노드 간 pairwise 키 설정 메커니즘을 제안하였다. 제안 메커니즘에서는 먼저 네트워크 필드를 육각형태의 클러스터로 나누고 센서 노드를 2차원 가우시안 분포에 따라 필드에 배치한다. 각 육각형태의 클러스터는 3차원의 좌표값을 가지며 각 센서 노드가 배치 후 예상되는 위치에 따라 키 스트링 풀 ($KP_X$, $KP_Y$, $KP_Z$) 로부터의 서브키 스트링을 센서 노드별로 사전에 할당한다. 동일한 클러스터 내의 이웃 노드들 간의 pairwise 키 설정을 위해서 각 노드는 서브키 스트링의 $OLP_{INTRA}$ 정보를 사용하고 서로 다른 클러스터에 포함된 노드 간의 키설정에는 $OLP_{INTER}$ 정보를 사용한다. 이웃한 두 클러스터 간에는 최소한 하나이상의 서브키 스트링을 갖게 되어 이 스트링을 클러스터 간의 키 설정에 사용한다. 결과적으로 제안한 메커니즘은 모든 이웃 노드 간에 pairwise 키를 설정할 수 있으며 네트워크를 클러스터링하고 OKS 개념을 적용함으로써 저장 오버헤드를 줄이는 효과를 가져올 수 있다. 또한 서로 다른 세 개의 키스트링 풀을 설정함으로써 보안 수준을 높이고 노드포획 공격에 대한 저항성을 높일 수 있다. 향후 연구로는 제안된 키 설정 기법을 바탕으로 안전한 데이터 전송에 관련된 연구를 진행하고자 한다.

## 참 고 문 헌


[1] D.W. Carman, P.S. Kruus, and B.J.Matt, "Constraints and approaches for distributed sensor network security," Technical report, NAI Labs, 2000.

[2] R. Blom, "An optimal class of symmetric key generation systems. Advances in Cryptology," Proc. of EUROCRYPT'84, LNCS 209, 1985.

[3] L. Eschenauer and V.D. Gligor, "A key management scheme for distributed sensor networks," Proc. of the 9th ACM CCS'02, pp.41-47, 2002.

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

[5] W. Du, J. Deng, Y. S. Han, and P. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," Proc. of 10th ACM CCS'03, 2003.

[6] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," Proc. of 10th ACM CCS'03, pp.52-61, 2003.

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

[8] W. Du, J. Deng, Y. S. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," Proc. of IEEE INFOCOM, 2004.

[9] Z. Yu and Y. Guan, "A Robust Group-based Key Management Scheme for Wireless Sensor Networks," IEEE Communications Society, WCNC 2005.

[10] B. Lai, D. Hwang, S. Kim, and I. Verbauwhede, "Reducing radio energy consumption of key management protocols for wireless sensor networks," Proc. of ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED'04), pp.351-356, 2004.

[11] I. Doh, K. Chae, "A key setup mechanism utilizing dual key strings for secure sensor communication," Proc. of 9th International Conference on Advanced Communication Technology(ICACT), 2007.

[12] D. Huang, M. Mehta, D. Medhi, L. Harn, "Location-aware key management scheme for wireless sensor networks," Proc. of ACM Workshop Security of Ad Hoc and Sensor Networks, 2004.

[13] A. Durresi, V. Bulusu, V. Paruchuri, L. Barolli, "SCON: Secure management of continuity in sensor networks," Computer Communications 29, 2458-2468, 2006.

[14] Seyit A. Camtepe, Bulent Yene, "Key Distribution Mechanism for Wireless Sensor Networks : a Survey," TR-05-07 Rensselaer Polytechnic Institute, Computer Science Department, March, 2005.

[15] S. Zhu, S. Setia, S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," Proc. of the 10th ACM Conf. on Computer and Communications Security (CCS'03), pp.62-72, 2003.

[16] M. Wen, Y. Zheng, W. Ye, Ke. Chen, W. Qui, "A key management protocol with robust continuity for sensor networks," Computer Standards & Interfaces 31 642-647, 2009.



### 도 인 실

e-mail : isdoh@ewhain.net

1993년 이화여자대학교 전자계산학과(학사)

1995년 이화여자대학교 전자계산학과(석사)

1995년~1998년 삼성SDS

2001년~2007년 이화여자대학교 컴퓨터공학과(박사)

2007년~2008년 서울대학교 박사후연구원

2008년~현 재 이화여자대학교 컴퓨터공학과 연구교수

관심분야 : 네트워크 보안, 인터넷/무선통신망/고속통신망/센서네트워크/홈네트워크 보안

**채 기 준**

e-mail : kjchae@ewha.ac.kr

1982년 연세대학교 수학과(학사)

1984년 미국 Syracuse University 컴퓨터학과(석사)

1990년 미국 NorthCarolina State University 컴퓨터공학과(박사)

1990년~1992년 미국 해군사관학교 컴퓨터학과 조교수

1992년~현 재 이화여자대학교 컴퓨터공학과 교수

관심분야 : 네트워크 보안, 인터넷/무선통신망/고속통신망/센서네트워크(보안) 프로토콜 설계 및 성능분석