분산 센서 네트워크에서 Multi-hop Pairwise Key를 이용한 Cluster Routing 기법

박소영[O] 김형찬, R.S. Ramakrishina
광주과학기술원 정보통신공학과
{spark[O], kimhc, rsr}@gist.ac.kr

Cluster Routing Scheme using Multi-hop Pairwise Key for Distributed Sensor Networks

Soyoung Park[O] Hyung Chan Kim, R.S. Ramakrishina
Dept. of Information and Communications
Gwangju Institute of Science and Technology

요 약

본 논문에서는 센서네트워크를 위한 기존의 클러스터 라우팅 기법에 multi-hop pairwise key를 적용시킴으로써 multi-hop pairwise key를 기반으로 하는 클러스터를 구성하고 이를 통한 클러스터 간의 통신을 제안한다. 이는 암호화된 클러스터 통신을 위한 키 분배에 있어서 메모리 효율성을 높이고, 클러스터 라우팅의 난제였던 클러스터 헤드 선택과 관리를 효과적으로 할 수 있게 한다.

1. 서 론

최근 센서 네트워크에 대한 활발한 연구가 진행되고 있다. 센서 네트워크는 기존의 네트워크와 달리 라우터가 없는 adhoc 네트워크 방식을 사용하므로 각각의 노드들이 라우팅을 한다. 다양한 센서 네트워크 어플리케이션의 요구사항에 맞추어 저전력, 대체 경로, 보안 등을 지원하는 라우팅 프로토콜에 대한 연구가 활발하게 진행되고 있다.

센서 네트워크에서의 라우팅 기법은 크게 direct communication과 cluster routing의 두 가지 방법으로 나눌 수 있다. Direct communication은 센서 네트워크 내의 모든 노드들이 라우팅에 관여하여 노드간 통신을 직접적으로 하는 방법이며, cluster routing 기법은 전체 센서 네트워크를 여러 개의 클러스터들로 나누고, 각 클러스터 내의 한 노드(cluster head)가 라우팅 노드가 되어 클러스터간 통신을 하는 방법을 말한다. 후자의 경우는 전자에 비해 여러 가지 장점을 가지고 있다. 첫째, 계층구조로 인해 scalability를 제공하고 둘째, 목적지까지 가는 available route를 찾는데 있어서 에너지 효율성을 높일 수 있다. 더불어, 센서와 route들을 관리하는 데 있어 장점을 가지고 있다. 그러나, 이러한 장점들에도 불구하고 클러스터 라우팅 기법은 몇 가지 제약들을 가지고 있는데, 현재 가장 큰 이슈는 각각의 cluster head를 관리하는 문제이다. Cluster head의 failure는 전체 네트워크의 단절을 가져 올 수 있으며, 이와 관련된 문제로 cluster head selection 문제도 함께 제기되고 있다. 이러한 제약 때문에 cluster routing 기법보다도 direct communication에 접근하는 프로토콜이 많이 개발되고 있다.

본 논문에서는 센서 네트워크의 클러스터링 라우팅 기법에 있어서 클러스터를 생성시키고 cluster head selection 문제에 새로운 접근 방법을 제시한다. 세부적으로 센서 네트워크에서 보안 메커니즘으로 사용되고 있는 pairwise key를 이용하여 클러스터를 생성시키는 방법과 cluster head 관련 문제들 - cluster head selection과 클러스터 헤드 failure시 클러스터 복구 - 을 효율적으로 할 수 있는 방법을 제시한다.

2. 센서 네트워크에서의 Pairwise Key

센서 네트워크에서는 각각의 센서 노드간의 암호화된 통신을 위해 각 노드 상호간의 고유키(pairwise key)를 이용한다. 현재 개발되고 있는 센서 네트워크 통신 프로토콜들 중에는 다수가 이러한 pairwise key를 사용하고 있다.

센서 네트워크에서 pairwise key를 생성시키기 위하여 보통 pre-distribution 과정을 거친다. 이 과정에서는 센서 노드들을 분산시키기 전에 초기값(seed key)를 생성시켜 각 센서 노드에 저장하고, 노드들이 분산된 후 이웃한 노드들끼리 agreement 과정을 거쳐 pairwise key를 설정한다.

또 다른 방법은 pre-distribution 을 이용한 pairwise 키 생성 메커니즘에 확률을 사용하는 것으로, 랜덤 그래프를 이용하여 전체 네트워크의 complete graph를 생성하는 방법이다[1]. 이 방법은 모든 이웃한 노드와 pairwise

key를 생성하지 않고 확률을 이용해 전체 네트워크의 complete graph를 생성시키는 n개의 이웃한 노드와 pairwise key를 생성한다.

Localized Encryption and Authentication Protocol (LEAP)[2]은 pairwise key를 이용해 통신하는 대표적인 센서 네트워크의 라우팅 프로토콜이다. LEAP에서 제안된 방법은 우선 pre-distribution을 거쳐 생성된 pairwise key로 센서 네트워크를 구성하고, 이를 이용해서 클러스터 키를 생성하고 클러스터를 이룬다. 그러나 LEAP 프로토콜에서의 클러스터는 라우팅을 위한 클러스터가 아닌 local area의 암호화된 브로드캐스팅을 위한 한 노드와 그 주변의 인접하는 노드들간의 클러스터를 말한다. 그러므로 각각의 센서 노드마다 자신의 클러스터를 생성시키는 데 이는 각 센서 노드의 클러스터 키를 위한 메모리 사용을 높이게 된다 [그림 1].

