배치정보를 이용한 클러스터 기반 센서 네트워크 키 설정 메커니즘

도 인 실[†] · 채 기 준[††] · 김 호 원[†††]

요 약

센서 네트워크를 실생활에 적용하기 위해서는 보안 서비스가 반드시 같이 제공되어야하며 보안에 있어서 핵심은 노드 간에 안전한 통신을 가능하게 하는 pairwise 키 설정이다. 본 연구에서는 센서 네트워크를 사전에 클러스터링하고 각 클러스터에 헤드를 두어 기본적인 정보는 사전에 예측된 배치정보에 의해 배분하고 노드 배치 후 실제적으로 이웃 노드를 파악하여 정보가 필요한 노드들만이 클러스터헤드에게 해당 정보를 요청하는 메커니즘을 제안한다. 제안 메커니즘은 클러스터헤드가 좀 더 많은 정보를 사전 분배받는 대신 일반 노드의 메모리 부담을 훨씬 줄였으며 불필요한 정보를 분배하지 않음으로써 노드 포획 시에도 이에 대한 저항성을 높여 보안성을 한층 강화할 수 있을 뿐 아니라 모든 이웃 노드 간 직접키 설정을 보장함으로써 효율적인 키 설정과 통신이 가능하다.

키워드 : 센서 네트워크, 키 설정, 클러스터, 배치 정보

Sensor network key establishment mechanism depending on deployment information

Inshil Doh[†] · Kijoon Chae[††] · Howon Kim[†††]

ABSTRACT

For applying sensor networking technology for our daily life, security service is essential, and pairwise key establishment is the key point for security. In this paper, we propose pairwise key establishment mechanism for secure communication in sensor networks. In the mechanism, we cluster the network field before deployment and predistribute key materials to normal sensor nodes and clusterheads. For clusterheads, more key materials are predistributed, and after deployment, sensor nodes which need to establish pairwise keys with other sensor nodes in different clusters make request for related key materials to their own clusterheads. Our proposal reduces the memory requirements for normal sensor nodes by distributing more information to clusterheads, and it raises the security level and resilience against node captures. In addition, it guarantees perfect pairwise key establishments for every pair of neighboring nodes and provides efficient and secure sensor communications.

Key Words : Sensor Networks, Key Establishment, Cluster, Deployment Information

1. 서 론

사용자가 네트워크나 컴퓨터를 의식하지 않고 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 정보통신 환경인 유비쿼터스 컴퓨팅의 중요성이 점차 부각됨에 따라 최근 기반 기술로서의 센서 네트워킹의 중요성 또한 강조되고 있다. 센서 네트워크는 보통 다수의 소형 센서 노드를 필드에 배치하고 이들을 통한 다양한 형태의 자료를 수집하고 분석하는 목적을 가지며 환경 감시, 대상 추적, 환자의 모니터링, 또는 군사적 목적 등에서 매우 다양하게 사용될 수 있다. 그러나 이는 무선 통신의 기본적인 취약점뿐만 아니라 센서 노드 자체의 제약, 즉, 에너지가 제한되어 있고 크기가 작아서 메모리나 처리 능력이 떨어지는 등 여러 가지 문제점 또한 갖고 있다. 특히 노드가 오동작하거나 잘못된 데이터가 주입되는 경우 그 결과는 크게 달라져 정보의 신뢰성이 떨어진다. 단순한 오동작으로 인한 오류가 아니라 의도적인 공격자에 의한 침입이 발생하는 경우, 그 피해는 더욱 커지게 되므로 네트워크의 안전성을 높이고 정보의 신뢰성, 프라이버시 보호 등을 위해 보안 메커니즘이 필요하다. 그러나 앞서 나열한 여러 가지 센서 네트워크의 특성들로 인해 기존의 보안 메커니즘을 그대로 적용할 수 없어 센서 네트

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터(ITRC) 육성·지원사업 및 한국전자통신연구원(ETRI)의 지원을 받아 수행되었음.
† 정 회 원 : 이화여자대학교 컴퓨터학과 박사과정
†† 종신회원 : 이화여자대학교 컴퓨터학과 교수
††† 종신회원 : 한국전자통신연구원 정보보호연구단
논문접수 : 2005년 11월 8일, 심사완료 : 2006년 3월 22일

