# 무선 센서 네트워크를 위한 효율적인 키 분배 기법

김회복* · 김형진**

*군산대학교 · **전북대학교

# An Efficient Key distribution Scheme for Wireless Sensor Networks

Hoi-bok Kim* · Hyoung-Jin Kim**

*Kunsan National University

**Chonbuk National University

E-mail : kim@chonbuk.ac.kr

## 요 약

무선 센서 네트워크는 저가의 한정된 자원들을 갖는 수많은 센서 노드들로 구성된다. 보편적으로 대부분의 센서들은 안전하지 않거나 제어할 수 없는 환경에 배치되며, 만일 넓은 목표 지역에 센서 노드들을 무작위로 배치할 때에는 센서 노드들의 정확한 위치를 파악하기 매우 어렵다.

따라서 본 논문에서는 이러한 문제를 해결하기 위한 방안으로서 효율적인 키 분배 기법을 제안하고자 한다. 이에 제안된 기법을 통해 센서 노드들이 선-분배된 키들을 사용하여 안전한 링크를 확립한 후 근접한 이웃 노드들과 서로 정보를 교환할 수 있도록 하였다. 또한 제안된 기법에서는 센서 노드의 위치 정보를 이용함으로써 노드 간에 공통-키를 발견할 수 있는 확률을 높일 수 있게 하였다.

## 키워드

무선 센서 네트워크, 키 분배

## Ⅰ. 서 론

무선 센서 네트워크는 신뢰성 있는 정보를 제공하고 개인의 사생활을 보호해 주어야 한다. 그런데 이런 신뢰성과 개인의 사생활 보호에는 많은 문제점을 안고 있다.

첫째, 센서 노드 사이의 통신이 무선의 특성을 가지고 있다. 둘째, 센서 노드들의 자원이 제한적이다. 셋째, 아주 광범위하고 밀집되어 센서 네트워크가 배치된다. 넷째, 고정된 인프라스트럭처가 결여되어 있다. 다섯째, 배치 이전에 네트워크 토폴로지를 알 수가 없다. 여섯째, 네트워크에 속하지 않은 센서들의 물리적인 공격들에 대해 높은 위험성을 갖는다.

이에 대한 해결책으로 효율적인 키 분배 기법이 있다. 따라서 본 논문에서는 무선 센서 네트워크을 위한 효율적인 키 분배 기법을 제한 하고자 한다.

논문의 구성은 다음과 같다. 2장에서는 관련연구에 대해 언급하고, 3장에서는 제안된 기법을 설계하고 4장에서 본 논문의 결론을 맺는다.

## Ⅱ. 기본 키 분배 기법

키 분배 기법의 기본 동작은 크게 3단계로 이

* 군산대학교 전자정보공학부

** 전북대학교 응용시스템 공학부(교신저자)

루어진다. 키 선-분배, 공통-키 발견, 경로-키 확립의 3가지 단계이다. 각각에 대해 알아보면 다음과 같다.

키 선-분배 단계는 어떤 2개의 노드들이 선택된 확률로 최소한 하나의 키를 공유하는 것을 보장하기위해(예 : 10,000 키들을 포함한 키-풀에서 선택한 단 75 키들이 어떤 key ring에 저장될 필요가 있다.) 단지 적은 수의 키들이 각 센서 노드의 key ring에 배치될 필요가 있다는 것을 보장한다. 그림 에서와 같인 키-풀 S로부터 임의로 m개의 키들을 선택하여 각각의 센서 노드내의 key ring에 저장한다.

공통-키 발견 단계는 WSN의 라우팅 계층에 의해 보이는 것처럼 센서 배열의 토폴로지를 확립한다. 2개의 센서 노드들이 키를 공유한다면 노드들 사이에는 링크가 존재하고 이 링크상의 모든 통신은 링크 암호화에 의해 안전하게 된다. 같은 키가 한 쌍이상의 센서 노드들에 의해 공유되는 것이 가능하다. 왜냐하면 key ring은 같은 키-풀로부터 임의로 선택된 키들을 포함하기 때문이다. 따라서 각각의 센서 노드가 m개의 키들을 저장하고 있을 때, 센서 노드 간에 하나의 공통-키를 발견하여 안전한 링크를 확립한다.

