센서 네트워크에서의 쿼럼 시스템을 이용한 키 사전 분배

(Key Pre-distribution using the Quorum System in Wireless Sensor Networks)

강 지 명 † 이 성 렬 † 조 성 호 † 김 종 권 †† 안 정 철 †††
(Jimyung Kang) (Sungryeoll Lee) (Seongho Cho) (Chong-kwon Kim) (Joung-Chul Ahn)

요 약 센서 네트워크는 침입탐지, 원격 감시 등 보안이 꼭 필요한 환경에서 사용될 것으로 예상된다. 이와 같은 센서네트워크에서 기밀성과 같은 보안성을 제공하기 위해서 센서 노드들은 공유키를 가지고 있어야 한다. 현재까지 제안된 기본적인 키 분배 기법은 키가 너무 많이 필요하거나, 노출된 센서에 의해서 키가 너무 많이 노출되는 등 보안 측면에서 취약했다. 이와 같은 문제를 해결하기 위하여 확률적 키 분배 기법이라는 적은 수의 키로 노드 간의 키 공유를 확률적으로 보장하는 새로운 키 분배 기법이 제안되었다. 그러나 이 기법은 노드 간에 키의 공유가 항상 보장되지 않기 때문에 물리적인 이웃 노드라도 통신을 진행하지 못하게 되어 비효율적인 라우팅이 발생하거나, 별도의 라우팅 프로토콜을 필요로 하는 문제가 있다. 본 논문에서는 쿼럼 시스템(quorum system)을 이용하여, 노드에서 필요로 하는 키의 수를 줄이면서도 이웃 노드와 키 공유를 언제나 보장하는 새로운 키 분배 방법을 제안한다. 또한 노드 분포 정보(deployment knowledge)를 아는 상황에서 쿼럼 시스템을 확장하여 센서 노드에서 필요로 하는 키의 수를 줄이고 보안성과 연결성을 지원할 수 있는 방안을 제시한다.

키워드 : 센서 네트워크, 보안, 공유 키 분배, 쿼럼 시스템, 노드 분포 정보기반 키 분배

Abstract The security feature is essential in wireless sensor network such as intrusion detection or obstacle observation. Sensor nodes must have shared secret between nodes to support security such as privacy. Many methods which provide key pre-distribution need too many keys or support poor security. To solve this problem, probabilistic key pre-distribution is proposed. This method needs a few keys and use probabilistic method to share keys. However, this method does not guarantee key sharing between nodes, and neighbor nodes may not communicate each other. It leads to waste of network resource such as inefficient routing, extra routing protocol. In this paper, we propose new key distribution method using quorum system which needs a few keys and guarantee key sharing between nodes. We also propose extension of the method which needs fewer keys and guarantee key sharing when node deployment knowledge is well known.

Key words : Wireless sensor network, Security, Symmetric key pre-distribution, Quorum system, Key pre-distribution using deployment knowledge

1. 서 론

센서네트워크는 필요한 지역에 뿌려진 센서 노드들의 집합이 상호간 통신을 통해서 수집한 정보를 필요한 곳에 전달하는 네트워크를 말한다. 센서의 가격이 저렴해지고 통신 프로토콜이 발전함에 따라서 실제로 여러 분야에서 센서네트워크가 실용화 될 것으로 예측된다. 이러한 센서네트워크가 일반적으로 쓰일 것이라고 생각되는 용도, 즉 적진의 동태를 살피거나 침입자를 탐지하는 등의 응용에는 통신 보안이 꼭 필요하다.

네트워크에서 보안을 지원하기 위해서는 키 분배가

· 본 연구는 국가보안연구소 및 한국과학재단 목적기초연구(R01-200400010-37202005)지원으로 수행되었음
† 학생회원 : 서울대학교 전기.컴퓨터공학부
jmkang@popeye.snu.ac.kr
srlee@popeye.snu.ac.kr
shcho@popeye.snu.ac.kr
†† 종신회원 : 서울대학교 전기.컴퓨터공학부 교수
ckim@popeye.snu.ac.kr
††† 정 회 원 : 국가보안기술연구소 보안기술팀 팀장
jcahn@etri.re.kr
논문접수 : 2005년 11월 10일
심사완료 : 2006년 3월 23일

선행되어야 한다. 모든 보안 프로토콜은 키를 가지고 서로를 인증하고, 데이타를 암호화하기 때문이다. 현재 인터넷에서는 공개키(Public Key)방식이 많이 사용되고 있다. 공개키 방식에서의 키는 공개키(Public Key)와 비밀키(Private Key)의 한 쌍으로 구성되는데, 공개키로 암호화된 것은 비밀키를 가지고 있는 노드만 해독할 수 있다. 이 방식은 지수적인 방법으로 디자인 되어서 아주 강력한 보안성을 제공하지만, 그 알고리즘이 까다로워서 컴퓨팅 파워를 아주 많이 필요로 한다. 그런데 센서 네트워크는 작고 계산 성능이 좋지 않은 센서들로 구성되기 때문에, 공개키 방식의 키 분배는 적용하기 어렵다[1]. 그러므로 센서 네트워크에서는 공유키를 센서 노드에 미리 분배 해둔 뒤, 이 키를 토대로 해서 통신을 진행하여야 한다.