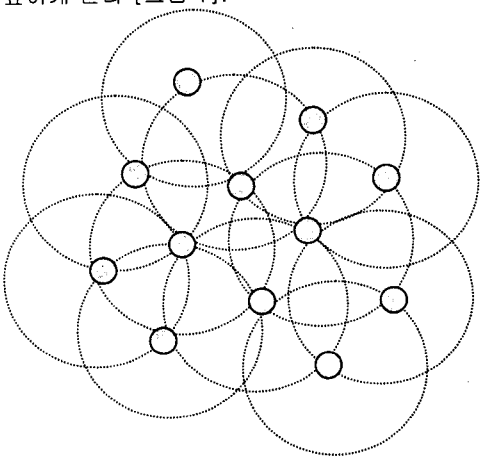

그림 1. LEAP 프로토콜의 클러스터.

3. Multi-hop Pairwise Key와 Clustering

본 연구에서는 LEAP의 암호화된 통신을 위한 클러스터 원리를 클러스터 라우팅 기법에 적용시키고자 한다. 이를 위해서 pairwise key를 multi-hop 노드들간의 통신까지 확장시키고 이러한 multi-hop pairwise key를 기반으로 하여 클러스터를 생성시키는 방법을 제안한다.

3. 1 Multi-hop Pairwise Key Scheme

본 연구에서는 multi-hop pairwise key를 생성시키는데 Blom의 symmetric key generation system[3]을 기반으로 한pairwise key pre-distribution scheme[4]을 사용한다. Blom에 따르면 λ 개 이상의 센서 노드가 외부 네트워크에 의해 손상되지만 않는다면 네트워크는 완벽하게 안전하다고 한다(λ -secure property).

Blom의 symmetric key generation system 방법은 다음과 같다.

1. Pre-distribution phase에서 base station은 finite field GF(q)에서 연산하는 (λ +1) x N 크기의 행렬 G를 생성한다(이하 모든 연산은 finite field GF(q)에서 연산된다). 이 때 λ 는 blom이 제안한 λ -secure property를 제공하는 수이고 N은 네트워크의 전체 노드의 수이다. 행렬 G는 내부 네트워크의 센서 노드와 외부 네트워크 모두에게 공개되는 정보이다.
2. 행렬 G를 생성시킨 후 또한 임의의 (λ +1) x (λ +1) 크기의 행렬 D를 생성한다. 단, 행렬 D는 symmetric 행렬이다.
3. 이렇게 생성된 행렬 G와 행렬 D를 이용해서 key 값을 가지는 행렬 K를 다음과 같이 생성시킨다 [그림 2].
   - $A = (D \cdot G)^T$.
   - $K = A \cdot G$.

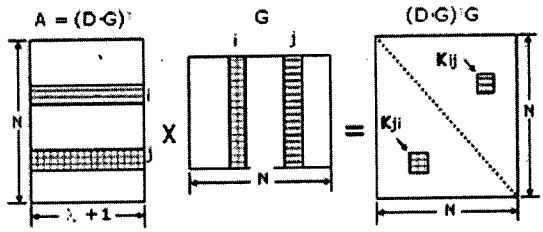

그림 2. Blom' s symmetric key generation system. K=A·G.

이렇게 해서 생성된 행렬 K는 symmetric 행렬이 된다. 그러므로, 센서 노드 i와 j의 pairwise key K_{ij} 와 K_{ji}값은 동일하게 된다. 또한 pre-distribution 중에 임의의 노드 i는 행렬 A의 i번째 행과 행렬 G의 i번째 열만을 저장함으로 노드 i의 모든 pairwise key를 계산할 수 있게 된다. 덧붙여, λ -secure property에 의해 모든 행렬 G의 λ +1 열은 독립적이기 때문에 센서 노드는 각각의 seed key만으로도 모든 pairwise key를 계산 할 수 있다.

Blom의 키 생성 기법은 각각의 pairwise key들의 저장을 필요치 않고 seed key만을 가지고 양쪽의 노드가 동일하게 계산 가능하므로, 센서 노드에서의 메모리 사용의 효율성을 높여준다. 특히 pairwise key를 multi-hop으로 확장시키는 경우 센서 노드에 저장되어야 할 키의 수가 hop 수에 따라서 지수 함수의 모양으로 증가하는데 반하여 Blom의 키 생성 기법은 그러한 overhead를 효율적으로 줄여준다.

3. 2 Multi-hop Pairwise Key를 이용한 Cluster 구조

센서 노드가 분산된 후에 각 센서 노드는 Multi-hop pairwise key를 생성하고 각각의 클러스터를 이룬다. 클러스터의 사이즈는 pairwise key의 확장된 hop count에 따라 클러스터의 사이즈도 확장되게 된다. 그러므로 클러스터를 어느 정도 확장시킬 지에 따라서 hop count의 선택은 달라진다.