경로-키 확립 단계는 무선통신 범위 내에 키를 공유하는 않지만 공통-키 발견 단계 후에 2개 혹은 더 많은 링크들에 의해 연결되는 선택된 쌍들의 센서 노드들에 경로-키를 할당한다. 경로-키들은 센서 노드들에 의해 발생되지 않을 필요가 있다. 공통-키 발견 단계가 끝난 후에, key ring상의 많은 키들은 어떤 링크에 사용되지 않고 남겨진다. 따라서 센서 노드는 안전한 경로를 통해 다른 노드와 경로-키를 확립한다.

## Ⅲ. 키 분배 기법

본 논문에서 제안하고자 하는 키 분배 기법의 목표는 센서 노드들이 배치 후에 각각의 이웃 노드들과 공통적인 비밀 키를 찾도록 하는 것이다. 따라서 본 논문의 기법은 크게 4단계로 설계하였다.

### 3.1 초기화 단계

이 단계는 센서 노드들이 배치되기 전에 오프라인으로 수행된다. 제일 먼저 키-풀 S를 그림 1과 같이 m x n 개의 서브 키-풀 $S_{i,j}$(i=1, ..., m and j=1, ..., n)로 나눈다. 서브 키-풀 $S_{i,j}$의 크기는 $|S_c|$라 한다. 나눠진 $S_{i,j}$에 대해 각각이 배치 그룹 $G_{i,j}$에 대응된다. 만일 배치 그룹들이 인접한 위치에 배치된다면 대응되는 서브 키-풀 $S_{i,j}$이 서로 이웃으로 정의한다. 키-풀 S를 서브 키-풀 $S_{i,j}$로 나누는 것은 근접한 키-풀이 더 많은 키를 공유하도록 하고 서로 멀리 떨어져있는 키-풀은 더 적은 키를 공유하거나 공유하는 키가 전혀 없도록 하기 위해서이다.

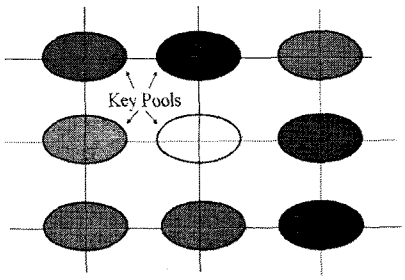


그림 1. 서브 키-풀

수직이나 수평으로 이웃하는 두 개의 키-풀은 정확히 $a|S_c|$ 키($0 \le a \le 0.25$)를 공유한다. 대각선으로 이웃하는 두 개의 키-풀은 정확히 $b|S_c|$ 키($0 \le b \le 0.25$)를 공유한다. 서로 이웃하지 않는 두 개의 키-풀은 어떤 키도 공유하지 않는다. 그림 2에서 이것을 보이고 있다.

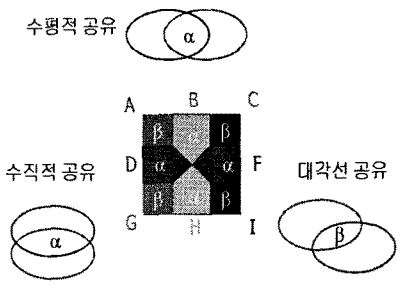


그림 2. 서브 키-풀 사이의 키 공유

키-풀 $|S|$과 중복 인자 a, b가 주어지면 다음 식에 의해 $|S_c|$이 계산됨으로서 서브 키-풀의 크기가 결정된다.

$$|S_c| = \frac{|S|}{tn-(2n-t-n)a-2(tn-t-n+1)b} \quad (1)$$

키-풀 S가 서브 키-풀 $S_{i,j}$로 나눠진 후 배치 그룹 $G_{i,j}$내에 각각의 센서 노드에 대해, 대응되는 서브 키-풀 $S_{i,j}$로부터 n개의 키를 임의로 선택한 후 노드의 메모리로 로드한다.