가장 간단하게 센서 노드에게 키를 분배하는 방법은 모든 센서 노드에게 하나의 공유키(symmetric key)를 분배하는 것이다. 하나의 키를 사용하기 때문에 간편하며 노드가 유지해야 하는 정보도 많지 않다. 하지만 하나의 센서 노드가 노출되면 공유키가 알려질 수 있는 문제가 있다. 반대로 또 생각해 볼 수 있는 방법은 각각의 센서 쌍 마다 다른 키를 할당하는 것이다. 이렇게 하게 되면 노드 하나가 노출 되더라도 다른 노드끼리 통신하는 키는 전혀 노출되지 않기 때문에 전체 네트워크가 공격에 노출 되는 것을 막을 수 있다. 그러나 이런 방법들은 보안측면에서 너무 약하거나, 센서 노드들이 가지고 있어야 하는 키의 양이 너무 많다.

센서 네트워크에서는 센서 네트워크의 특성에 잘 맞게 특화된 키 관리 기법을 사용해야 한다. 논문에서는 쿼럼 시스템을 이용해 이웃 노드와의 키 공유를 보장하는 새로운 기법을 제시하고자 한다. 쿼럼 시스템을 통해서 하나의 센서 노드가 가지고 있어야 하는 키의 양을 제한하면서 동시에 보안성은 유지할 수 있는 방법을 제시한다. 특히 모든 센서 쌍이 항상 공유키를 갖도록 보장하여 데이타 수집을 위해서 사용되는 라우팅 프로토콜의 별도의 수정을 하지 않아도 되는 장점이 있다. 그리고 주변 노드의 밀도와 무관하게 언제나 노드 간에 공유키를 갖고 있기 때문에 네트워크의 연결성(connectivity)가 보장되는 장점이 있다. 또한 논문에서는 일반적으로 센서 노드가 이동성이 적은 센서 네트워크의 특성을 고려하여 노드 분포정보를 이용하여 필요로 하는 키의 양을 줄일 수 있는 방법을 추가적으로 제시한다.

논문의 2장에서는 센서에서의 키 분배에 관련된 기존 연구를 소개하고, 3장에서는 쿼럼 시스템(Quorum system)을 설명한 뒤, 이를 이용한 키 분배 방법과 추가로 노드 분포정보까지 이용한 키 분배 방법을 제안한다. 4장에서는 제안된 방안의 성능을 분석하고 5장에서 결론을 맺는다.

2. 관련 연구

센서네트워크에서의 키 분배 방안으로 SPINS[1], LEAP[2]이 제안되었다. SPINS는 상호인증된 제 3자(trusted third party)가 존재한다고 가정한 뒤 통신을 통해서 키를 셋업하고, LEAP은 키를 셋업하는 초기에는 센서가 노출되지 않는다고 가정한다. 그러나 이런 방안들은 공격적인 환경에 노출된 센서네트워크를 생각해 볼 때 그 가정이 적절하지 못하다.

이런 점을 생각 해 볼 때 센서네트워크에서 사용할 수 있는 적절한 방안은 키의 선 분배(Key pre-distribution)라고 생각된다[3]. 센서 노드에 키분배를 위해 많은 통신을 유발시키지 않고, 컴퓨팅 파워를 많이 소비하지 않기 위해서는 미리 키를 나눠 주고 그 키로 통신을 진행하여야 하는 것이다. 이에 따라 센서 노드 간에 키 공유를 통해 주변 노드와 통신을 가능하게 하면서 노드가 가지고 있어야 하는 키 정보의 양은 적게 만드는 것이 고려해야 할 중요한 대상이다. 앞으로 논문에서 키 분배는 키 선 분배(Key pre-distribution)만을 고려한다.

Laurent는 처음 키 선분배(Key pre-distribution)를 사용하였고 이 때 확률적 키 분배의 개념을 사용하였다[3]. 노드들에게 키를 나눠주기 위해 확률적 키 분배에서는 큰 키 풀(large size key pool)을 만들고, 각각의 센서 노드는 이렇게 만들어진 키 풀 중에서 일정량의 키를 랜덤(random)하게 골라서 가지게 된다. 일반적으로 두 노드가 통신을 하려면 노드 사이에 같은 키의 공유가 필수적이지만 이렇게 하면 임의의 두 노드 사이에 키의 공유가 일정 확률로 이루어지므로 항상 키의 공유가 보장되지 않는다. 즉 같은 키를 공유한 노드끼리는 통신이 가능하고, 그렇지 않은 노드는 비록 인접한 노드이더라도 통신을 바로 진행할 수가 없다. 두 노드가 확률적으로 키를 공유하도록 함으로써, 전체 네트워크가 같은 키를 사용하지 않도록 해서 보안적 측면을 유지하면서도 센서 노드가 가지고 있어야 하는 키의 개수를 적절히 유지할 수 있다는 장점이 있다.

그런데 확률적으로 키를 공유하더라도 전체 네트워크의 연결은 꼭 되어야 한다. 이를 위해서 랜덤 그래프 이론(random graph theory)[4]을 사용하여 전체 네트워크의 연결성(connectivity)를 일정확률로 보장할 수 있음을 증명하였다. 랜덤 그래프 이론을 통해서 랜덤 네트워크에서 전체 네트워크의 연결을 보장하기 위해서 필요한 평균 이웃 노드를 계산할 수 있다. 키 분배를 고려할 경우, 필요한 이웃 노드의 수는 키 공유가 이루어진 이웃 노드 수를 의미한다. 예를 들어 10,000개의 노드가

연결 되기 위해서는 랜덤 그래프 이론에 의해서 평균 이웃 노드가 20개가 있어야 한다. 그리고 실제 물리적인 이웃 노드가 40개라면 임의의 두 노드 사이에 키 공유 확률이 50%가 되어야 20개의 노드와 키 공유를 할 수 있다. 50%의 키 공유 확률을 위해서는 100,000개의 키 풀에서 263개의 키를 뽑으면 된다. 위의 예시와 같이 확률적 키 분배 방법은 실제로 매우 작은 키만 가지고도 높은 키 공유 확률을 제공해 좋은 성능을 보인다.

