센서 네트워크에서의 안전한 통신을 위한 클러스터 기반 키 분배 구조

천 은 미[†] · 도 인 실[††] · 오 하 영[†] · 박 소 영[††]
이 주 영[†] · 채 기 준[†††] · 이 상 호[†††] · 나 재 훈[††††]

요 약

센서 네트워크는 다양한 환경에 설치되어 대상 탐지나 환경 감시 등, 유용한 정보를 제공하는데 사용될 수 있다. 이러한 센서 네트워크에서 센서 노드 간 키를 설정하는 것은 안전한 통신을 위한 가장 기본적인 요구 사항이다. 따라서 본 논문에서는 센서 네트워크에서의 효율적 키 설정을 위해 클러스터에 기반한 구조와 다항식(polynomial)을 사용한 pairwise key 설정 방법을 제안하였다. 제안한 메커니즘에서는 네트워크를 클러스터링하여 각 클러스터 별로 유일한 다항식을 할당하고, 동일 클러스터에 있는 센서들은 클러스터헤드로부터 분배받은 다항식 부분정보(polynomial share)를 사용하여 자신의 전송 범위에 있는 이웃 노드들과 pairwise key를 생성할 수 있다. 그러나 통신하고자 하는 두 센서가 서로의 전송 범위 내에 있으나 다른 클러스터에 존재할 경우 클러스터헤드를 통하여 두 센서 간의 경로키를 전송하여 공유함으로써 두 센서는 안전하게 통신할 수 있다. 경로키의 수가 많아지는 경우 오버헤드가 높아지므로 경로키 수가 적을수록 유리한데, 그 수는 클러스터의 크기, 센서 노드의 수, 센서의 전송 범위, 센서의 밀집도에 따라 다르게 나타나고 시간도 이에 따라 다르기 때문에 적절한 조건을 제공함으로써 경로키 설정을 줄일 수 있다. 따라서 적절한 클러스터 크기와 센서의 전송 범위를 고려하면 제안한 메커니즘의 효율성을 더욱 높일 수 있음을 시뮬레이션을 통해서 확인할 수 있었다.

키워드 : 센서 네트워크, 보안, 클러스터, 키 설정

Cluster-based Pairwise Key Establishment in Wireless Sensor Networks

Eunmi Chun[†] · Inshil Doh[††] · Hayoung Oh[†] · Soyoung Park[††]
Jooyoung Lee[†] · Kijoon Chae[†††] · Sang-Ho Lee[†††] · Jaehoon Nah[††††]

ABSTRACT

We can obtain useful information by deploying large scale sensor networks in various situations. Security is also a major concern in sensor networks, and we need to establish pairwise keys between sensor nodes for secure communication. In this paper, we propose new pairwise key establishment mechanism based on clustering and polynomial sharing. In the mechanism, we divide the network field into clusters, and based on the polynomial-based key distribution mechanism, we create bivariate polynomials and assign unique polynomial to each cluster. Each pair of sensor nodes located in the same cluster can compute their own pairwise keys through assigned polynomial shares from the same polynomial. Also, in our proposed scheme, sensors, which are in each other's transmission range and located in different clusters, can establish path key through their clusterheads. However, path key establishment can increase the network overhead. The number of the path keys and time for path key establishment of our scheme depend on the number of sensors, cluster size, sensor density and sensor transmission range. The simulation result indicates that these schemes can achieve better performance if suitable conditions are met.

Key Word : Sensor Network, Security, Cluster, Key Establishment

1. 서 론

센서 네트워크는 유비쿼터스(ubiquitous) 컴퓨팅 구현을 위한 기반 네트워크로 초경량, 저전력의 많은 센서들로 구성된 무선 네트워크이다. 유비쿼터스 컴퓨팅 개념의 도입과 함께 이를 실생활에 적용시킬 수 있는 방안이 활발하게 연구되는 가운데 현실적인 유비쿼터스 환경을 제공해줄 수 있는 센서 네트워크가 주요 이슈로 부각되고 있다. 센서 네트워크는 많은 수의 센서 노드들로 구성되고 센서를 통한 정보 감지 및 감지된 정보를 처리하는 기능을 수행한다. 그러나 센서들을 통해 보다 많은 다양한 정보를 습득하고 처리할 수 있는 반

※ 본 논문은 정보통신부 정보통신연구진흥원에서 지원한 ITRC 프로그램 및 한국전자통신연구원 위탁과제의 연구결과입니다.
† 준 회 원 : 이화여자대학교 컴퓨터학과 석사과정
†† 준 회 원 : 이화여자대학교 컴퓨터학과 박사과정
††† 종신회원 : 이화여자대학교 컴퓨터학과 교수
†††† 정 회 원 : 한국전자통신연구원 P2P보안연구팀 책임연구원
논문접수 : 2005년 2월 7일, 심사완료 : 2005년 5월 23일

면, 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 감지된 정보를 안전하게 처리하고 관리할 수 있는 센서 네트워크 상에서의 보안 메커니즘 개발이 반드시 함께 연구되어 적용되어야 한다[6, 7].

따라서 본 논문에서는 센서 네트워크에서 효율적 키 설정을 위한 클러스터 구조와 다항식을 사용한 pairwise key 설정 방법을 제안하였다. 안전한 통신을 위한 직접키 설정을 위해 다항식을 사용하되 이를 공유하는 센서의 수를 줄이고자 클러스터 단위로 다항식을 분배하고, 클러스터헤드에게는 근접 노드와의 키를 사전에 분배하는 방식을 조합한 키 분배 구조를 제안한다.

본 논문은 다음과 같은 순서로 구성되어 있다. 1장의 서론에 이어서 2장에서는 기존에 제안된 센서 네트워크를 위한 키 관리 기법을 살펴본다. 3장에서는 기존의 키 사전 분배 방식의 문제점을 살펴보고 안전한 통신을 위해 본 논문에서 제안한 메커니즘을 살펴본다. 4장에서는 제안하는 메커니즘의 안전성 분석 및 성능평가를 위한 시뮬레이션 환경과 시나리오를 설명하고 그 결과를 분석한 후, 5장에서는 본 논문의 결론과 향후 연구 방안에 대하여 기술한다.