### 3.2 그룹 기반 배치 모델

센서 노드들은 일반적으로 비행기나 기타 운송 장비를 통해 타깃 지역에 배치될 수 있고 배치된 센서 노드들은 서로 간에 안전한 채널을 확립할 수 있다.

센서 노드들은 일단 배치가 되면 움직임이 없는 상태라고 가정한다. 그룹기반 배치를 가정하고

다음처럼 배치 정보를 가정한다.

1) 배치되는 N개의 센서 노드들은 m x n 개의 동등한 크기의 그룹들로 나뉜다. 각각의 그룹 $G_{i,j}$[i=1, ..., m and j=1, ..., n]은 인덱스(i,j)를 갖는 배치 지점에 배치된다. $(x_i, y_j)$를 배치 그룹 $G_{i,j}$에 대한 배치 지점을 나타내도록 한다.

2) 배치 지점들이 그리드 내에 정렬된다.

3) 배치 동작 중에, 그룹 내의 센서 노드 k의 배치 지점은 표준 분포 함수 $f(x,y|k\in G_{i,j})$를 따른다. 표준 분포 함수의 예는 2차 가우시안 분포이다.

배치 그룹 내의 어떤 센서 노드 k에 대한 배치 분포는 다음의 2차 가우시안 분포를 따른다고 가정한다. 그룹 내의 배치 지점이 일 때, 그룹 내의 센서 노드 k에 대한 표준 분포 함수가 다음 공식 (2)과 같다.

$$f(x,y|k\in G_{i,j}) = \frac{1}{2\pi\sigma^2} e^{-[(x-x_i)^2+(y-y_j)^2]/2\sigma^2} \qquad (2)$$

비록 각각의 단일 그룹에 대한 배치 함수가 비-정규이더라도, 센서 노드들이 전체 영역에 동등하게 배치된다고 가정한다. 각각의 배치 그룹의 표준 분포 함수의 $\sigma$의 값과 관련해서 근접한 배치 지점들 사이의 적절한 거리를 선택함으로서, 각각의 작은 영역에서 센서 노드를 찾을 확률이 대략적으로 동등할 수 있다.

### 3.3 공통-키 설정 단계

기본 기법에서, 어떤 두 이웃노드들은 키-설정 단계에서 안전한 링크를 확립하기위해 key rings로부터 단일 공통-키를 찾을 필요가 있다. 이 단계에서는 기본 기법에서의 단 하나의 공통-키 대신에 q개의 공통-키들이(q > 1) 필요하다.

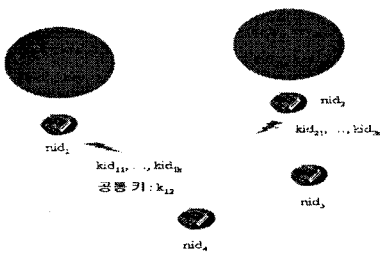


그림 3. 공통-키 설정

키-설정 단계에서, 그림 3과 같이 각각의 센서 노드는 이웃노드들 각각과 지니는 모든 공통-키들을 발견해야 한다. 이것은 한 노드가 지니는 모든 키 식별자들의 단순한 로컬 브로드캐스트로 달성될 수 있다.

키 발견 후에, 각각의 노드는 최소한 q 키들을 공유하는 모든 이웃 노드를 확인할 수 있다. 공유되는 실제 키들의 수를 q'라 하자, q' ≥ q.

키들은 오리지널 키-풀 S내에서 발생한 순서를 기반으로 형식 순서로 hash 된다. 키-설정은 q 키들보다 더 적게 공유하는 노드들 사이에는 수행되지 않는다. 새로운 통신 링크 키 K가 모든 공통-키들의 hash로서 발생된다.