그러나 확률적 키 분배 방법에서는 노드가 얼마나 촘촘하게 배치되어 있는지, 즉 전송 범위 내에 몇 개의 노드를 찾을 수 있는지에 따라 가지고 있어야 하는 키의 개수가 달라지기 때문에 센서 노드의 분포 밀도를 미리 예측해서 계산을 통한 키의 분배가 이루어 져야 한다. 또한 이 방법에서는 모든 노드와의 키 공유가 보장되지 않기 때문에 실제로 물리적으로 이웃 노드라 하더라도 키 공유가 되지 않으면 그 노드와는 통신할 수 없는 단점이 존재한다. 그리고 키의 공유 확률이 너무 낮으면 전체 네트워크가 연결되지 않을 수도 있다. 키의 개수를 줄이면서도 보안성을 증가시키기 위해서 확률적 기법의 성능을 개선한 방법도 몇 가지 제시되었다[5-7]. 이웃노드와 q개의 키가 공유되면 키 공유로 인정하거나[5], Blom[8]의 키분배 방법을 이용해서 확률적 기법의 성능을 개선하였다[6]. 그러나 이런 방법은 근원적으로 모든 노드와 통신이 보장되지 않는 확률적 기법들의 문제를 해결해 주지는 못한다.

위의 방법은 센서 노드들이 연관성 없이 임의로 배치된다는 가정에서 이루어진 방법인데, 만약 센서 노드 들이 어떻게 배치되는지 알게 되면 훨씬 더 효율적인 방법으로 키를 분배 할 수 있게 된다. 즉, 주위에 있는 노드들을 미리 어느 정도 알 수 있다면 그 정보를 이용해 주변에 있는 노드와 키의 공유를 더 효율적으로 할 수 있다. 예를 들어, 비행기에서 어떤 특정지역에 센서들을 살포한다고 할 경우 센서들을 묶음 단위로 떨어뜨린다고 할 수 있다. 10,000개의 노드를 살포 할 경우 100개씩 묶어서 100번 떨어뜨린다고 하면, 100개 단위 내에서는 서로 인접해 있을 확률이 훨씬 높게 된다. 이런 가정하에 확률적 키 분배 기법을 더 발전시킬 수 있다[9]. 각각의 패키지가 살포되는 단위를 하나의 셀로 가정하고 각각의 셀 단위로 작은 크기의 키 풀을 독자적으로 만든다. 그리고 각 패키지 내의 센서 노드들은 해당하는 키 풀에서 임의로 일정량의 키를 선택한다. 키를 뽑는 키 풀의 크기가 작기 때문에 같은 패키지 내에 있는 센서 노드들은 적은 수의 키를 가지고도 같은 키를 공유하고 있을 확률이 높아지게 된다. 그러나 같은 패키지 내에서만 키 공유의 확률을 높이면, 전체 네트워크의 연결은 여전히 요원하게 된다. 그래서 인접한 셀의 패키지 간에 서로 키 풀을 공유하도록 해서, 셀 간에 키의 공유를 보장해 줄 필요가 있다. 그림 1에서 보듯이, 인접한 8개의 셀과 자신의 키 풀의 일정량씩을 공유하도록 한다. 상하 좌우로는 a 만큼 대각선으로는 b 만큼 키 풀을 공유하도록 하면 인접 셀의 노드들 간에도 키 공유의 확률이 높아지게 된다.

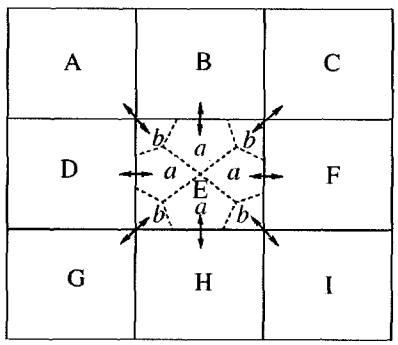

그림 1 인접 셀 사이의 키풀의 공유

이렇게 노드 분포 정보(deployment knowledge)를 이용하면 인접한 노드간에 키를 공유하게 될 확률은 기존 방법에 비해서 월등히 높아진다. 그러나 모든 노드와 키 공유가 보장되지 않고, 먼 길로 돌아서 통신을 해야 하거나 다른 키 셋 업 프로토콜이 필요하다는 단점은 여전히 존재한다.

3. 쿼럼 시스템에 기반을 둔 키 분배

센서 네트워크는 센서 노드가 공격적인 환경에 있을 확률이 높아서 키가 노출되기 싶고, 작은 컴퓨팅 파워를 가진 센서끼리 통신을 진행한다. 따라서 센서 네트워크에서의 키 분배는 아래와 같은 점들이 고려되어야 한다.

첫째, 일부의 센서 노드가 노출됨으로써(compromised) 전체 네트워크의 기밀성이 파괴되지 않아야 한다.

둘째, 센서 노드 하나가 가지고 있어야 하는 키의 양은 많지 않아야 한다.

셋째, 센서의 밀도와 무관하게 전체 네트워크의 연결성이 보장되어야 한다.

넷째, 컴퓨팅 파워나 에너지를 많이 사용하지 않아야 한다.