워크 특성을 고려한 별도의 보안 메커니즘의 연구가 필요하다[1]. 센서 네트워크 보안은 다양한 분야에 있어 연구가 진행되고 있는데 보안 연구에 있어 가장 핵심적인 요소는 역시 키 관리 기법이라 할 수 있다. 센서 노드 간 키가 적절하게 설정되면 이를 통해 인증이나 암호화 등 다양한 보안 기술을 적용할 수 있기 때문이다. 안전한 센서 네트워크 통신을 위한 키 관리 메커니즘은 다양하게 연구되어 왔는데 그 중 한 분야가 센서 노드를 필드에 배치하기 전에 키 혹은 키를 위한 관련 정보를 사전에 배분하는 방법이다. 이 방법은 에너지 제약이 심한 센서 노드가 배치 후 키를 설정하는데 필요한 에너지를 절약할 수 있다는 장점이 있는 반면 센서 노드가 실제로 배치되고 나서 적절한 키를 설정하기 위해서는 많은 양의 키 정보를 가져야하며 이에 따라 보안에 위협이 가해질 수 있다는 문제점을 갖는다. 이를 보완한 방법으로 사전에 배치될 위치를 예상하여 필요한 정보를 적절히 배분하는 메커니즘들이 제안되었는데 이 또한 상당 부분 불필요한 정보를 배분받고 그로 인해 보안상 취약성이 높아질 수 있다는 단점을 갖는다. 본 논문에서는 이를 좀 더 보완하기 위하여 네트워크 필드를 클러스터링하고 각 클러스터에 배치될 센서 노드의 위치정보를 이용하여 키정보를 배분하되 일반 노드에 비해 좀 더 계산과 저장 능력이 뛰어난 클러스터헤드에게 필요한 정보를 배분함으로써 일반 센서 노드의 부담을 줄이고 보안성을 더 높이며 오버헤드를 낮출 수 있는 방법을 제안한다.

본 논문은 다음과 같은 순서로 구성되어 있다. 1장의 서론에 이어서 2장에서는 관련 연구에 대해 간단히 살펴본 다음, 3장에서는 제안하는 키 설정 메커니즘을 설명한다. 4장에서는 제안하는 메커니즘의 효율성과 오버헤드를 분석한 후, 5장에서는 본 논문의 결론과 향후 연구 방안에 대하여 기술한다.

2. 관련 연구

센서 네트워크를 위한 여러 가지 키 설정 메커니즘이 제안되었다. 그 중 대표적인 것을 살펴보면 다음과 같다.

Eschenauer와 Gligor는 랜덤 키 선분배 방식[3]에서 각 센서 노드가 필드에 배치되기 전에 공통되는 키 풀에서 키를 일정 수만큼 분배받고 필드에 배치된 후 이웃 노드와의 공통키를 찾아 이를 pairwise 키로 사용하는 방식을 제안하였다. Chan 등은 이 방식을 좀 더 발전시켜 pairwise 키를 설정해야하는 두 노드가 최소 $q(q>1)$개 이상의 키를 공유해야하고 q개 키의 연산을 통해 새로운 키를 만들어 사용하는 방법[4]을 제안하였다. Du 등은 Eschenauer와 Gligor에 의해 제안된 기본 스킴[3]에 Blom의 키관리 스킴[2]을 조합한 키분배 방식[5]을 제안하였고, Liu와 Ning은 Blundo가 제안한 다항식 기반 키 분배 프로토콜[7]을 적용한 키분배 방식[8]을 제안하였다. Du 등은 센서 노드의 배치 정보를 이용한 키 선분배 메커니즘을 최초로 제안하였는데 이는 센서 필드를 $t * n$ 개의 그룹으로 나눈 다음 키 풀을 오버랩되는 요소 a와 b에 따라 서브키 풀로 나누고 센서 노드가 배치될 위치에 따라 오버랩 요소의 비율을 고려하여 키를 사전 분배하는 방식이다. Yu 등은 Blom의 키분배 스킴[2]을 기반으로 센서 필드를 육각 모양의 그리드로 그룹화한 후 각 그룹에 포함될 센서의 배치 정보를 이용한 키의 사전 분배 방안[9]을 제안하였다. 이는 본 연구의 성능 평가 시 비교 대상이 되므로 3.2.2.1 절에서 좀 더 소개하도록 한다. 그밖에 H. Chan과 A. Perrig는 PIKE[10]라는 메커니즘에서 각 센서 노드가 가지는 대칭 키의 수를 줄이기 위한 방법으로 n개의 센서 노드를 $\sqrt{n}*\sqrt{n}$개의 좌표로 나누고 두 노드가 pairwise 키를 설정하기 위해 공통되는 x, 혹은 y 좌표에 위치한 노드를 이용하는 방법을 제안하였으며, M. Chorzempa 등은 센서 네트워크를 다중의 계층을 가진 구조로 정의하고 키 풀을 여러 개의 서브키 세트로 나누고 다시 이 세트의 원소 중 서로 다른 조합의 키를 적절히 할당하는 방법을 제안하였다[11].

