# 센서 네트워크에서의 하이브리드 방식의 키 분배 구조

천은미° 도인실 채기준
이화여자대학교 컴퓨터학과
{emchun°, isdoh, kjchae}@ewha.ac.kr

# A hybrid key pre-distribution scheme for sensor networks

Eunmi Chun°, Inshil Doh, Kijoon Chae
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

센서 네트워크는 다양한 탐지 대상 및 환경을 감시하는데 유용하게 사용될 수 있다. 이러한 센서 네트워크에서 센서 노드간 키를 설립하는 것은 보안을 위한 가장 기본적인 요구 사항이다. 하지만 센서가 가진 기본 특성인 자원의 제약 때문에 일반 네트워크에서 사용되고 있는 중앙 키 분배 서버를 이용한 키 분배나 공개키 기법을 사용하는 것은 적합하지 않다. 따라서 본 논문에서는 센서 네트워크 특성에 맞는 키의 사전 분배 방식을 제안한다. 본 논문에서 제시한 기법은 클러스터를 기반으로 위치 정보를 이용하여 키를 사전 분배하였기 때문에 노드간 키 설립확률을 높였을 뿐만 아니라, 악의적인 노드에 의해 다항식이 공개되어 정상 노드가 붕괴되는 것을 막기 위해 클러스터당 헤드를 두어 다항식을 공유하는 노드의 범위를 줄여 보안을 보다 강화 시켰다.

## 1. 서론

유비쿼터스 컴퓨팅 개념의 도입과 함께 이를 실생활에 적용시킬 수 있는 방안이 활발하게 연구되는 가운데 현실적인 유비쿼터스 환경을 제공해 줄 수 있는 센서 네트워크가 주요 이슈로 부각되고 있다. 매우 많은 수의 센서 노드들로 구성되는 센서 네트워크는 센서를 통한 정보 감지 및 감지된 정보를 처리하는 기능을 수행한다. 그러나 센서들을 통해 보다 많은 다양한 정보를 습득하고 처리할 수 있는 반면, 감지된 넘쳐 나는 정보들로부터 정보의 무결성 및 개인의 프라이버시도 함께 보장할 수 있어야 한다. 즉, 보다 현실적이고 원활한 유비쿼터스 컴퓨팅 환경을 구현하기 위해서는 센서 네트워크의 활용 방안 및 센서 기술 개발과 함께 센싱된 정보를 안전하게 처리하고 관리 할 수 있는 센서 네트워크 상에서의 보안 메커니즘 개발이 반드시 함께 연구되어 적용되어야 한다[2].

안전한 통신을 위하여 일반적인 네트워크에서는 키 관리 방법에 대한 다양한 연구가 진행되어 왔다. 첫째, 신뢰된 인증 서버에 의하여 키를 분배 받는 방법으로, 이는 센서 네트워크와 같은 구조적인 기반 구조가 없는 환경에서는 적용이 어렵다. 둘째, 공개키 인증서를 활용한 비대칭 암호화 방법으로, 한정된 계산력과 에너지로 구성된 센서 노드에서 Diffie-Hellman이나 RSA 방법을 적용하는 것은 바람직하지 않다. 따라서 센서 네트워크에 가장 적합한 방식은 센서 노드를 배치하기 전에 키 정보를 미리 저장하는 키 사전 분배 방식이라 할 수 있다.

본 논문에서는 메모리를 적게 사용할 뿐만 아니라 키 공유로 인한 보안 위협 문제를 해결 할 수 있는 하이브리드한 방식을 사용한 키 사전 분배 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 센서 네트워크에서 키 분배를 위해 지금까지 수행된 연구들과 문제점을 살펴보고 3장에서는 하이브리드 방식의 키 사전 분배 방법을 살펴본다. 마지막으로 4장에서는 결론을 내리도록 한다.

## 2. 기존 연구

기존에 제안된 확률적 랜덤 키 사전 분배 방법은 센서가 센서 필드에 설치되기 전에 각 센서 노드가 대규모 키 풀(Key pool)로부터 부분 키 집합을 받는 방식이다[3]. 센서 노드들이 통신을 하기 위하여 임의의 두 노드는 그들의 키 집합 내에서 공통키를 찾고 노드간 통신을 위한 공유키로 사용한다. 또한 이 방법 기반에 필요한 키 기준치를 통신 채널의 파라미터로 추가하여 보안을 좀더 향상시킨 q-composite 랜덤 키 사전 분배 방법도 있다[4].