이러한 점들을 고려해 볼 때 2장에서 설명한 [3]과 이를 확장한 [4]의 키 분배 방법은 이러한 조건들을 어느정도 만족시키는 것처럼 보인다. 그러나 이러한 확률적 키 분배 방법에서는 임의의 두 노드 사이에 키 공유가 보장되지 않기 때문에 먼 길을 돌아서 통신을 진행하던지, 새로운 키 공유 프로토콜이 부가적으로 필요하게 된다. 그러나 가까운 길을 놓아두고 멀리 돌아가는

것은 아주 비효율적일 뿐만 아니라, 새로운 키를 생성하기 위한 새로운 프로토콜에 따르는 비용도 크다는 단점이 존재한다. 이러한 문제점을 해결하면서도 센서 네트워크의 키 분배를 원활히 하기 위해서 임의의 두 노드 사이에 키 공유가 항상 보장되는 쿼럼 시스템을 기반으로 한 키 분배를 제안한다.

3.1 쿼럼 시스템

쿼럼(Quorum)이라는 것은 두 집합의 교집합의 원소가 하나 이상 존재하는 것을 말한다. 즉, 임의의 두 집합을 가지고 교집합을 만들더라도 공집합이 되지 않는다. 이런 집합들의 모임을 쿼럼 시스템(Quorum system)이라고 한다. 예를 들어 {1,2,3}, {1,4,5}, {2,5,7}은 쿼럼 시스템이라고 할 수 있다. 왜냐하면 {1,2,3}∩{1,4,5} = {1}, {1,2,3}∩{2,5,7} = {2}, {1,4,5}∩{2,5,7} = {5}이기 때문에 어떤 집합끼리 교집합 하여도 겹치는 원소는 있게 된다. 그러나 {1,2,3}, {1,4,5}, {2,6,7}은 {1,4,5}와 {2,6,7}의 교집합이 공집합이기 때문에, 쿼럼 시스템이 아니다.

쿼럼 시스템을 만드는 방법은 여러 가지가 있지만, 대표적으로 아래와 같은 세 가지 방법들을 들 수 있다.

① 그리드(Grid) 쿼럼 시스템

그리드 쿼럼 시스템에서 원소들은 2차원 평면 상에 줄지어서 위치해 있다. 쿼럼 시스템을 구성하기 위해서 각각의 집합은 그림 2와 같이 행과 열을 각각 하나씩 고른다. 선택한 행에 속한 원소들과, 선택한 열에 속한 원소들을 합쳐서 자기의 원소로 정한다. 이렇게 각각의 집합을 일정한 규칙에 따라서 임의로 정하면 이 시스템 내에서 임의의 집합 두 개를 선택 하더라도 서로 겹치는 부분이 최소 2개 이상 나오는 것을 확인할 수 있다.

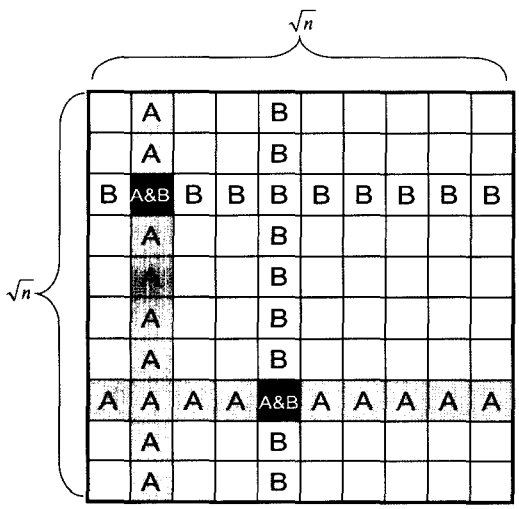

그림 2 그리드 쿼럼 시스템

이 쿼럼 시스템은 전체 원소 n개 중에서 $2\sqrt{n}-1$개의 원소를 뽑음으로 2개 이상의 공통원소를 보장 할 수 있다.

② 토러스(Torus) 쿼럼 시스템

토러스 쿼럼 시스템에서 원소들은 가로가 2배 더 긴 직사각형 상에 위치해 있다. 각각의 집합은 그림 3과 같이 한 열을 선택하고, 그 열에서 오른 쪽으로 한 열씩 이동하면서 임의의 행에서 한 원소를 선택한다. 이 작업은 가로 길이의 절반을 이동할 동안 진행 된다. 그림 3처럼 선택을 다 하고 나면 임의의 두 집합 사이에서 적어도 하나의 공통 원소가 있다는 사실을 알 수 있다.

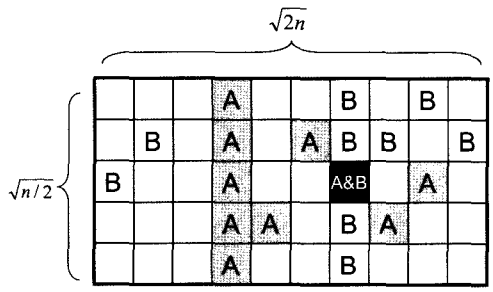

그림 3 토러스 쿼럼 시스템

이 쿼럼 시스템은 n개의 원소에서 $2\sqrt{n}-1$개의 원소를 뽑음으로 1개 이상의 공통 원소를 보장 할 수 있다. 그리드 쿼럼 시스템보다 더 작은 원소를 뽑아도 공통원소를 보장 할 수 있게 된다.

③ 사이클릭(cyclic) 쿼럼 시스템

사이클릭 쿼럼 시스템은 difference set으로부터 출발한다. Difference set $D=\{d_1,d_2,\cdots,d_k\}$라는 것은 $Z_n\{0,1,2,\cdots,n-1\}$ 공간에서 D의 원소들의 차이를 이용해, Z_n의 모든 원소를 만들어 낼 수 있는 집합을 말한다. 즉 $Z_8=\{0,1,2,3,4,5,6,7\}$에서 $D=\{0,1,2,4\}$이다. 왜냐하면 D의 집합 내에 원소 두 개의 차이에 mod 8을 함으로써 0에서 7까지의 모든 원소를 만들어 낼 수 있기 때문이다. 즉

(0-0)mod 8=0
(1-0)mod 8=1
(2-0)mod 8=2
(4-1)mod 8=3
(4-0)mod 8=4
(1-4)mod 8=5
(0-2)mod 8=6
(0-1)mod 8=7

이기 때문에 $D=\{0,1,2,4\}$는 Z_8에서 Difference Set이다. Z_n 공간에서 Difference Set $D=\{d_1, d_2, \cdots, d_k\}$일 때 사

이클릭 쿼럼 시스템 Q는 아래와 같이 이루어 진다.