3. 키 설정 메커니즘

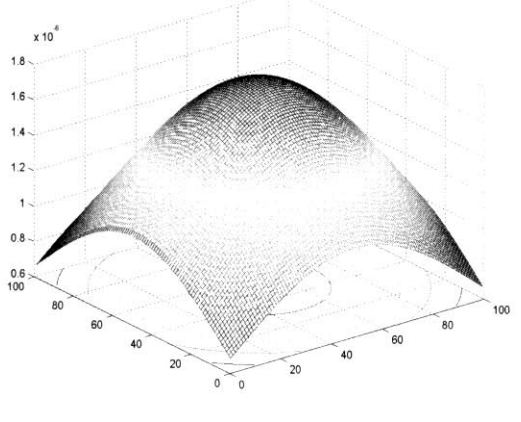
3.1. 네트워크 모델

제안 메커니즘을 위한 기본 가정 사항은 다음과 같다.

- 센서 노드는 이동성이 없다고 본다.
- 클러스터헤드는 일반 센서 노드보다 저장, 계산 능력이 더 뛰어나고 에너지 수명도 길며, 센서 노드가 배치된 후 위치는 가능한 한 배치 중심에 가까이, 최소한 클러스터의 영역 내에 존재한다고 가정한다.
- 클러스터헤드는 일반 노드에 비해 좀더 높은 정도의 보안이 적용된다.

센서 네트워크 영역은 노드 배치 전에 클러스터링되고, 클러스터 내에서는 평면상의 센서 노드의 위치를 2차원 가우시안 분포로 모델링한다. 즉, (x, y)는 각 센서 노드의 좌표이며 배치 중심 (x_i, y_i)를 중심으로 가우시안 분포(정규분포)를 따라 분포된다고 가정한다.

$$f_i(x,y) = \frac{1}{2\pi\sigma^2} e^{-[(x-x_i)^2+(y-y_i)^2]/2\sigma^2}$$



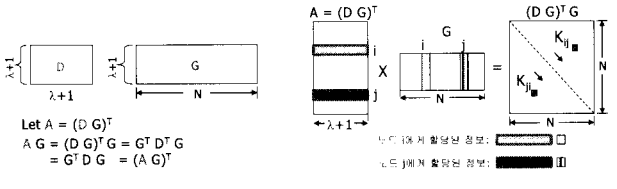
(그림 1) 가우시안 분포에 따른 센서 노드 배치 모델

이때, σ는 표준 편차 값이며 클러스터헤드의 위치는 배치 중심점(x_i, y_i) 가까이에 위치한다. (그림 1)은 하나의 클러스터에 대해 가우시안 분포에 의해 노드를 배치한 그림을 나타낸 것으로 배치중심에 가장 많은 센서 노드가 모여 있고 중심에서 멀어질수록 센서 노드의 출현 횟수가 적어짐을 알 수 있다. 즉, 중앙 쪽에 위치한 노드는 자신이 위치한 클러스터 내의 이웃 노드와의 pairwise 키를 설정하는 것만으로 다른 노드와의 안전한 통신이 가능하며 바깥쪽에 위치한 노드만이 클러스터헤드에게 필요한 정보를 요청하여 전달된 정보를 바탕으로 이웃 노드와의 pairwise 키를 설정한다.