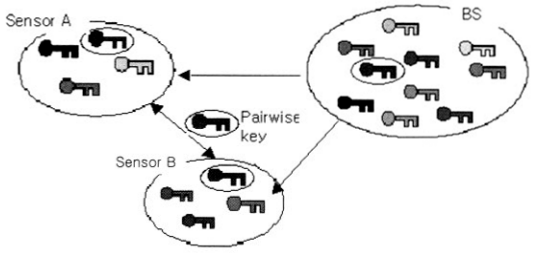
2. 센서 네트워크에서의 키 관리 기법

이 장에서는 센서 네트워크에서의 키 관리 구조로서 센서 노드 간에 안전한 통신을 위해 키를 생성하고 분배하고 갱신하는 키 관리 연구 분야에 대해 살펴보겠다. 센서 네트워크 환경에서 센서 노드가 위험 지역에 설치된 경우 보안성은 특히 중요한데, 이를 위해 주로 센서 네트워크에 적합한 방식의 키 생성, 분배, 갱신에 관한 프로토콜들이 제안되고 있다.

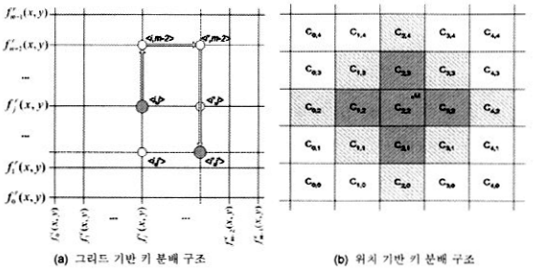
2.1 랜덤키

L. Eschenauer, V. Gligor가 센서 네트워크에서의 안전한 통신을 지원하기 위해 센서 노드 간 pairwise key 설정 프로토콜을 제안하였다[1]. (그림 1)과 같이 베이스 스테이션은 다량의 랜덤 키를 생성하여 이를 키 풀(pool)에 저장하고 키 풀에서 무작위로 임의의 키 셋을 선택하여 각 센서 노드에게 분배한다. 센서 노드 A, B는 부여받은 키 셋에서 서로 공유되는 키를 두 노드 간의 pairwise key로 사용하고 서로 공유하는 키가 없는 두 센서 노드들은 경로키를 생성하여 pairwise key로 사용한다.

H. Chan, A. Perrig, D. Song은 센서 네트워크에서의 키 설정을 위한 노드 사이에 q개의 키를 공유하는 q-composite 스킴을 제안하였는데 해쉬 함수나 XOR 방식을 통한 새로운 키 생성 방식은 기존의 노드 간의 통신을 위한 키 분배 방식보다 노드가 공격을 당했을 때의 통신 채널의 보안성을 높일 수 있는 장점을 가진다[2].



(그림 1) 랜덤키 분배 구조



(그림 2) 다항식 기반 키 분배 구조

$$K = hash(\ k1 \ || \ k2 \ || \ . \ . \ . \ ||kq\ )$$

2.2 다항식 기반 키 분배 구조

D. Liu, P. Ning은 센서 노드 간 pairwise key 설정 프로토콜로서 다항식을 이용한 그리드 기반 키 분배 구조를 제안하였다[3]. 기존 스킴과의 두드러지는 차이점은 실제 키 값을 센서 노드들에게 할당하는 것이 아니라 키를 유도할 수 있는 다항식을 생성하여 분배한다는 것이다. 임의의 두 센서 노드가 동일한 t차 다항식을 공유하면 두 노드는 그 다항식으로부터 서로 공통되는 키 값을 유도할 수 있다.

(그림 2)의 (a)와 같이 동일한 행 또는 열에 위치한 노드들은 서로 간에 pairwise key를 바로 생성할 수 있다. 동일한 행 i에 있는 임의의 두 노드는 i행에 부여된 다항식을, 동일한 열 j에 위치한 임의의 두 노드는 j열에 부여된 다항식을 공통적으로 갖고 있기 때문이다. 즉, 임의의 두 노드에 대해서, 한 노드는 $<c_i, r_i>$에 위치하고, 다른 노드는 $<c_j, r_j>$에 위치할 때, $c_i = c_j$ 이면, 두 노드는 $f^{c}_{c_i}(x, y)$를 공통적으로 공유하고, $r_i = r_j$이면, 두 노드는 $f^{r}_{r_i}(x, y)$를 공유함으로써 각 센서의 ID를 이용하여 공유키를 설정할 수 있다.

D. Liu, P. Ning이 제안한 또 다른 다항식 기반 키 분배 방식은 위치 기반(location-based) pairwise key 설정 프로토콜이다[4]. 그리드 기반 키 분배 구조에서 사용하였던 방식처럼 다항식을 분배하는데, 그리드 방식이 i행 j열에 있는 센서 노드에게 두개의 다항식을 배분하였다면 여기서 제안하는 방법은 (그림 2)의 (b)와 같이 센서 필드를 셀 단위로 나누고 그 셀과 고유한 다항식을 연관시킨다. 그리하여 특정 셀에 위치하고자 하는 센서는 그 위치에 해당하는 다항식과 그 셀 인접 4개 셀에 해당하는 4개의 다항식이 할당되어 이웃 4개 셀에 배치된 센서와 pairwise key를 생성한다[8].

3. 클러스터 기반 키 분배 메커니즘

본 장에서는 키 노출시 네트워크에 끼치는 영향을 최대한 줄이기 위해 다항식을 이용한 클러스터 기반 키 분배 메커니즘을 제안한다. 센서 노드들은 클러스터링되어 있고 각 클러스터는 클러스터헤드를 가지며 클러스터헤드 간에는 비밀키를 공유하고 있다. 클러스터 단위로 하나의 다항식을 공유하며 클러스터 내 센서 노드들은 그 다항식을 바탕으로 노드 간 키를 생성하여 공유한다. 우선, 제안 메커니즘의 구조와 가정을 기술한 후 키 분배 메커니즘을 기술한다.