사이클릭 쿼럼 시스템 $Q=\{G_1, G_2, ..., G_n\}$,

where $Gi = \{d_1 + i, d_2 + i, ..., d_n + i\}$

(mod n), i = 0, ..., n-1

즉 위에서 제시한 예제에서, Z={0,1,2,3,4,5,6,7}이고 D={0,1,2,4}일 때 쿼럼 시스템은 아래와 같은 집합으로 이루어진다.

쿼럼 시스템 Q = {{0,1,2,4}, {1,2,3,5}, {2,3,4,6}, {3,4,5,7}, {4,5,6,8}, {5,6,7,1}, {6,7,1,3}, {7,1,2,4}}

위에 있는 집합 중에서 임의의 두 집합의 교집합은 공집합이 아니고, 위와 같은 조건을 만족하는 difference set을 이용해 만든 사이클릭 쿼럼 시스템은 n개의 원소에서 약 $\sqrt{n}$개의 원소들을 뽑아 가지게 되고 한 개의 공통원소를 보장한다.

3.2 쿼럼 시스템을 기반으로 한 키 분배

위와 같은 쿼럼 시스템을 센서 네트워크에서의 키 분배에 적용시킬 수 있다. 이러한 쿼럼 시스템은 분산 시스템에서 널리 이용되어 왔고[10-13], 최근에는 네트워크의 에너지 절약 모드에서 동기화를 맞추기 위해 사용되었다[14]. 즉 기존방법인 확률적 키 분배 방법에서의 전체 키 풀을 쿼럼 시스템이 되게 하고, 센서가 키들을 선택할 때 쿼럼 시스템에서의 규칙에 맞게 선택하는 것이다. 예를 들어 그리드 쿼럼 시스템을 적용시키면, 그림 2에서의 모든 원소가 키 풀이 되고, 가로 세로에서 한 줄의 키를 선택하는 것이다. 모든 센서 노드가 이런 규칙에 따라 키를 뽑게 되면 어떤 임의의 두 노드 사이에서도 키의 공유가 보장되게 된다. 즉 쿼럼 시스템의 특성상 센서 노드는 모든 노드들과 키를 공유하는 것이 보장되고, 확률적 기법에서의 이웃 노드와의 연결 확률이 낮은 문제점을 해결할 수 있게 된다.

3.3 노드 분포 정보를 이용한 키 분배

센서를 뿌릴 때 어느 노드들이 어느 지역에 뿌려질지를 아는 노드 분포 정보를 가정할 수 있다[9]. 똑 같은 가정을 본 논문에서 제안한 쿼럼 시스템을 이용한 방식에도 적용시킬 수 있다. 셀을 나눠서 시스템을 구성하게 되면 쿼럼 시스템을 셀 단위로 작게 구성할 수 있다. 같은 셀에 속한 노드끼리 이웃이 될 확률이 매우 크기 때문이다. 그러나 이웃 셀의 노드와도 키의 공유가 보장되어야 하기 때문에 셀 단위로 독자적으로 쿼럼 시스템을 만들 수는 없다.

쿼럼 시스템을 이용한 키 분배에서 k^2개의 셀로 구성되는 노드 분포 정보를 안다고 가정하자. 그림 4와 같이 먼저 작고 독립적인 쿼럼 시스템을 $(k+1)^2$개 만든다(A, B, C…). 그 후 이 쿼럼 시스템들의 교차지점에 실제 센서가 뿌려진 셀들을 위치시킨다(1, 2, 3,…). 이렇게 하면 각각의 셀들은 4개의 쿼럼 시스템과 만나게 된다. 각각

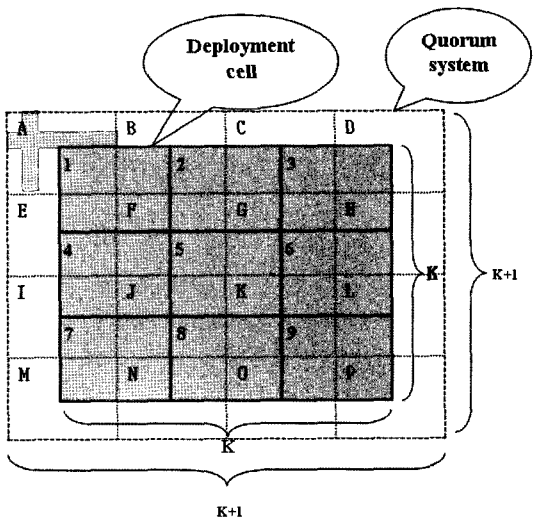

그림 4 노드 분포정보를 이용한 쿼럼 기반 기법의 키분배

의 셀은 자신이 만나는 이 4개의 쿼럼 시스템에 모두 속하게 되고, 정해진 방식에 따라 쿼럼 시스템에서 키를 뽑는다. 즉 1번 셀은 A, B, E, F 4개의 쿼럼 시스템에서 키를 뽑고, 2번 셀은 B, C, F, G 4개의 쿼럼 시스템에서 키를 뽑는다. 각각의 셀들은 4개의 쿼럼 시스템에 속해 있기 때문에, 이웃한 셀과는 적어도 같은 쿼럼 시스템을 1개 이상 공유하게 된다. 그리고 쿼럼 시스템은 키의 공유를 보장해주기 때문에 센서노드는 이웃노드와 키의 공유가 보장되게 된다. 이렇게 노드 분포 정보를 알 수 있는 경우에는 센서 노드 하나가 가져야 하는 키의 개수를 현격히 줄일 수 있다.