그러나 기존의 LEAP 프로토콜의 방식대로 클러스터를 생성시키게 되면 모든 노드가 클러스터를 생성시키게 된다. 불필요한 클러스터의 생성을 제한하고 클러스터 간의 라우팅을 효율적으로 하기 위해서 클러스터 헤드를 선택

하고 관리하는 것이 필요하다.

본 연구에서는 클러스터 헤드를 선택하는 방법으로 각 클러스터의 n-hop 노드들 - 클러스터의 경계에 있는 노드들 - 만을 클러스터 헤드로 사용하고 Multi-hop pairwise key를 생성하고 클러스터를 이룬다 [그림 3].

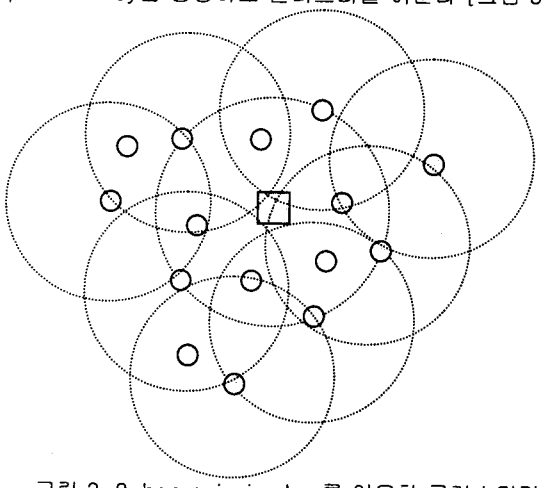

그림 3. 2-hop pairwise key를 이용한 클러스터링.

Base station이 n-hop 이내에 있는 이웃 노드들과 pairwise key를 설정하고 클러스터를 이루면 클러스터의 경계에 있는 노드, 즉 base station으로부터 n-hop 거리에 있는 노드들이 base station과 같이 클러스터 헤드가 되어 pairwise key를 설정하고 클러스터를 만든다.

그러나 n-hop 거리에 있는 모든 노드들이 클러스터를 생성할 경우 여러 개의 클러스터와 중복되는 불필요한 클러스터의 생성이 불가피하다.

그렇기 때문에 불필요한 중복된 내부 클러스터의 생성을 막기 위하여 하나의 센서 노드가 속할 수 있는 클러스터의 수에 제한을 둔다. 각 노드마다 노드 자신이 속한 클러스터의 수를 기억하고 만약 현재 포함되어 있는 클러스터의 수가 일정한 범위를 넘게 된다면 경계 노드라 할지라도 multi-hop pairwise key 생성을 제한함으로 과도한 클러스터의 생성을 제한할 수 있다.

이러한 방법을 사용한다면 클러스터 헤드의 장애 등으로 인해 클러스터의 실패가 생겨도 주위의 노드들이 클러스터의 수가 일정 수치 이하에 있다는 것을 판별할 수 있게 된다. 곧, 다른 경계 노드가 새로운 클러스터 헤드의 역할을 수행해 새로운 클러스터를 생성시킬 수 있게 되고 이는 네트워크의 신뢰성을 높여준다.

4. 결 론

본 논문에서는 클러스터 라우팅 기법에 새로운 접근을 시도하였다. 이는 pairwise key의 multi-hop 확장인 multi-hop pairwise key를 이용하여 클러스터를 생성하도록 하는 것이다.

Blom의 symmetric key generation system을 도입해서 multi-hop pairwise key를 생성하도록 하고 생성된 키를 이용해 클러스터를 생성한다. 그리고 불필요한 클러스터의 생성을 제한하고 클러스터 간의 라우팅을 위하여 각 클러스터의 경계 노드들만을 클러스터 헤드로 선택하고, 하나의 노드가 속할 수 있는 클러스터의 수에 제한을 둠으로써 불필요한 클러스터 헤드의 생성을 막고 필요할 시 다른 노드가 클러스터 헤드로 대체할 수 있게끔 한다.

이러한 방법은 기존의 클러스터 라우팅 기법에서 난제였던 클러스터 헤드 selection과 failure 문제를 해결하는 데 있어 도움이 된다. 또한 클러스터 내부에서 각 노드의 pairwise key를 사용함으로써 통신 데이터의 안전성에도 효과적이다.

참고문헌

[1] L. Eschenauer, V.D. Gligor. A Key Management Scheme for Distributed Sensor Networks. CCS' 02, Washington, DC, USA, November 2002.

[2] S. Zhu, S. Setia, S. Jajodia. LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. CCS' 03, Washington, DC, USA, October 2003.

[3] R. Blom. An Optimal Class of Symmetric Key Generation Systems. Advances in Cryptology: Proceedings of EUROCRYPT 84 (Thomas Beth, Norbert Cot, and Ingemar Ingemarssan, eds.), Lecture Notes in Computer Science, Springer-Verlag, 209:335-338, 1985.

[4] W. Du, J. Deng. A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. CCS' 03, Washington, DC, USA, October 2003.