센서네트워크에서의 다중선택 그리드 쿼럼을 이용한 안전한 키 분배

이병길* 전문석**
숭실대학교 대학원 컴퓨터학과
lbksuper@nate.com* mjun@ssu.ac.kr**

Key distribution using the Multi-Select Quorum System in Wireless Sensor Networks Environment

Byoung-Kil Lee*, Moon-Seog Jun**
Dept of Computer Science, Soongsil University

요 약

센서 네트워크는 구성의 편리성과 이동성, 확장성이 뛰어난 장점을 가지고 있어서 침입 탐지나 원격 감시 등 여러 분야에서 응용이 가능한 네트워크로 앞으로 계속 발전해야할 과제가 남아 있다. 즉, 센서 네트워크 환경에서는 보안성을 위해 센서 노드들은 키를 공유해야 하는데, 기존에 제안된 키 분배 기법은 키가 너무 많이 필요하거나, 비 효율적인 문제가 있고 노드간 연결이 안되서 도태 되는 노드가 생기는 등 취약한 점이 많다. 본 논문에서는 무선 센서 네트워크 환경에서 안전한 키 분배를 위한 방법중에 쿼럼 시스템을 응용한 다중선택그리드 쿼럼방식을 사용해 센서 노드들 사이의 인증을 강화시켜 외부의 공격 노드들로부터 안전하고 노드간 연결성이 보장되는 방법을 제시하고 있다.

1. 서론

무선 센서 네트워크(Wireless Sensor Network)는 필요한 지역에 뿌려진 센서 노드들로 하여금 물리적 또는 환경적 조건을 모니터링 하기 위해 구성된 독자적인 네트워크를 말한다. WSN은 현재에도 많은 분야에 쓰이고 있다. 하지만 네트워크를 구성하는데 있어서 각 노드들과 노드들 사이의 통신이 실시간으로 노출되기 때문에 기밀을 요하는 분야에서의 센서 네트워크 환경 구축을 위해서는 보안 프로토콜이 필수적 이다. 이런 보안을 지원하기 위해서는 각 노드들에게 키 분배가 되어야 한다. 보안 키를 사용하는 방식에는 대칭키 방식과 비 대칭키 방식을 들 수 있는데, 현재 가장 많이 쓰이고 있는 것은 비 대칭 키로, 비 대칭키는 공개키와 개인키를 한 쌍으로 공개키로 암호화 된 것은 개인키로 해독이 가능하고 개인키로 암호화 된 것은 공개키로 암호 해독이 가능한 방식이다. 이 방식은 강력한 보안성을 제공해 주긴 하지만, 알고리즘을 구현하는데 있어서 센서 노드의 제한된 자원소모가 크다. 일반적으로 센서 네트워크를 구성하는 센서들은 크기가 작고 계산 성능이 좋지 않기 때문에 비 대칭키 방식의 암호 알고리즘은 부적합 하다고 할 수 있다. 즉 센서 네트워크에서는 공유키를 노드에 미리 분배 해 둔 뒤, 이 키를 토대로 해서 통신을 진행하여야 한다.

키 분배 방식에서 가장 간단한 방법은 모든 센서 노드에 하나의 공유된 키를 분배하는 것 인데, 하나의 키를 사용하게 되면 연산이 간단하고 노드가 가지고 있는 정보도 많이 않다. 하지만 센서 네트워크에서 하나의 노드라도 외부로 노출이 된다면 공유키가 알려지는 문제점이 있다. 또한 각각의 센서 쌍마다 다른 키를 할당하는 방법이 있는데, 이 경우엔 하나의 노드가 노출이 되어도 전체 네트워크에 미치는 영향을 줄일 수 있다. 그러나 이 방법은 보안측면에서 너무 약하거나, 하나의 센서가 가지고 있어야 하는 키의 양이 너무 많아지게 된다.