물론 이 방법에서 만약 센서 노드가 자기 셀에서 멀리 떠나서 다른 셀에 떨어지게 되면 이 노드는 통신을 할 수가 없다. 그러나 이런 경우는 거의 일어나지 않는다고 볼 수 있으므로, 고려하지 않아도 좋다.

4. 성능 평가

쿼럼 시스템을 기반으로 한 키 분배 방법의 가장 큰 장점은 임의의 두 노드 간에 키의 공유가 항상 보장된다는 것이다. 즉, 키 공유가 안된 노드끼리의 키 셋 업을 위한 추가적인 프로토콜이 필요가 없고, 또한 모든 노드와 직접 통신할 수 있기 때문에, 라우팅 프로토콜을 키 분배와 독립적으로 생각할 수 있다. 반면 확률적 키 분배의 경우에는 노드 간에 키를 공유키를 만드는 새로운 프로토콜이 필요하거나 새로운 라우팅 프로토콜을 디자인해야 하는 문제가 발생한다.

쿼럼 시스템에서의 성능에 영향을 미치는 요소는 크게 두 가지가 있다. 첫 번째, 노드 당 필요한 키의 수이다. 노드 당 유지하고 있어야 하는 키의 개수가 확률적 키

분배 기법에 비해서 적절하게 유지되어야 한다. 두 번째, 노출된 노드에 의해서 알려진 키가 전체 링크의 노출비율에 미치는 영향이다. 임의의 두 노드의 통신은 각각의 노드가 공유하고 있는 공유키를 이용하기 때문에 일부 노출된 노드에 의해서 알려진 키가 전체 링크의 노출에 미치는 영향이 키 분배 기법의 성능에서 중요한 평가 항목이 된다. 따라서 이후의 성능 평가에서는 센서 노드가 필요로 하는 키의 개수와 일정량의 키가 노출되었을 때 전체 링크의 노출비율을 분석하고 현재까지 알려진 기법 중에서 가장 적은 수의 공유키를 필요로 하고 노출된 노드에 의한 전체 링크의 노출비율이 가장 낮은 확률적 키 분배기법과 비교한다. 또한 노드 분포 정보가 고려된 쿼럼 기반 키 분배의 경우에 이러한 노드 분포 정보를 이용해서 센서 노드가 필요로 하는 키의 개수를 얼마나 더 줄일 수 있는지 분석하였다. 여기서 10,000개의 노드와 100,000개의 키 풀을 가정하였다.

4.1 노드 당 필요한 키의 수

쿼럼 시스템기반의 방법에서는 노드 개수나, 노드 밀도와는 무관하게 키 풀의 사이즈와 키를 뽑는 개수를 정할 수 있기 때문에 cyclic 쿼럼 시스템을 사용한다고 하면 316개의 키를 각각의 노드가 선택하면 된다. 쿼럼 시스템의 특성에 따라 키의 공유가 보장되고, 네트워크가 연결 된다. 확률적 기반의 방법에서는 노드의 밀도에 따라서 키 풀에서 뽑아야 하는 키의 개수가 달라지는데 [3] 만약 전송범위 내에 40개의 노드가 있다고 하면 263개 정도의 키를 뽑으면 되고, 30개의 노드가 있다고 하면 331개의 키를 뽑아야 한다.

그림 5에서는 필요한 키의 개수 분석[3]을 통해서 확률적 키 분배기법에서 99.999%의 네트워크 연결을 보장하기 위해 노드 하나가 필요로 하는 키의 개수와 쿼럼 시스템을 이용한 키 분배기법에서 필요로 하는 키의 개수를 네트워크의 밀도에 따라서 나타내었다.

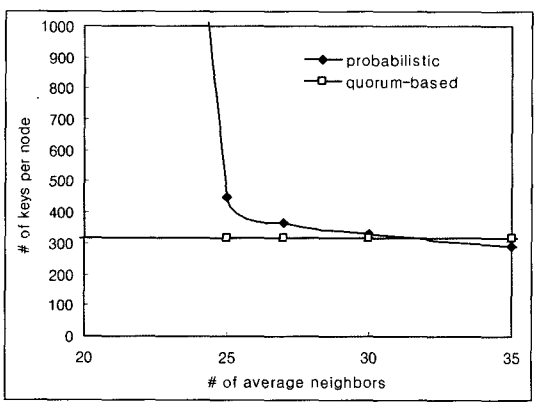

그림 5 이웃 노드 수에 따라 필요한 키의 수

그림 5에서 볼 수 있듯이 평균 이웃 노드가 많은 환경에서는 확률적 키 분배가 적은 키를 필요로 하지만 노드 밀도가 낮은 환경에서 확률적 키 분배는 점점 훨씬 많은 키를 필요로 한다. Random graph theory에서 네트워크의 연결을 위해 20개의 키가 공유된 이웃 노드가 필요하기 때문에, 평균 이웃 노드가 20에 가까워지면 노드가 가지고 있어야 하는 키의 개수는 급격하게 늘어나게 된다. 즉 이때 키 공유의 확률이 거의 1로 수렴해야 하기 때문에 각각의 노드는 키 풀 사이즈의 절반인 50,000개의 키를 가져야 하게 된다. 따라서 확률적 기법은 노드 분포 밀도가 충분히 클 때에만 사용할 수 있다. 그러나 쿼럼 시스템을 기반으로 한 방법은 노드 분포와 무관하게 일정량의 키를 필요로 하게 된다. 그런데 센서 네트워크에서 매우 많은 이웃이 있다고 생각 하기는 어렵기 때문에 낮은 밀도에서는 키의 개수가 더 적게 필요한 쿼럼 시스템이 더 적절하다고 생각된다.