그러나 확률적 랜덤 사전 키 분배 방식과 q-composite 방식은 노출된 센서의 수가 많지 않아도 노출되지 않은 센서들과 공유하는 키로 인해 정상 센서가 붕괴될 가능성이 높아진다는 단점을 갖는다. 물론, 확률적 랜덤 pair-wise 키 구조는 노드 포획에 대한 저항성을 가지고 있지만 두 센서가 원하는 키를 설립할 확률과 각 센서가 키 집합을 저장해야 하는 오버헤드로 네트워크의 크기의 제한이 있다.

또한 좌표를 기반으로 하는 다항식 사전 분배 방식[5]과 위치를 기반으로 하는 다항식 사전 분배 방식[6]은 다항식을 사용하기 때문에 그 다항식이 t차식일 경우 t+1개의 노드가 노출되면 그 다항식을 공유하는 모든 센서들의

의 키가 노출되는 결과를 초래한다.

또 다른 제안 구조는 지역 정보를 아는 배치 모델로써 센서의 이동성이 많지 않다고 가정하고 센서의 위치를 특정 범위 내에서 사전에 결정할 수 있다는 방식을 사용한다. 이 방식은 센서의 위치 정보를 사용하여 센서 상호간의 키 설립 확률을 높일 수 있다. 센서들은 target field라 지칭되는 2차원 평면에 배치된다고 설정한다. 센서의 위치는 target field의 좌표로 표현된다. 각 센서는 미리 결정되어지거나 혹은 예상되어 질 수 있는 예상 위치 정보를 가지고 있다[5]. 또한 여기서는 다항식 사전 분배 방식을 사용하는데 이는 pair-wise 키를 미리 분배하기 위해서 Base Station은 무작위로 t차 다항식 f(x,y)를 고정 필드 $f_q$에서 생성한다. 여기서 q값은 암호화 키를 만들 수 있을 정도로 큰 소수여야 한다. 또한 이 다항식은 f(x, y) = f(y, x)의 성질을 만족 한다. 각 센서가 공통의 다항식을 소유하게 되면 상대방의 ID를 사용하여 공통의 키를 계산할 수 있다[1].

또한 근접 노드간 키 사전 분배 방식이 제안 되었는데 이는 지역정보를 사용하여 가장 인접한 센서에 키를 사전에 분배하는 방식이다. 이 방식을 살펴보면, 임의의 센서 u를 중심으로 c개의 센서들이 설치 되고자 하는 장소가 u 센서와 가장 인접한 지역이라면 u와 c들의 집합 S와 pair-wise 키를 사전 분배하여 사용하게 된다. S에 포함되는 각각의 센서 v를 위해서, Base Station은 유일한 pair-wise 키 $K_{u,v}$를 생성한다. 그러면 Base Staion은 각 센서 u와 v에게 키 $(v, K_{u,v})$ 와 $(u, K_{u,v})$을 분배한다[6].

### 3. 제안 스킴

본 논문에서는 다항식을 공유하는 키의 수를 줄이고자 클러스터 단위로 다항식을 사전에 분배하고, 클러스터 헤드에게는 근접 노드와의 키를 사전에 분배하는 방식을 조합한 하이브리드한 방식의 키 사전 분배 구조를 제안하고자 한다. 우선 제안 시스템의 구조와 가정을 살펴 본 후 키 관리 메커니즘을 살펴 보도록 하겠다.

3.1 제안한 시스템의 구조와 가정

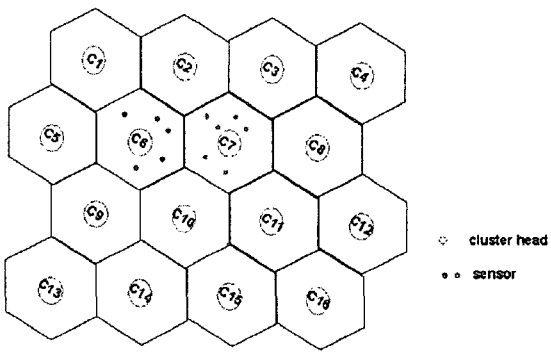
본 논문은 센서 네트워크의 target field를 육각형 모양의 클러스터 형태로 나눈다. 기존 연구 [6]에서 사용 하였던 사각의 클러스터 보다 육각구조를 사용함으로써 상호 키 설립 확률을 높이는 이점을 가진다. 각 클러스터에는 클러스터 헤드가 존재한다. target field를 사각형으로 나누는 것보다 육각형 모양으로 나누게 되면 클러스터 헤드가 저장해야 하는 pair-wise 키의 수는 6개지만 4개의 pair-wise키를 갖는 기존의 방법보다 직접 키 설립 확률이 더 크기 때문에 통신 채널을 설립하는 비용이 적게 든다.