$K = hash(k_1||k_2||...||k_q)$

#### 3.3.1 key ring과 key pool 크기의 계산

중요한 파라미터인 키-풀의 크기 |S|를 계산할 필요가 있다. 만일 키-풀의 크기가 너무 크다면, 어떤 두 개의 센서 노드들이 최소한 q 키를 공유할 확률은 p보다 낮게 되고 네트워크는 연결되지 않을 수 있다. 만일 키-풀의 크기가 너무 작다면, 쓸데없이 보안성을 희생하게 된다. 어떤 두 개의 센서 노드들이 최소한 q 키를 공유할 확률이 ≥ p가 되는 만큼의 키-풀의 크기를 선택하고자 한다. 어떤 센서 노드가 key ring내에 지닐 수 있는 키들의 수를 m이라 가정한다. S로부터 크기 m인 두 개의 랜덤 샘플들이 최소 p의 확률로 공통으로 최소한 q개의 키를 가지기 위해 가장 큰 S를 찾고자 한다. |S|를 다음처럼 계산한다. 어떤 두 개의 센서 노드들이 공통으로 정확히 i 키를 가질 확률을 p(i)라 가정한다. 어떤 한 센서 노드는 크기 |S|인 키-풀로부터 m 키를 선택하는 $\binom{|S|}{m}$의 다른 방법들을 가진다. 따라서, 두 센서 노드들이 각각에 대해 m 키를 선택하는 방법의 총 수는 $\binom{|S|}{m}^2$이다. 두 개의 센서 노드들이 공통으로 i 키를 가짐을 가정한다. i개의 공통-키들을 선택하는 $\binom{|S|}{m}$의 방법들이 있다. i 공통-키들이 선택된 후에, |S|-i 키들의 남아있는 키-풀로부터 선택되어야하는 두 개의 key ring내에는 2(m-i)의 서로 다른 키들이 남아있다. 이 남아있는 키-풀로부터 키들을 선택하는 방법들의 수는 $\binom{|S|-i}{2(m-i)}$이다. 2(m-i)의 서로 다른 키들은 두 개의 센서 노드들 사이에 동등하게 나뉘어져야 한다. 그러한 동등한 부분들의 개수는 $\binom{2(m-i)}{m-i}$이다. 따라서, 공통으로 i 키들을 지니는 두 개의 key ring을 선택하는 방법의 총 수는 $\binom{|S|}{i}\binom{|S|-i}{2(m-i)}\binom{2(m-i)}{m-i}$이다.

따라서, 어떤 두 개의 센서 노드들이 공통으로 정확히 i 키를 가질 확률이다음 식 (3)에 의해 계산된다.

$$p(i) = \frac{\binom{|S|}{i}\binom{|S|-i}{2(m-i)}\binom{2(m-i)}{m-i}}{\binom{|S|}{m}} \qquad (3)$$

어떤 두 개의 센서 노드들이 안전한 통신을 형성하기위해 충분한 키들을 공유할 확률을 $p_{connect}$라 가정한다. $p_{connect}$ = 1-(두 개의 센서 노드들이 연결을 형성하기 위해 불충분한 키들을 공유

할 확률)

$$p_{connect} = 1 - (p(0) + p(1) + \ldots + p(q-1)) \quad (4)$$

크기가 m인 key ring, 최소의 key overlap q, 최소의 연결 확률 p 에 대해, $p_{connect} \geq p$ 만큼의 가장 큰 |S|를 선택할 수 있다.