4.2 전체 link의 노출 비율

보안 측면에서 가장 중요하게 생각되는 것은 노드가 노출되었을 때 네트워크에서 얼마나 많은 부분이 노출되느냐 하는 것이다.

x 개의 노드가 노출되었을 때 노출되는 링크의 비율

$$= 1-(1-\frac{m}{|n|})^{x} \quad (1)$$

n = 전체 키 풀 사이즈

m = 노드 하나가 가지는 키의 수

노드가 노출(compromised) 되었을 때 전체 link의 노출된 비율은 식 (1)과 같이 나타낼 수 있다[9]. 식에서 알 수 있듯이, 전체 키 풀 사이즈가 일정하다고 할 때 중요한 것은 하나의 노드가 몇 개의 공유키를 가지고 있는지 이다.

식 (1)을 이용해 네트워크가 보안에 얼마나 취약한지를 그림 6에서 나타내었다. 즉 노출된 노드가 증가함에 따라 노출되는 링크의 수를 확률적 방법과 비교하였다. 이때 확률적 방법에서는 평균 이웃 노드의 개수를 27, 30, 40으로 변경 해 가면서 계산하였다.

그림 6에서 볼 수 있듯이 위에서 노드 밀도에 따라서 성능이 변화한다. 노드가 조밀하게 분포 할 경우에는 확률적 기법이 좋은 성능을 나타내고, 그렇지 않을 경우는 확률적 기법의 성능이 떨어져서 더 많은 통신 링크가 노출 된다는 것을 볼 수 있다. 앞에서 설명 했듯이 이웃이 너무 많은 환경은 실제적이지 않기 때문에 쿼럼 시스템을 기반으로 한 방법이 보안 측면에서도 나쁘지 않다는 것을 알 수 있다.

4.3 노드 분포 정보를 고려한 쿼럼 기반 키 분배

노드 분포 정보를 고려해서 키 분배를 할 경우 필요

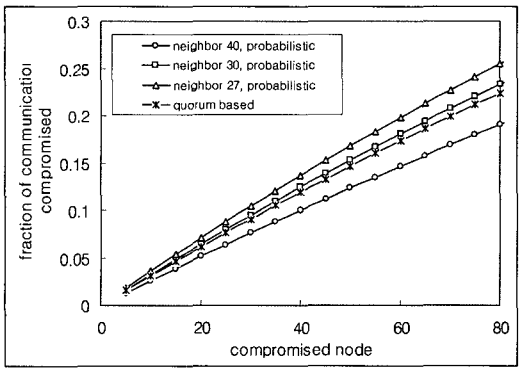

그림 6 네트워크에서 노출되는 키의 비율

한 전체 키의 개수를 크게 줄일 수 있다. 그림 4처럼 k*k개의 셀로 센서 노드가 나눠서 뿌려진다고 하고, 전체 키풀의 크기를 S라고 하면 $(k+1)^2$개의 쿼럼 시스템으로 S를 나누어야 한다. 즉 하나의 쿼럼 시스템이 가지고 있는 키 풀은 S/(k+1)이 되고, 센서 노드는 이 쿼럼 시스템에서 키를 뽑는다. 그런데 센서 노드는 4개의 쿼럼 시스템에 속해 있어야 하기 때문에 센서 노드 하나가 가지고 있어야 하는 키의 개수는 사이클릭 쿼럼 시스템을 사용한다고 할 경우 식 (2)와 같이 나타난다.

$$\text{센서 노드에 필요한 키의 수} = 4 \times \sqrt{\frac{S}{(k+1)^2}} \quad (2)$$

100,000개의 키풀을 사용하였고, 노드는 10*10의 셀로 나누어 져서 분포된다고 가정하였을 경우 노드 분포 정보를 고려 했을 때 노드가 가지고 있어야 하는 키의 개수를 그림 7에서 나타내었다.

노드 분포 정보를 고려하지 않았을 때 보다 훨씬 적은 키로 키의 공유를 보장할 수 있음을 알 수 있다.

그림 8에서는 노드 분포 정보를 알고 있고, 노드들은 똑 같은 키 개수를 가지고 있다고 할 때 쿼럼 기반 기법의 키 공유 확률을 확률적 기법[9]과 비교하였다. Probabilistic-far는 대각선으로 위치한 셀일 경우 키의

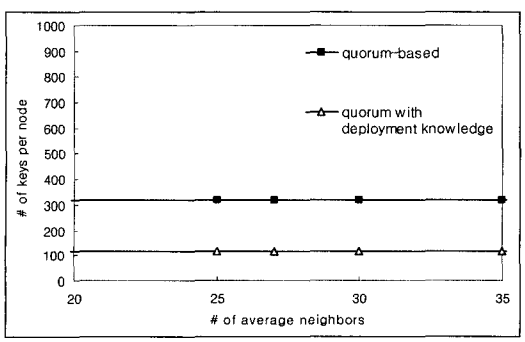

그림 7 노드 분포 정보를 알 경우 필요한 키의 수

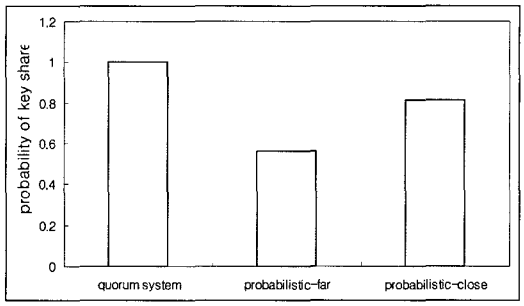

그림 8 노드간의 키 공유 확률

공유 확률이고, probabilistic-close는 상하좌우로 위치한 셀일 경우의 키 공유 확률이다. 그림 8에서 제시된 대로 이웃 셀의 노드와 키 공유 확률을 비교해 볼 때 쿼럼 기반 기법은 이웃셀의 노드와 키 공유가 보장되지만 확률적 기법에서는 대각선으로 위치한 셀에서는 공유 확률이 많이 떨어진다는 것을 볼 수 있다.