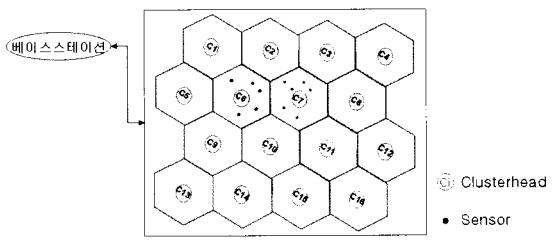
3.1 제안한 메커니즘의 구조와 가정

본 논문은 센서 네트워크의 영역을 육각형 모양의 클러스터 형태로 나눈다. 센서 네트워크의 구성 요소로는 베이스 스테이션과 클러스터헤드, 클러스터에 존재하는 센서들로 구성되어 있다. 베이스 스테이션은 모든 정보를 수집하여 전달하는 게이트웨이 역할을 한다. 클러스터헤드는 클러스터의 정중앙에 위치하고 클러스터 당 하나씩 존재한다. 제안한 메커니즘에서 사용되는 표기법은 <표 1>과 같다.

〈표 1〉 제안 메커니즘에서 사용되는 표기법

Ci	클러스터 영역, 클러스터헤드 식별자
Ni	센서 식별자
Ka,b	노드 a, b사이의 비밀 키
$EK\{\}$	키 K를 사용한 대칭 암호화 함수
$\|\|$	연결(concatenation) 연산자

클러스터헤드의 전송 범위는 클러스터 영역을 포함한다고 가정하고 클러스터 내 센서들의 전송 범위는 임의로 변화를 주었다. 센서들은 자신의 전송 범위에 있는 이웃 노드들과 클러스터헤드로부터 분배받은 다항식 부분정보를 사용하여 pairwise key를 생성할 수 있다. 단, 임의의 두 센서가 동일 클러스터 내에 위치할 경우에는 직접키를 생성하여 pairwise key로 사용하고, 서로 다른 클러스터에 포함될 경우에는 경로키를 생성하여 pairwise key로 사용한다. 또한 제안 모델에서는 센서 네트워크는 애드혹 네트워크만큼 이동성이 크지 않다고 가정한다. 제안한 메커니즘의 기본 구조는 다음 (그림 3)과 같다.



(그림 3) 제안한 센서 네트워크 구조

3.2 제안한 키 관리 메커니즘

제안하는 키 관리 메커니즘은 기존에 제안되었던 다항식 사전 분배 방식을 응용한다[5]. 기본적인 다항식 기반 방법은 키를 생성하고 분배하는 키 셋업 서버가 단 하나의 다항식만을 생성하여 사용하게 되는데 이 다항식이 노출되는 경우 전체 센서 네트워크의 안전성이 보장되지 않는 문제점이 있다. 또한, 센서 노드의 개수가 많아질수록 다항식의 차수가 높아져야 하는데 다항식의 차수가 높아지면 상대적으로 각 센서 노드들이 저장해야 하는 계수의 개수도 증가한다. 그러나 센서 노드의 저장 공간의 제약으로 다항식의 차수를 높이는데 한계가 있으므로 다수의 다항식을 생성하여 사용할 필요가 있다. 이를 위해 공유하는 다항식 풀을 두어 풀에서 공통된 다항식을 찾는다. 하지만 다항식 풀에서 다항식을 선택할지라도 공통된 다항식이 존재하지 않을 확률이 높을 뿐만 아니라 다항식 풀의 크기가 키 설정 확률에 영향을 끼치게 된다. 풀 크기에 따라 키 설정 확률이 변하는 것은 랜덤키 기반 키 분배 구조도 동일하게 갖는 문제점이다[1], [3]. 또한 다항식을 이용한 그리드 기반 방식은 다항식이 노출될 경우 이 좌표에 할당된 다항식을 사용하는 모든 센서들이 노출되는 문제점이 있고, 위치 기반 방식은 공통의 다항식을 5개의 셀에 위치하는 센서들이 공유함으로써 다항식이 노출될 때 이에 따라 노출되는 센서의 수가 많아지는 문제점이 있다[3], [4].

따라서 제안하는 메커니즘은 하나의 다항식을 공유하는 센서 네트워크 영역을 하나의 클러스터로 제한하여 다항식을 공유하는 센서의 수를 제한하여 향상된 보안 효과를 기대할 수 있다. 같은 클러스터 영역에 있는 센서들 중 자신의 전송 범위에 있는 센서들은 공통의 다항식을 사용하고 서로의 ID를 이용하여 pairwise key를 만들 수 있어 키 풀 크기에 상관없이 직접키를 설정할 수 있다. 또한 클러스터 내의 센서들은 클러스터에 배치되면 그 후에 클러스터헤드로부터 다항식 부분정보를 분배받기 때문에 기존의 방법보다 사전에 분배해야 하는 정보의 양을 줄일 수 있다. 센서가 다른 클러스터 영역에 있어서 경로키를 만들어야 하는 경우도 클러스터헤드 간의 키는 센서가 배치되기 전에 미리 분배되어 있으므로 클러스터헤드를 통하여 안전하게 경로키를 다른 클러스터에 있는 센서 노드에게 전달할 수 있다.

3.2.1 사전 키 분배

센서 네트워크의 영역을 $s = n \times n$ 육각 클러스터로 구획을 나누어 베이스 스테이션은 임의의 s개의 다항식을 생성한다. (그림 4)에서 베이스 스테이션은 $C6$의 이웃에 위치하고 있는 6개의 클러스터헤드 $C1$, $C2$, $C5$, $C7$, $C9$, $C10$과의 키 $K_{C6,C1}$, $K_{C6,C2}$, $K_{C6,C5}$, $K_{C6,C7}$, $K_{C6,C9}$, $K_{C6,C10}$을 생성하여 클러스터헤드 노드에게 미리 분배한다. 또한 베이스 스테이션은 소수 q에 대하여 유한체 F_q 상에서 임의의 t차 이변(bivariate) 다항식을 아래와 같이 생성한 후 각 클러스터헤드에게 임의의 다항식을 선택하여 분배한다.