### 3.4 경로-키 확립 단계

두 개의 이웃 노드들은 어떤 공통-키를 노드들 사이에 찾을 수 없을 수도 있다. 이 경우에, 그림 4와 같이 이웃 노드들 간에 공통-키를 합의하기위한 안전한 방법을 찾을 필요가 있다. 공통-키를 공유하지 않는 두 개의 이웃 노드들 i와 j가 어떻게 비밀 키를 구성하는 지를 보인다. 아이디어는 key-space sharing graph GKS내에 이미 확립된 안전한 채널들을 이용하는 것이다. 그래프가 연결되는 만큼, 두 개의 이웃 노드들 i와 j는 GKS내에서 i에서 j로의 경로를 항상 찾을 수 있다. i, $v_1$, ... , $v_h$, j 로의 경로를 가정한다. i와 j 사이에 공통-키를 찾기 위해, i는 랜덤 키 K를 먼저 발생시킨다. 그리고 i는 키를 i와 $v_1$사이의 안전한 링크를 사용해서 $v_1$에 보낸다. $v_1$은 키를 $v_1$과 $v_2$사이의 안전한 링크를 사용해서 $v_2$에 보낸다. j가 로부터 키를 받을 때까지 계속 보내진다. 센서 노드들 i와 j는 이 비밀 키 K를 노드들의 pairwise 키로서 사용한다. 키는 항상 안전한 링크를 통해 보내지므로, 이 키를 알아낼 수 있는 노드들은 이 링크 상에만 존재한다. 센서 노드들 i와 j에 대한 안전한 경로를 찾기 위해, 가장 쉬운 방법은 멀티-홉 무선 네트워크에서 일반적으로 사용되는 기법인 flooding[7]을 사용하는 것이다. i와 j 사이에 3-홉 내에 안전한 경로가 있을 확률은 아주 높다(1에 가깝게). 그러므로 flooding 오버헤드를 줄이기 위해 flooding 메시지의 수명을 3-홉으로 항상 제한할 수 있다.

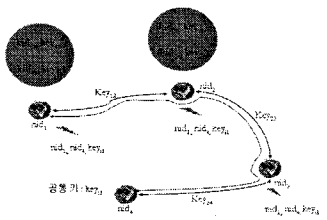

그림 4. 경로-키 확립

## Ⅳ. 결론

본 논문에서는 무선 센서 네트워크에서 정보 보안 서비스 제공을 위한 키 관리 방법으로서 효율적인 키 분배 기법을 제안하였다. 센서 네트워크에서는 센서 노드들이 안전하지 않은 지역에 배치되고 센서 노드에 다시 접근하는 것이 쉽지 않아 공격자에 의해 센서 노드들이 물리적인 공격에 노출될 수 있다. 최악의 경우에는 들키지 않고 센서 노드의 제어권이 공격자에게 넘어가서 보안을 위해 필요한 비밀 암호-키들이 손상될 수 있다.

본 논문에서는 이를 위해 제안된 기법을 통해 센서 노드 간에 키를 확립하는 방법을 제안하여 공격자가 센서 노드의 제어권을 쉽게 얻을 수 없도록 하여 센서 노드 간에 키 확립이 안전하게 이루어지게 되어 안전한 링크를 통해 데이터가 송수신될 수 있도록 가능해진다.

또한 제안된 기법에서는 센서 노드의 위치 정보를 이용함으로서 정보를 교환하는 센서 노드 간에 공통-키를 발견할 수 있는 확률을 높일 수 있도록 하였다.

향후 성능 평가를 통해 기존의 키 분배 기법에 비해 본 논문에 제안된 기법이 연결성과 복원력에 관해 성능이 개선됨을 보이고자 한다.

## 참 고 문 헌


[1] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM conference on Computer and communications security, pp. 41-47, 2002.

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

[3] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen and Pramod Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge,", Proceedings of the IEEE INFOCOM' 04, pp.586-597, 2004.

[4] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in Proceedings of the 10th ACM Conference on CCS, pp. 52-61, October 27, 2003.

[5] S. A. Camtepe, B. Yener, "Key Distribution Mechanisms for Wireless Sensor Networks : a Survey," Technical Report TR-05-07, March 23, 2005.

[6] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security(CCS), pp. 42-51, October 27-31, 2003.

[7] C. E. Perkins, Ed., Ad Hoc Networking. Addison-Wesley, 2001.