센서네트워크의 구성요소로는 Base Station과 클러스터 헤드, 클러스터에 존재하는 센서들로 구성되어 있다. Base Station은 모든 정보를 수집하여 전달하는 게이트웨이 역할을 한다. 클러스터 헤드가 설치 될 위치를 Base Station은 정확히 알고 있어 클러스터 헤드에는 6개 이웃 클러스터에 존재하는 클러스터 헤드와의 pair-wise키가 미리 분배되어 있다.

Base Station은 클러스터 내에 존재하는 센서들이 위치하고자 하는 예상위치를 알고 있어 이 위치에 해당하는 다항식을 클러스터 헤드를 포함한 센서들에게 사전 분배한다. 이 다항식을 이용하여 클러스터 내의 센서들은 센서간 통신 키를 계산할 수 있다. 다항식을 사용한 기존의 방법들도 다항식을 사전 분배하여 이를 공유하는 센서간 키를 설립하는 기법을 사용하였다. 그러나 기존 방법은 다음과 같은 단점이 있다. 만약 다항식이 t차 식일 경우 t개 노드가 노출되어도 다항식이 노출되지 않아 안전하지만 센서 노드의 수가 매우 클 경우 노출되는 센서 수가 t개를 넘어서면 센서 네트워크 전체가 마비되는 상황이 될 수 있다.

따라서 본 논문은 기존에 제안 되었던 방법을 응용하여 클러스터에 헤드를 두어, 클러스터간 통신은 클러스터 헤드만의 고유 키를 사용하게 함으로써 다항식을 공유하는 센서의 수를 줄인다. 그 결과 노출되는 센서의 수도 줄 일 수 있어 보안에 있어 좀더 향상된 결과를 가져올 수 뿐만 센서간 효율적인 키 설립도 가능해 진다.

이와 같은 구조를 위해 가정하고 있는 내용은 다음과 같다. 첫째, Base Station은 네트워크의 전송범위를 알고 있다. 둘째, 클러스터 Ci에 존재하는 클러스터 헤드는 ID로 Ci를 사용하고 센서들은 각각의 고유한 정수 ID를 가지고 있다. 셋째, 클러스터간 통신은 반드시 클러스터 헤드를 통해 이루어진다. 넷째, 패킷은 멀티 홉을 거쳐 목적지에 도달할 수 있다. 다섯째, 센서 네트워크는 애드 혹 네트워크 만큼 이동성이 크지 않다.




[그림 1]

3.2 제안한 키 관리 메커니즘

3.2.1 사전 키 분배

센서 네트워크의 target field를 s = n x n 육각 클러스터로 구획을 나누어 Base Station은 임의의 s개의 다항식을 생성한다. 여기서 클러스터의 위치는 물리적인 위치가 아닌 논리적 위치로 생각한다. 따라서 지역 Ci에 해당 하는 다항식은 $f_{ci}$이 된다. 각 셀은 하나의 클러스터 헤드를

가진다. [그림1]에서 Base Station은 C6의 근처 위치 하고 있는 6개의 클러스터 헤드 C1, C2, C5, C7, C9, C10와의 키 $K_{C6,C1}$, $K_{C6,C2}$,. $K_{C6,C5}$, $K_{C6,C7}$, $K_{C6,C9}$, $K_{C6,C10}$를 생성하여 노드에게 미리 분배 한다. 센서들의 예상 배치위치를 아는 Base Station은 논리 주소 C6에 위치하고자 하는 클러스터 헤드를 포함한 센서들에게 이 지역에 해당하는 다항식 $f_{C6}$을 할당한다.

3.2.2 직접 키 설립

■ 센서 대 센서

각 센서에 키가 사전에 분배되어 있다면 센서들은 그 정보를 이용하여 직접 키로 사용할 수 있다. 예를 들어 셀 C6에 배치되는 센서는 이미 이 위치에 해당하는 다항식 $f_{C6}$을 할당 받았기 때문에 이 셀에 위치하는 어떤 센서들과도 상대방의 ID만 알고 있으면 공통의 키를 구할 수 있다.