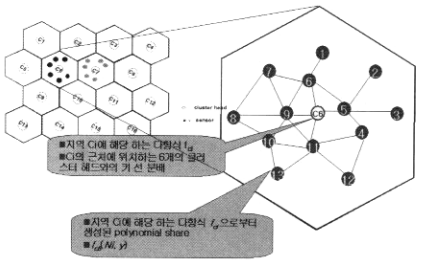
$$f_{Ci}(x, y) = \sum_{i,j=0}^{t} a_{ij}\, x^i y^j$$

단, 이 다항식은 $f_{Ci}(x, y) = f_{Ci}(y, x)$의 성질을 만족해야 한다. 클러스터헤드 Ci에게 분배된 다항식을 $f_{Ci}(x, y)$라고 한다.

임의의 클러스터 영역에 센서들이 임의로 배치되면 클러스터 헤드는 자신의 클러스터에 존재하는 센서들의 존재 여부를 파악한 후 이 센서들에게 다항식에서 생성된 다항식 부분정보를 분배한다. 예를 들어 클러스터헤드 Ci는 해당하는 클러스터에 위치하는 모든 센서들에게 다항식 $f_{Ci}(x, y)$로부터 생성된 다항식 부분정보를 생성하여 분배하는데, 노드 Ni에게 분배되는 다항식 부분정보는 $f_{Ci}(Ni, y)$이다.

3.2.2 직접키 설정

3.2.1에서와 같이 임의의 영역에 배치되어 다항식 부분정보를 분배받은 각 센서들은 Hello 메시지를 통해 주위 노드에게 자신의 존재를 알린다. (그림 4)에서와 같이 Hello 메시지를 수신한 센서가 메시지를 보낸 센서의 전송 영역 내에 위치하고, 두 센서가 같은 클러스터에 존재하면 공통의 다항식으로부터 생성된 다항식 부분정보를 사용하여 통신하고자 하는 센서 사이에 pairwise key를 생성하여 통신한다.



(그림 4) 직접키 설정

• 센서 대 센서

동일한 클러스터 Ci에 위치하는 임의의 두 센서 Ni, Nj가 pairwise key를 생성하는 방법은 다음과 같다. Ni는 $f_{Ci}(Ni, y)$를 갖고 있고, Nj는 $f_{Ci}(Nj, y)$를 갖고 있다. Ni는 Nj의 ID를 이용하여 $f_{Ci}(Ni, Nj)$를 생성하고 Nj는 Ni를 이용하여 $f_{Ci}(Nj, Ni)$를 생성할 수 있다. 앞에서 가정한 다항식 $f_{Ci}(x, y)$의 성질에 따라 $f_{Ci}(Ni, Nj) = f_{Ci}(Nj, Ni)$ 이므로 두 센서 노드는 동일한 직접키를 생성하여 공유할 수 있다.

• 센서 대 클러스터헤드

센서와 클러스터헤드가 통신을 하고자 하면 센서뿐만 아니라 클러스터헤드도 다항식을 이미 알고 있으므로 해당 지역에 할당된 다항식을 이용하여 서로 간의 키를 계산하여 사용할 수 있다.

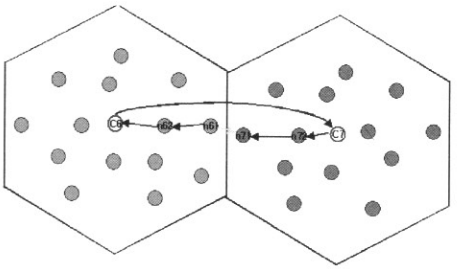
• 클러스터헤드 대 클러스터헤드

클러스터헤드는 자신과 이웃하는 지역의 클러스터헤드들 간의 pairwise key를 이미 알고 있으므로 이 키를 직접키로 사용한다.

3.2.3 경로키 설정

• 센서 대 센서

통신하고자 하는 센서들이 서로 물리적 전송 범위에 있으나 논리적인 전송영역이 다른 경우 즉, 두 센서가 다른 클러스터에 존재할 경우에는 경로키를 생성한다. 이는 클러스터의 경계에 두 센서가 존재하게 되는 경우로 두 센서가 소유하고 있는 다항식이 다르기 때문에 직접키를 설정할 수 없다. 통신을 요청한 센서는 임의의 값을 경로키로 설정하여 클러스터헤드를 통해 통신하고자 하는 센서에게 전달함으로써 두 센서는 경로키를 pairwise key로 사용한다. 다음 (그림 5)의 예를 살펴보도록 하자.



(그림 5) 경로키 설정

Initialization : N61 ⟶ broadcast Hello message

ID_{N61} || $source\_id(ID_{N61})$ || $dest\_id(all)$ || $data(Hello\ message)$

N61은 자신의 전송 범위에 있는 센서 노드에게 Hello message를 브로드캐스팅 한다.

case 1. 상대 노드가 N61의 전송영역에 있고 N61과 클러스터 영역이 같은 경우
: N61과 상대 노드 N62는 공통의 다항식으로부터 생성된 다항식 부분정보를 사용하여 직접키를 설정한다.

case 2. 상대 노드가 N61의 전송영역 안에 있으나 클러스터 영역이 다른 경우
: N61과 상대 노드 N71은 서로 다른 클러스터에 해당하므로 경로키를 설정한다.

• 경로키(*path key*) 설정 과정

step 1 : N61 ⟶ C6

ID_{N61} || $source\_id(ID_{N61})$ || $dest\_id(ID_{N71})$ || $E_{fC6}\{path\_key\}$

N61과 N71은 직접키를 설정할 수 없으므로 경로키를 생성한다. N61은 생성된 경로키를 C6과 다항식을 사용하여 생성한 키로 암호화한 후 브로드캐스트하여 N62를 거쳐 C6에게 전달한다.

step 2 : C6 ⟶ C7

ID_{C6} || $source\_id(ID_{N61})$ || $dest\_id(ID_{N71})$ || $E_{KC6,C7}\{path\_key\}$

C6은 수신한 경로키를 복호화한다. 복호화한 경로키를 C6과 C7 사이에 미리 분배된 키로 암호화한 후 브로드캐스트하여 C7에게 전달한다.

step 3 : C7 ⟶ N71

ID_{C7} || $source\_id(ID_{N61})$ || $dest\_id(ID_{N71})$ || $E_{fC7}\{path\_key\}$

C7은 경로키를 복호화한다. 경로키를 복호화한 C7은 N71과의 다항식을 사용하여 생성된 키로 경로키를 암호화한 후 브로드캐스트하여 N72를 거쳐 N71에게 전달한다.

step 4 : N71 ⟶ N61 (Confirm message)

ID_{71} || $source\_id(ID_{N71})$ || $dest\_id(ID_{N61})$ || $E_{path\_key}\{confirm\ message\}$

N71은 받은 데이터를 경로키를 복호화하여 경로키를 받게 되고 N61에게 확인 메시지를 전달한다.