센서 네트워크같이 자원이 제한된 환경에서는 그 환경에 맞는 키 관리 기법이 필요한데, 본 논문에서는 다중선택 쿼럼 방식을 이용해 이웃 노드와의 키 공유를 보장하는 새로운 기법을 제시하고자 한다. 쿼럼시스템은 하나의 센서 노드가 가지고 있어야 하는 키의 양을 제한 하면서 보안성은 강력한 방법을

제시한다. 특히, 쿼럼 시스템을 이용하게 되면 모든 센서 쌍이 항상 공유된 키를 가지게 되기 때문에 네트워크 상에서 분포된 노드들의 밀도와는 무관하게 네트워크의 연결성이 보장되는 효과를 볼 수 있다. 또한 노드간의 연결성이 보장되기 때문에 근접한 노드와 통신을 하기위해서 다른 노드로 돌아갈 필요가 없는 이점도 있다.

논문의 2장에서는 쿼럼 시스템(Quorum system)을 설명하고 3장에서는 제안하는 키 분배 방식을 소개한다. 4장에서는 제안된 방안의 성능을 분석하고 5장에서는 결론을 맺는다.

2. 관련 연구

센서 네트워크 환경에서 키를 분배하는 방식으로는 크게 상호인증된 제 3자를 두고 통신을 통해 키를 셋업하는 방식과 미리 사용할 키를 분배하는 방식으로 나눌 수가 있는데, 전자의 경우 키를 셋업하는 초기에 센서가 노출되지 않는다고 가정하거나, 키 셋업을 위한 컴퓨팅 파워가 많이 소모되는 단점이 있다. 따라서 본 논문에서는 키를 미리 분배하는 방식을 위주로 설명되어 있다.

키의 선 분배(Key pre-distribution)방식은 Laurent가 확률적 키 분배를 하기위해 처음 사용 하였다. 확률적 키 분배 방식에서는 처음에 큰 키 풀에서 일정량의 키를 랜덤(random)하게 골라서 가지게 된다. 일반적으로 노드들 간에 통신을 하기위해서는 같은 키의 공유가 필수적 이지만 확률적 키 분배를 사용하게 되면 두 노드 사이에 공유되는 키가 일정 확률로 이루어지기 때문에 노드 간 연결성이 항상 보장되지 않아서 인접한 노드인데도 불구하고 직접 통신을 진행 할 수 없다. 하지만 전체 네트워크가 같은 키를 사용하지 않으므로 보안성 유지 측면이나, 하나의 노드가 가지고 있는 키의 개수를 줄일 수 있는 측면에서 장점을 가지고 있다.

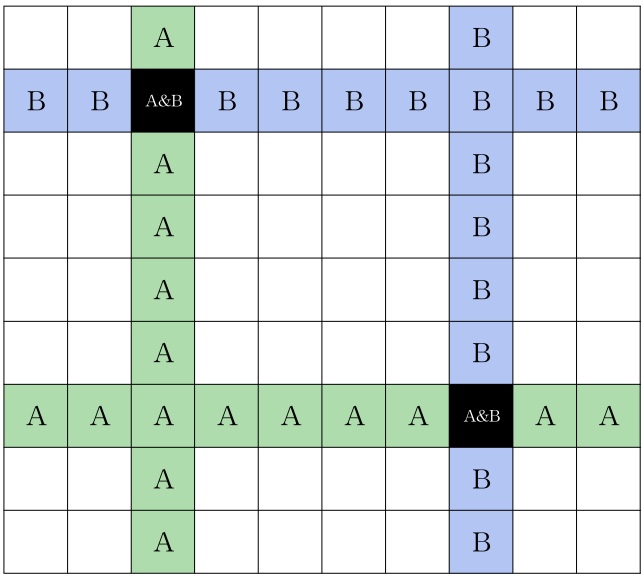
그러나 이러한 확률적 키 분배 방법은 임의의 두 노드 사이에 키 공유가 보장되지 않기 때문에 통신을 하기 위해서 먼 길을 돌아서 통신을 진행 하던지, 새로운 키 공유 프로토콜이 추가적으로 필요하게 되는데, 가까운 인접 노드가 있는데 굳이 멀리 돌아서 통신 하는 것은 매우 비효율적인 방법이며 새로운 키를 생성하기위한 프로토콜은 한정된 자원의 센서에서는 부담이 너무 커진다는 단점이 존재한다.