■ 센서 대 클러스터 헤드

센서와 클러스터가 통신을 하고자 하면 센서 뿐만 아니라 클러스터 헤드도 다항식을 이미 알고 있으므로 센서와 클러스터 헤드도 지역에 할당된 다항식을 이용하여 서로간 키를 계산하여 사용할 수 있다.

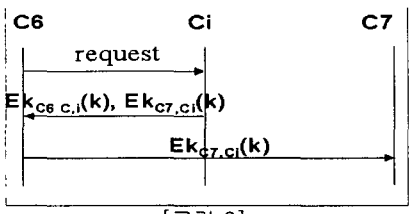
■ 클러스터 헤드 대 클러스터 헤드

클러스터 헤드는 자신과 이웃 하는 지역의 클러스터 헤드들간의 상호 키를 이미 알고 있으므로 이 키를 직접 키로 사용한다.

3.2.3 간접 키 설립

셀 내의 센서들은 자신에게 할당된 다항식을 이미 알고 있으므로 간접 키를 설립할 경우는 생기지 않지만 클러스터 헤드 간은 간접 키를 생성해야 하는 경우가 발생한다.

키 배치 후, 인접 위치에 있는 두 클러스터 헤드가 사전 분배 된 키를 가지고 있지 않다면 이 두 개의 클러스터 헤드는 이 두 센서와 상호 키를 가진 근접 클러스터에 위치한 클러스터 헤드를 이용하여 세션 키를 설립한다. 예를 들어 [그림 2]에서와 같이 센서 C6와 C7가 사전 분배 키를 가지고 있지 않다면 C6은 C7과 키를 설립하고자 C6과 C7의 사전 분배 키를 모두 알고 있는 Ci에게 키 생성 요청 메시지를 보낸다. 이 메시지를 수신한 Ci는 세션 키를 생성하여 $K_{C6,Ci}$, $K_{C7,Ci}$ 키로 세션 키 k를 암호화하여 C6에게 전송한다. C6는 이 세션 키를 복호화하고 키 $K_{C7,Ci}$로 암호화된 세션 키를 C7에게 전달해 줌으로 C6과 C7사이에 세션 키를 공유할 수 있다.




[그림 2]

3.2.4 키 추가

센서 네트워크의 존속 기간 동안 센서들이 추가되거나 손상되는 경우가 발생 할 수 있다. 본 논문은 센서가 추가되는 경우만 살펴 보도록 한다. 아래와 같이 두 가지로 분류하여 키의 추가 과정을 살펴보자.

■ 클러스터 내의 센서 노드

새로운 센서를 추가하고자 하면 Base Station은 새로운 센서가 위치하고자 하는 예상 지역의 다항식을 미리 나눠주기만 하면 된다.

■ 클러스터 헤드 노드

새로운 클러스터 헤드가 추가 되고자 하면, Base Station은 키의 사전 분배 과정을 수행한다. 그리고 배치된 센서들에게 새로운 센서와 관련된 상호 키를 안전한 채널을 통해 알려준다.

## 4. 결론

본 논문에서는 센서 네트워크 환경에서의 효율적인 네트워크 구조와 키 분배 방법을 제안하였다. 본 연구는 기존 논문에서 제안 되었던 네트워크 구조를 보완하여 키 설립 확률을 높였을 뿐만 아니라, 클러스터 헤드를 두어 클러스터 간 다항식을 공유 하는 센서의 수를 제한함으로써 키 노출 가능성도 줄일 수 있었다. 제안한 구조는 첫째, 육각의 클러스터 형태로 센서의 target field를 나눔으로써 클러스터 헤드간에 키 설립 확률을 높였다. 둘째, 클러스터에 존재하는 클러스터 헤드간 쓰이는 키와 클러스터 내에 존재하는 센서들이 사용하는 키를 분리 함으로써 보안을 더 향상 시켰다.

[참고 문헌]

[1] 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, pages 471-486, 1993.

[2] D. W. Carman, P. S. Kruus, and B. J. Matt, Constraint and approaches for distributed sensor network security, Technical Report##00-010, NAI Labs, 2000.

[3] L. Eschenauer and V. D. Gligor, A Key-Management Scheme for Distributed Sensor Networks, ACM CCS 2002.

[4] A. Perrig, H. Chan and D. Song, Random Key Predistribution Schemes for Sensor Networks, IEEE S&P 2003.

[5] D. Liu and P. Ning, Establishing Pairwise Keys in Distributed Sensor Networks, ACM CCS 2003.

[6] Donggang Liu and Peng Ning, Location-Based Pariwise Key Establishments for Static Sensor Networks, First ACM Workshop, SASN 2003.