제안한 메커니즘은 직접키 및 경로키 생성과정을 통해 센서 노드 간 pairwise key를 설정한다. 직접키 설정에 비해 경로키 설정에는 좀 더 많은 시간이 필요하지만 클러스터 경계상에 있는 노드들만 수행하므로 경로키 설정에 따른 오버헤드를 줄일 수 있다. 경로키가 생성되는 경우는 클러스터의 크기, 센서 노드의 수, 센서의 전송 범위, 센서의 밀집도에 따라 크게 영향을 받으므로 적절한 조건을 제공함으로써 경로키 생성을 줄일 수 있다.

4. 성능 평가

본 장에서는 제안 모델인 클러스터 기반 키 분배 메커니즘을 평가하기 위한 시뮬레이션 모델을 설명하고 그 결과를 분석한다. 4.1절에서는 제안한 메커니즘의 안전성을 분석하고 4.2절에서는 시뮬레이션 환경 및 시나리오를, 4.3절에서는 시뮬레이션 결과를 제시하였다. 4.4절에서는 안정성과 시뮬레이션 결과에 대해 종합적으로 분석하였다.

4.1 안전성 분석

본 절에서는 키 노출 시 네트워크에 끼치는 영향에 대해 기존에 제안된 위치 기반 키 분배 방식에 제시된 분석을 참고로 본 연구에서 제안한 방식의 안전성을 분석한다. 안전성 분석에 사용되는 표기법은 <표 2>와 같다.

• 노드 포획에 대항한 안전성

센서의 전송 범위를 d라고 할 때 네트워크 상의 센서의 밀집도는 다음과 같이 계산된다. $D=\frac{m}{\pi d^2}$ (m : 평균 노드 수)

클러스터는 정육각형이고 육각형 한 변의 길이를 a라고 할 경우, 특정 클러스터에 위치하면서 다항식을 공유할 센서의 수는 $\frac{m^* \frac{3\sqrt{3}a^2}{2}}{\pi d^2}$이다. 전송 범위를 거리를 측정하는 기본 단위라고 할 때(d=1), 같은 다항식을 공유하는 평균 노드 수는 다음과 같다.

$$Ns = \frac{m^* \frac{3\sqrt{3}a^2}{2}}{\pi}$$

〈표 2〉 안전성 분석에 사용되는 표기법

d	센서의 전송 범위
m	평균 노드 수
a	정육각형 클러스터 한 변의 길이
Ns	임의의 클러스터에 위치하면서 다항식을 공유할 센서 수
$Pc(i)$	같은 다항식을 공유하는 센서 중 i개 센서가 노출될 확률
Pc	임의의 클러스터의 다항식이 노출될 확률
t	다항식 차수

공격자에 의해서 네트워크 상에 노출되는 센서의 비율을 P_c라 하면 특정 클러스터에서 같은 다항식을 공유하는 센서 중 i개 센서가 노출될 확률은 다음과 같이 계산된다.

$$P_c(i) = \frac{N_s!}{(N_s - i)!\,i!} p_c^{\,i} (1 - p_c)^{N_s - i}$$

따라서 위 클러스터의 다항식이 노출될 확률은 다음과 같다.

$$p_c = 1 - \sum_{i=0}^{t} p_c(i)$$

제안한 메커니즘은 임의의 t차 이변 다항식을 사용하여 pairwise key를 생성하는데 같은 다항식을 공유하는 센서의 수를 t까지 제한하면 노드가 t개까지 노출되어도 사용되는 다항식을 추측할 수 없어 노드 노출에 대해 완벽하게 대항할 수 있는 안전성을 갖게 된다.

$$Ns = \frac{m^* \frac{3\sqrt{3}a^2}{2}}{\pi} < (t+1)$$

기존의 방법은 다항식을 공유하는 센서가 인접한 셀, 혹은 같은 열과 행에 존재하게 되지만, 제안한 메커니즘은 다항식을 공유하는 센서의 범위를 클러스터 내로 한정함으로 t의 수를 기존 방법보다 줄일 수 있고 다항식이 노출된다고 할지라도 노출되는 센서가 클러스터 내로 한정되며 다른 클러스터의 노드에게 영향을 끼치지 않는다.

4.2 시뮬레이션 환경 및 시나리오

제안한 메커니즘은 클러스터 별로 다항식을 분배하기 때문에 클러스터 내에 있는 센서들은 pairwise key를 생성하여 안전한 통신을 할 수 있다. 하지만 통신하고자 하는 두 센서가 서로의 전송 범위에 존재하나 다른 클러스터 영역에 있게 되면 경로키를 설정해야 하며 이때 영향을 미치는 경로키 수와 시간에 의해 제안한 메커니즘의 효율성을 평가할 수 있다. 본 논문을 위한 경로키 수 구현은 C언어를 사용하였고 경로키 생성 시간은 NS-2 시뮬레이션 툴[8]을 Linux 9.0에서 수행하여 측정하였다.

• 경로키 수

센서 네트워크의 경로키 수는 센서의 수와 클러스터의 크기, 센서 노드의 전송 범위 및 센서의 밀집도에 의존적이다. 경로키 수를 최소화하기 위한 센서의 수와 클러스터의 크기, 센서 노드의 전송 범위 및 센서의 밀집도를 구한다. 경로키

수를 구하기 위해서 배열을 이용하여 센서 네트워크 필드를 구성한 후, 클러스터 반경과 센서의 전송 범위, 센서 수를 파라미터로 하여 경로키 수를 측정하였다.