2.1 쿼럼 시스템

쿼럼(Quorum)이라는 것은 두 개의 교집합 원소가 무조건 하나 이상 존재하는 것을 말한다. 즉, 임의의 두 집합을 교집합 연산을 했을 때, 공집합이 되지 않는 집합들의 모임을 쿼럼 시스템(Quorum System)이라 한다. 예를 들어 {1,2,3,4,}, {2,5,6,8}, {3,8,9,0}은 쿼럼 시스템 이다. {1,2,3,4}∩{2,5,6,8}={2}, {2,5,6,8}∩{3,8,9,0}={8}, {1,2,3,4}∩{3,8,9,0}={3}으로 어떤 집합 셋끼리 교집합 연산을 하여도 공집합이 나오지 않기 때문에 쿼럼 시스템이 된다. 만약에 집합이 {1,2,3,4,}, {2,5,6,7}, {3,8,9,0} 이라면 {2,5,6,7}과 {3,8,9,0}의 교집합은 공집합이기 때문에 쿼럼 시스템이 되지 않는다.[1]

2.1.1 그리드(Grid)쿼럼 시스템

그리드 쿼럼 시스템에서 원소들은 2차원 평면 상에 줄지어서 위치해 있다. 쿼럼 시스템을 구성하기 위해서 각각의 집합은 그림 1과 같이 행과 열을 각각 하나씩 고르게 된다. 선택한 행에 속한 원소들과, 선택한 열에 속한 원소들을 합쳐서 자기의 원소로 정하면 이 시스템 내에서 임의의 집합 두 개를 선택하더라도 서로 겹치는 부분이 항상 최소 2개 이상 나오게 된다.



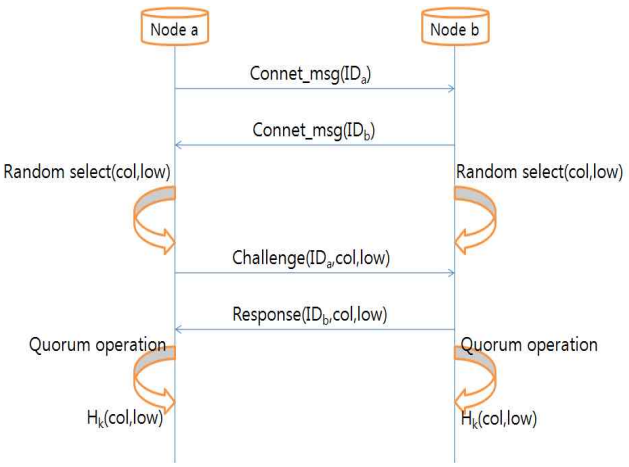
[그림 1] 그리드 쿼럼 시스템

이 쿼럼 시스템은 전체 원소 n개 중에서 $2\sqrt{n}-1$ 개의 원소를 뽑음으로 2개 이상의 공통 원소를 보장할 수 있는 특징이 있다.

3. 다중 선택 쿼럼 시스템

다중 선택 쿼럼 시스템의 개념은 기존의 그리드 쿼럼 시스템과 많이 다르지 않다. 그리드 쿼럼 시스템의 경우에는 각 노드마다 한 개의 행과 열을 선택하여 2개의 공통 되는 값이 나오는 방법을 설명하고 있다면, 다중 선택 쿼럼 시스템은 통신 키를 만들기 위해 행과 열을 k개 만큼 선택 하는 것이다.

예를 들면 n개의 키 풀이 있을 때, 각 노드마다 2개의 행과 열을 선택 한다면 8개의 공통된 값을 얻을 수 있고, 3개의 행과 열을 선택 한다면 18개의 공통된 값을 얻을 수 있다. 선택하는 행 열의 개수가 많아 질수록 유니크한 키가 만들어질 확률이 늘어나지만 반대로 전체 키 풀에서 사용되는 값도 많이 노출 되기 때문에 네트워크의 규모와 키 풀 사이즈를 고려해 조절해야 하고 사전에 분배되는 키 풀은 외부로부터 안전하다고 가정한다.