5. 결 론

센서네트워크에서는 노드 분포 환경에 적합하고 기존 라우팅 프로토콜 등에 영향을 주지 않으며 적은 자원을 사용하도록 키의 분배가 이루어져야 한다. 확률적 키 분배 기법은 적절한 양의 키를 노드가 가지고 있으면서도 전체 네트워크의 연결을 확률적으로 보장할 수 있지만 노드 밀도에 따라 가지고 있어야 하는 키의 개수가 달라지고, 밀도가 낮을 경우에는 이 방법을 사용할 수 없다. 또한 키 공유가 되지 못한 노드들을 위해서 새로운 라우팅 프로토콜이 필요하게 된다.

이에 비해 제안된 쿼럼 시스템을 기반으로 한 키 분배는 모든 노드들과의 키 공유를 보장해 준다. 이를 이용하면 센서 노드의 밀도와 무관하게 일정량의 키를 선택하게 되고, 모든 노드와의 키 공유를 보장 할 수 있게 되고, 추가적인 키 셋 업 프로토콜 오버헤드는 없다. 또한 필요한 키의 개수도 확률적 기법에 비해서 많지 않으며 만약 노드 분포 정보를 알고 있다고 가정하면 이웃 노드와의 키 공유를 여전히 보장하면서도 필요한 키의 개수를 현저하게 더 줄일 수 있게 된다. 논문에서는 쿼럼 시스템에 기반을 둔 키 분배 방법을 센서네트워크의 특징에 맞는 키 분배 방법으로 제시하고 그 성능을 비교 분석하였다.

참 고 문 헌

[1] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "Spins: Security protocols for sensor networks," in Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile

Computing and Networking (MobiCom), Rome, Italy, July 2001, pp. 189-199.
[2] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," in ACM Computer and Communications Security (CCS) 2003, October 2003.
[3] Laurent Eschenauer, "A Key-Management Scheme for Distributed Sensor Networks," ACM CCS 2002.
[4] J.Spence, "The Strange Logic of Random Graphs, Algorithms and Combinatorics 22," Springer-Verlag 2000.
[5] Haowen Chan,Adrian Perrig, Dawn Song, "random key pre-distribution schemes for sensor networks," IEEE symposium on Research in Security and Privacy, 2003.
[6] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, October 27-31 2003, pp. 42-51.
[7] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, October 27-31, 2003, pp. 52-61.
[8] R. Blom, "Non-Public Key Distribution," in Advances in Cryptology - CRYPTO 1982, August 1982.
[9] W.Du, J, Deng, Y.S. Han, S. Chen, and P.K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in Proc. of IEEE INFOCOM, 2004.
[10] C.J. Colbourn, J.H. Dinitz and D.R. Stinson, "quorum systems constructed from combinatorial designs," Information and Computation, pp.160-173, 2001.
[11] S.D. Lang and L.J. Mao, "A torus quorum protocol for distributed mutual exclusion," in Proc. of the 10th Internat. Conference on Parallel and Distributed Computing and Systems, pp. 635-638, 1998.
[12] W.S. Luk and T.T. Wong, "Two new quorum based algorithms for distributed mutual exclusion," in Proc. of International Conference on Distributed Computing Systems, pp. 100-106, 1997.
[13] M. Maekawa, "A $\sqrt{N}$ algorithm for mutual exclusion in decentralized systems," ACM Transactions on Computer Systems, 145-159, 1985.
[14] Y.C. Tseng, C.S. Hsu and T.Y. Hsieh, "Power-saving protocols for IEEE 802.11-based multi-hop ad hoc networks," in Proc. of IEEE INFOCOM, 2002.
[15] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, pp. 44-654, November 1976.
[16] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," ommunications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

강 지 명
2004년 서울대학교 컴퓨터공학부 졸업(학사). 2004년~2006년 서울대학교 대학원 전기·컴퓨터공학부 석사과정. 2006년~현재 한국전기연구원 연구원. 관심분야는 무선랜, 이동통신, 센서 네트워크, 홈 네트워킹

이 성 렬
정보과학회논문지 : 정보통신
제 33 권 제 2 호 참조

조 성 호
1999년 서울대학교 전산과학과 졸업(학사). 2001년 서울대학교 대학원 전기·컴퓨터공학부 졸업(석사). 2001년~현재 서울대학교 대학원 전기·컴퓨터공학부 박사과정. 관심분야는 프로토콜 디자인 및 성능분석, 이동성 관리, 이동통신, 센서네트워크

김 종 권
정보과학회논문지 : 정보통신
제 33 권 제 2 호 참조

안 정 철
1987년 한양대학교 전자공학과 학사 1990년 전북대학교 전자계산기공학 석사 1996년 일본 동경공업대학 전자물리공학 박사. 1990년~1999년 한국전자통신연구원 연구원. 2000년~현재 국가보안기술연구소 보안기술팀 팀장. 관심분야는 이동통신, 정보보호