〈표 3〉 시뮬레이션에서 사용하는 파라미터

파라미터	수준
Area	200m × 200m / 500m × 500m
Radio Range	10m, 20m, 30m
Placement	randomly
Movement	static
MAC	802.11
Number of nodes	50~500 nodes
Simulation Time	150s

• 경로키 설정 시간

경로키 설정 시간도 역시 센서의 수와 클러스터의 크기, 센서 노드의 전송 범위 및 센서의 밀집도에 의존적이다. 하나의 경로키를 설정하는데 걸리는 시간을 최소화하기 위한 센서의 수와 클러스터의 크기, 센서 노드의 전송 범위 및 센서의 밀집도를 구한다. 같은 전송 영역에 있으나 서로 다른 클러스터에 포함된 영역에 있는 센서 간 경로키를 설정하는데 걸리는 시간을 측정하기 위한 NS-2 네트워크 시뮬레이션 환경은 <표 3>과 같다.

4.3 시뮬레이션 결과

4.3.1 센서 네트워크 필드의 크기가 200m × 200m일 경우 경로키 수

(그림 6)의 (a)에서 센서의 전송 범위가 10m일 때 센서의 전송 범위와 클러스터 반경과 유사한 경우부터 클러스터의 반경을 증가시키면서 경로키 개수를 측정하였다. 센서 수가 일정할 경우 대체적으로 클러스터 반경이 커질수록 경로키 수가 적어진다. (b)는 클러스터 반경이 50m로 일정하고 센서 수가 200개로 일정할 때 센서의 전송 범위가 작을수록 경로키 수가 적게 생성됨을 나타낸다. (c)는 센서 수가 200개로 고정될 경우 클러스터 반경이 50m일 때 센서의 전송 범위를 증가시키면서 경로키 생성 수를 살펴본 것으로 센서의 전송 범위가 작을수록 경로키가 적게 생성됨을 나타낸다. 또한 센서 수와 센서의 전송 범위가 일정할 때 클러스터 반경을 증가시키면 경로키가 적게 생성된다.

따라서 센서 네트워크 필드가 200m×200m일 경우, 첫째, 전송 범위가 일정할 경우 고정된 센서 수에서 클러스터 반경을 증가시키면 경로키 수가 적게 생성되고, 고정된 클러스터 반경에서 센서 수를 증가시키면 경로키가 많이 생성된다. 둘째, 클러스터 반경이 일정할 경우 고정된 센서 수에서 센서의 전송 범위가 작아야 경로키가 적게 생성되고, 고정된 센서 전송 범위에서 센서 수를 증가시키면 경로키가 많이 생성된다. 셋째, 센서 수가 일정할 경우, 고정된 센서의 전송 범위일 경우 클러스터 반경이 커질수록 경로키는 적게 생성되고, 고정된 클러스터 반경일 경우 센서의 전송 범위가 작아야 경로키 수가 적게 생성된다.

4.3.2 센서 네트워크 필드의 크기가 200m×200m와 500m×500m일 경우 경로키 수

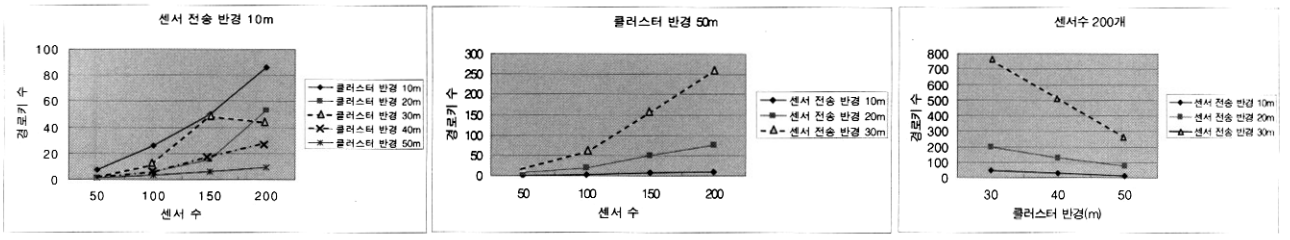
(그림 7)은 클러스터 반경이 50m로 일정하고 센서가 같은 전송 반경 10m이며 센서 수가 200개일 경우, 센서 필드가 500m × 500m인 경우가 200m × 200m보다 밀집도가 떨어져 경로키 수가 적음을 나타낸다.

4.3.3 센서 네트워크 필드의 크기가 200m × 200m일 경우 경로키 생성 시간

(그림 8)의 (a)는 4.3.1과 같은 조건에서 경로키 생성 시간을 측정하였다. 클러스터 반경이 일정할 때에는 센서 수의 변화와 상관없이 경로키 생성 시간이 거의 일정함을 보이고 센서 수가 일정할 때 클러스터의 반경이 커질수록 경로키 생성 시간도 오래 걸림을 알 수 있다. (b)에서는 센서 수를 200개로 고정시킬 경우 클러스터 반경이 일정할 때 센서의 전송 범위를 증가시키면 경로키 생성 시간이 적게 걸림을 알 수 있었고 센서의 전송 범위가 일정할 때는 클러스터 반경이 작을수록 시간이 적게 걸림을 알 수 있다. 경로키를 생성하는데 필요한 오버헤드는 (c)와 같이 센서 전송 반경이 일정할 때 클러스터 반경이 클수록 작게 나타나고 클러스터 반경이 일정할 때 전송 반경이 작을수록 작게 나타난다. 따라서 전송 반경이 10m이면 클러스터 반경이 50m인 경우가 가장 오버헤드가 작게 나타남을 알 수 있다.