[그림 2] 노드 간 키 생성 흐름

[그림 2]는 임의의 두 노드 사이에 키 교환 시 일어나는 메시지의 흐름을 나타내고 있다. node a에서 connection message를 자신의 ID와 함께 보내면 네트워크에 합류하려고 하는 node b에서 connection message에 대한 response를 자신의 ID와 보내게 되면 node a와 node b는 각각 자신의 키 풀에서 랜덤한 행과 열을 선택한다. 그 후 식별자로 쓸 ID와 선택한 행, 열 값을 주고받게 되는데, 키를 교환하고자 하는 node 와의 challenge-response 단계가 끝나면 각 노드에서는 키를 생성하기 위한 쿼럼 연산을 하게 되는데, 기존의 그리드 쿼럼 방식대로 하나의 행과 열을 선택한다면 공유할 수 있는 값이 두 개 밖에 나오질 않기 때문에 전수조사 공격에 취약 할 수 있다. 따라서 여러 개를 선택(multi-select)를 하되 키 풀 사이즈와 네트워크 규모에 맞게 조절 한다. 예를 들어 행, 열 각각 3개씩 선택 한다고 했을 때, node a와 node b가 공유 할 수 있는 값은 18개가 나오기 때문에 18개의 값을 가지고 해쉬 함수를 돌려서 유니크한 키를 만들면 안전한 키 교환이 완료된다.

4. 성능 평가

3장에서 제안한 다중 선택 쿼럼 시스템은 간단하지만 키 생성에서 안전하면서 유니크한 값을 뽑아낼 수 있고 연산 컴퓨팅 파워가 낮아 센서 네트워크처럼 자원을 사용할 수 있는 환경이 제한되어 있는 시스템에서 모두 적용이 가능하다.

[표 1] 제안 시스템과 기존 방법의 비교 표

	제안시스템	PKI	ZIGBEE
자원소모	적음	보통	많음
연산량	적음	많음	보통
안전성	높음	높음	보통
연결성	높음	보통	보통

[표 1]은 본 논문에서 제안한 시스템과 PKI, ZIGBEE등과 자원소모량과 연산량, 안전성 및 연결성을 상대적으로 비교 분석한 것이다. 표에서 보다시피 PKI시스템은 키 교환시 지수적인 알고리즘을 사용함으로 안전성이 높지만 알고리즘이 복잡한 만큼 자원소모량과 연산량이 사용할 수 있는 자원이 제한된 환경에서는 불리하게 작용한다. 마찬가지로 ZIGBEE의 경우 PKI시스템보다는 알고리즘의 연산량이 적지만 중간에서 브리지 역할을 하는 노드의 경우 네트워크의 규모가 커질수록 처리해야 하는 데이터 량이 많기 때문에 자원소모에서 불이익을 볼 수 있다. 게다가 노드간에 연결을 보장할 수 있는 방법이 없거나 연결하기 위해서는 다른 프로토콜을 추가 해야 하기 때문에 낙오되는 노드가 생기거나 시스템이 무거워 지게 된다. 반면 제안된 시스템은 2차원 행렬과 해쉬 함수만을 사용하기 때문에 자원소모량이나 연산량에 있어서 좋은 퍼포먼스를 기대할 수 있고, 안전성의 측면에서는 다중선택을 통해 키를 생성하는데 있어서 안전하게 보안했다. 또한 쿼럼 시스템의 장점인 노드간 공유할 수 있는 키가 100% 생성되기 때문에 연결성의 측면에서도 매우

우수하다.

5. 결론

다중 선택 쿼럼 시스템은 노드간 공유되는 키를 100% 제공하기 때문에 옆 노드와 통신하기 위해 일부러 먼 길을 돌아서 통신할 필요가 없고 2차원 행렬과 해쉬 함수만을 사용함으로써 연산 속도나 자원 소모량에 대해 다른 시스템 보다 적합한 형태의 시스템이라고 할 수 있다. 하지만 다중 선택 쿼럼 시스템은 2차원 행렬의 키 풀에서 여러 개를 선택하게 되므로써 보다 강력한 키를 생성할 수 있지만, 키 풀에서 선택되는 행렬이 많아질수록 키 풀의 노출이 커지는 문제점이 있다. 선택하는 행, 렬이 하나씩 많아 질 때 마다 키 자체의 보안 강도는 제곱 그래프를 그리지만, 네트워크 규모에 맞게 조절하는 과정이 필요 하다. 그러나 만약 노드의 위치정보를 알고 있다고 가정하면 위의 문제점을 최소화 시킬 수 있기 때문에 여러 가지 환경에서 적용이 가능한 장점이 있다.

참고문헌

[1] 강지명 “센서 네트워크에서의 쿼럼 시스템을 이용한 키 사전 분배” 정보과학회 논문지 : 정보통신 제 33권 제 3호(2006.6)