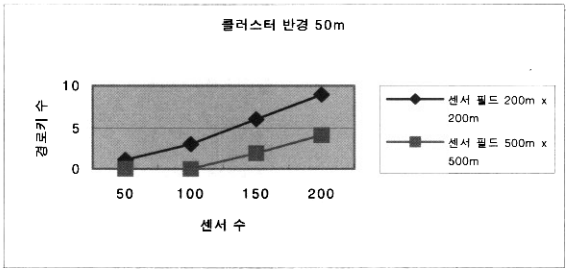
4.4. 결과 분석

안전성 분석과 시뮬레이션 결과를 종합하여 제안한 메커니즘을 분석해보면 기존에 제안된 방식과 달리 다항식의 사용 영역을 클러스터 내로 한정하여 다항식이 노출되어도 이 다항식을 사용하여 노출되는 센서 수가 특정 클러스터 영역 내로 한정되므로 기존의 방법보다 좀 더 안전함을 알 수 있고,

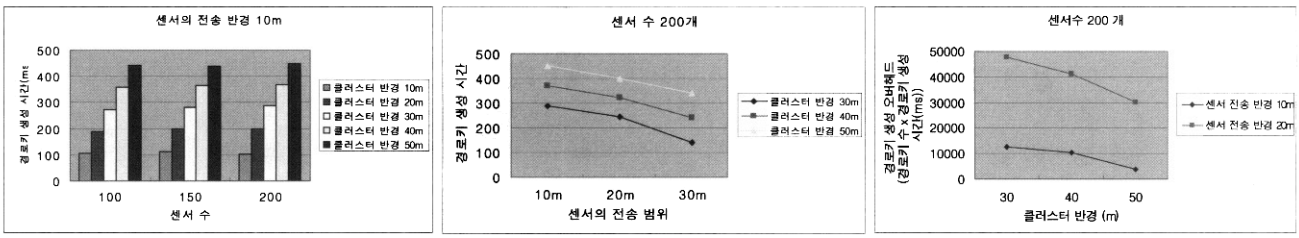


(a) 센서 전송 반경이 일정할 때 경로키 수 (b) 클러스터 반경이 일정할 때 경로키 수 (c) 센서수가 일정할 경우 경로키 수

(그림 6) 경로키



(그림 7) 밀집도에 따른 경로키 수



(a) 센서 전송 반경이 일정할 때 경로키 생성시간 (b) 센서 수가 일정한 때 경로키 생성시간 (c) 전체 경로키 생성 오버헤드

(그림 8) 경로키 생성 시간

통신하고자 하는 센서들이 서로 이웃해 있으나 다른 클러스터에 존재할 경우, 두 노드 간에 사용할 경로키를 각각의 클러스터헤드를 통해 통신하고자 하는 상대방 센서에게 전달함으로써 상호간 안전한 통신이 가능하도록 하였다. 이와 같이 경로키가 생성되는 경우는 클러스터의 크기, 센서 노드의 수, 센서의 전송 범위, 센서의 밀집도의 따라 다르게 나타나고 시간도 이에 따라 다르기 때문에 적절한 조건이 필요하다. 시뮬레이션을 통해서 클러스터 크기가 커질수록, 센서의 전송 범위가 작을수록, 또한 센서의 밀집도가 작을수록 전체 경로키 수가 적어짐을 알 수 있었다. 또한 경로키 하나를 생성하는데 걸리는 시간은 전송 범위가 일정할 때 클러스터 크기가 작을수록, 클러스터 크기가 일정할 때 전송 범위가 커질수록 짧게 걸렸다. 하지만 경로키를 생성하는데 드는 오버헤드는 센서의 전송 반경은 작고 클러스터 반경이 커야 작아졌다. 따라서 제안한 메커니즘은 적절한 클러스터 크기와 센서의 전송 범위를 고려하면 효율성을 높일 수 있을 뿐만 아니라 기존 방식보다 여러 가지 장점을 갖게 되는데 이를 정리하면 <표 4>와 같다. 즉, 기존에 제안되었던 랜덤키 기법이나 풀기반 t차 다항식 기법과 비교했을 때 제안 메커니즘의 pairwise key 설정 확률은 항상 1이다. <표 4>에서와 같이 랜덤키 기법이나 풀 기반 t차 다항식을 사용하는 경우 pairwise 키 설정 확률이 0.99라고 되어있지만 이것은 키 풀 크기에 따라 그 확률이 더 낮아질 수도 있다. 제안한 메커니즘은 랜덤키 분배 방식과 달리 t차 이변 다항식으로부터 키를 유도하기 때문에 키를 사용하는 노드가 t개까지 노출되어도 키를 유도한 다항식이 공개 되지 않아 안전하다. 또한 제안한 메커니즘은 기존의 다항식기반 방식과 달리 t의 범위를 하나의 클러스터로 제한함으로 안전성을 더욱 높일 수 있다. 뿐만 아니라 기존의 방법은 센서가 네트워크에 배치되기 전에 모든 센서에게 키를 사전에 분배해야 했지만 제안한 기법은 클러스터헤드에게만 키를 사전에 분배하면 되므로 부가적인 작업을 줄일 수 있다.

〈표 4〉 기존 연구와의 비교

비교항목	랜덤키 (pool 기반)	다항식 (pool 기반)	다항식 (그리드 기반)	다항식 (위치 기반)	제안한 메커니즘
Pairwise key 설정 확률	0.99	0.99	1	1	1
키 유도 방식	키	t차 이변 다항식	t차 이변 다항식	t차 이변 다항식	t차 이변 다항식
안전성(최대 노출키 수)	1	t+1	t+1	t+1	t+1
키 노출 피해 범위	동일키 공유 센서	동일 다항식 공유 센서	행, 열	5개 클러스터	1개 클러스터
키 갱신 오버헤드	전체 네크워크	전체 네크워크	행, 열	5개 클러스터	1개 클러스터
키 사전 분배	모든 센서	모든 센서	모든 센서	모든 센서	클러스터 헤드
센서 저장 오버헤드	다수개의 키	다수의 다항식 부분정보	2개의 다항식 부분정보	5개의 다항식 부분정보	1개의 다항식 부분정보
센서의 키 계산 오버헤드	없음	이웃 노드수 X 다항식 부분정보 계산량	이웃 노드수 X 다항식 부분정보 계산량	이웃 노드수 X 다항식 부분정보 계산량	이웃 노드수 X 다항식 부분정보 계산량

5. 결 론

센서 네트워크에 적합한 키 분배 방식은 대칭키를 기반으로 하되 적은 수의 키로 효과적으로 pairwise key를 생성할 수 있는 방법이어야 한다. 이를 위해 본 논문에서는 센서 네트워크에서의 효율적 pairwise 키 설정을 위한 클러스터 기반 키 분배 방법을 제안하였다. 안전한 통신을 위한 직접키를 설정하기 위해 다항식을 사용하되 이를 공유하는 센서의 수를 줄이고자 클러스터 단위로 다항식을 사전에 분배하고 클러스터헤드에게는 근접 클러스터헤드 노드와의 키를 사전에 분배하는 방식을 조합한 키 분배 구조를 제안하였다. 제안된 방식에서는 이웃 노드와 클러스터 영역이 서로 다른 경우 각각의 클러스

터헤드를 통해 pairwise key를 공유하는 방법으로 모든 노드가 이웃 노드와의 pairwise key를 가짐으로써 안전한 통신을 보장할 수 있다. 그러나 제안한 모델은 클러스터헤드가 안전하다고 가정하였기 때문에 그렇지 않을 경우를 고려한 연구가 필요하며, 본 논문에서는 제안된 메커니즘에 대한 시뮬레이션만을 수행하였으므로 기존에 제안된 키 분배 메커니즘과의 시뮬레이션을 통한 비교를 통해 그 효율성을 증명하는 방안이 추가로 연구되어야 할 것이다. 또한 제안한 키 설정 메커니즘을 바탕으로 클러스터헤드를 통한 효율적 라우팅이나 안전한 정보 교환을 위한 인증 방안 등에 대한 향후 연구도 필요하다.

참 고 문 헌

[1] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. 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," IEEE Symposium on Security and Privacy, pp.197-213, 2003.

[3] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," Proc. of the 10th ACM Conference on Computer and Communications Security (CCS), pp.52-61, 2003.

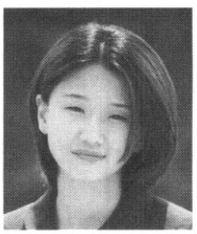
[4] D. Liu, P. Ning, "Location-Based Pairwise Key Establishments for Static Sensor Networks," SASN'03 First ACM Workshop on the Security of Ad Hoc and Sensor Networks, 2003.

[5] 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, pp.471-486, 1993.

[6] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks," IEEE Communications Magazine, 2002.

[7] 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.

[8] "The Network Simulator : ns-2," http://www.isi.edu/nsnam/ns.

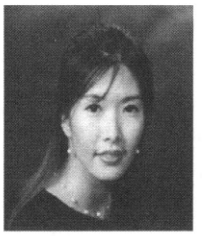


천 은 미

e-mail : emchun@ewhain.net
2002년 동덕여자대학교 전산학과(학사)
2003년~현재 이화여자대학교 컴퓨터학과 석사과정
관심분야 : 네트워크 보안, 센서 네트워크, 홈 네트워크, 유비쿼터스 컴퓨팅

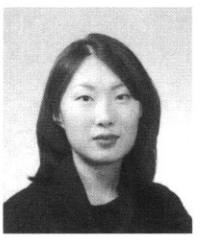
도 인 실

e-mail : isdoh@ewhain.net
1993년 이화여자대학교 전자계산학과(학사)
1995년 이화여자대학교 전자계산학과(석사)
1995년~1998년 삼성 SDS
2002년~현재 이화여자대학교 컴퓨터학과 박사과정
관심분야 : 네트워크 보안, 애드혹 네트워크, 센서 네트워크, 유비쿼터스 컴퓨팅



오 하 영

e-mail : hyoh@ewhain.net
2002년 덕성여자대학교 전산학과(학사)
2001년~2004년 신한금융지주회사 e-신한
2004년~현재 이화여자대학교 컴퓨터학과 석사과정
관심분야 : 네트워크 보안, 센서 네트워크, 홈 네트워크, 유비쿼터스 컴퓨팅, DDos



박 소 영

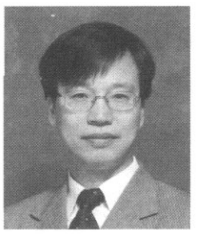
e-mail : soyoung@ewhain.net
1998년 이화여자대학교 컴퓨터학과(학사)
2000년 이화여자대학교 컴퓨터학과(석사)
2000년~현재 이화여자대학교 컴퓨터학과 박사과정
관심분야 : 정보보호, 암호프로토콜, 암호 알고리즘

이 주 영

e-mail : jjoo5021@ewhain.net
2002년 가톨릭대학교 컴퓨터공학과(학사)
2002년~2003년 (주)마이크로인포
2004년~현재 이화여자대학교 컴퓨터학과 석사과정
관심분야 : 정보보호, 암호프로토콜, 센서 네트워크 보안

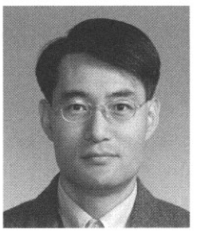
채 기 준

e-mail : kjchae@ewha.ac.kr
1982년 연세대학교 수학과(학사)
1984년 미국 Syracuse University 컴퓨터학과(석사)
1990년 미국 North Carolina State University 컴퓨터공학과(박사)
1990년~1992년 미국 해군사관학교 컴퓨터학과 조교수
1992년~현재 이화여자대학교 컴퓨터학과 교수
관심분야 : 네트워크 보안, 인터넷/무선통신망/고속통신망 프로토콜 설계 및 성능분석, 네트워크 보안, 센서네트워크, 홈 네트워크, 유비쿼터스 컴퓨팅



이 상 호

e-mail : shlee@ewha.ac.kr
1979년 서울대학교 계산통계학과(학사)
1981년 한국과학기술원 전산학과(석사)
1987년 한국과학기술원 전산학과(박사)
1983년~현재 이화여자대학교 컴퓨터학과 교수
관심분야 : 정보보호, 암호프로토콜, 알고리즘 설계, 계산기하, 그래프 드로잉, 데이터 마이닝, Bio-informatics



나 재 훈

e-mail : jhnah@etri.re.kr
1985년 중앙대학교 컴퓨터공학과(학사)
1987년 중앙대학교 대학원 컴퓨터공학과(석사)
1987년~현재 한국전자통신연구원 책임연구원
관심분야 : IPsec, Mobile IP, IPv6. 네트워크 보안