3.2. 키 설정 메커니즘

3.2.1. Blom의 대칭키 설정 메커니즘

본 연구를 통해 제안하는 메커니즘은 Blom의 대칭키 설정 방식을 기반으로 한다. Blom의 스킴은 $(\lambda+1)*N$의 공개 행렬(public matrix) G와 $(\lambda+1)*(\lambda+1)$의 개인 행렬(private matrix) D를 기본으로 하며 $A = (DG)^T$를 비밀 행렬이라 한다. 이 때, D는 대칭행렬, 즉, $k_{ij}=k_{ji}$이며 $A \cdot G$는 $A \cdot G = (A \cdot G)^T$, 즉, 전치행렬의 성격을 갖는다. 각 노드 i 는 A의 i번째 열과 G의 i번째 행을 저장하고 있다가 노드 배치 후 노드 i와 노드 j가 상호 간의 pairwise 키를 설정하고자 할 때 노드 i는 j에게 공개행렬의 i번째 행을 주고 노드 j는 i에게 공개행렬의 j번째 행 값을 전해주어 각각 자신이 갖고 있는 열과 상대방으로부터의 행을 dot 연산을 수행함으로써 상호간에 동일한 키 $k_{ij} = k_{ji}$를 생성하여 pairwise 키로 사용한다. Blom의 대칭키 설정 스킴이 (그림 2)에 나타나있다.



(그림 2) Blom의 대칭키 설정 스킴

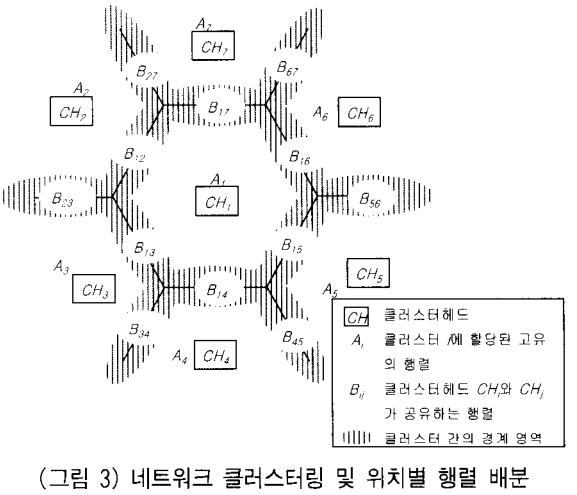
Blom의 스킴은 λ-security의 특성을 갖는다. 즉, 개인 행렬에서 노출되는 열의 수가 λ 이하 개이면 행렬 D는 안전하므로 다른 노드 간에 설정한 키는 노출되지 않으나 λ +1 개 이상의 열이 노출되면 행렬 자체를 복원시킬 수 있어 이 행렬을 기반으로 키를 설정한 모든 노드의 키가 노출되는 것이다. 그러므로 λ의 값을 기억 공간이나 계산 오버헤드를 고려하여 적절하게 유지하는 것과 행렬 G를 만드는 과정이 보안에 있어서 가장 핵심이 된다.

3.2.2. Pairwise 키 설정

본 연구를 통해 제안하는 메커니즘은 Blom의 대칭키 설정 메커니즘[2]과 Yu 등이 제안한 pairwise 키 설정 메커니즘[9]을 기반으로 육각의 클러스터와 중심의 클러스터헤드를 이용하여 pairwise 키를 생성하는 방식이다.

3.2.2.1. 제안 메커니즘의 특징

Yu 등이 제안한 pairwise 키 설정 메커니즘[9]은 센서 네트워크 필드를 육각의 그룹으로 나누고 각 그룹에 유일한 행렬을 배분하고 규칙적으로 반복되는 위치에 있는 특정 그룹을 공용 행렬을 사전에 할당받는 기본 그룹(basic group)으로 별도로 지정하여 이 그룹의 주변에 위치한 일반 그룹의 노드가 기본 그룹 노드에 할당된 공용의 행렬 B를 공유하도록 하는 방식이다. 이는 기존의 방식들에 비해 네트워크의 연결확률을 더 높이고 노드 포획에 대한 저항성을 높였다는 장점을 갖지만 공용의 행렬이 노출될 가능성을 줄이기 위해서는 공유 개수를 지정하는 파라미터 값 w를 낮게 조절함으로써 노드 간에 직접키를 생성할 가능성이 현저하게 줄어들어 효율적인 통신이 이루어질 수 없을 뿐만 아니라 사전에 예상되었던 위치를 많이 벗어나 다른 클러스터에 배치되는 노드는 키 설정이 불가능하여 노드를 포기할 수밖에 없다는 단점을 가진다. 또한 각 노드가 실제 배치된 위치에 따라서는 전혀 사용할 필요가 없는 정보를 사전에 분배받음으로 인해 기억장소의 낭비를 초래할 뿐 아니라 이 정보로 인해 보안이 깨질 위험이 높다. 또한 일정 수준의 네트워크 연결 가능성 및 보안성을 보장하기 위해서는 이 행렬을 공유하는 노드가 많아져야하므로 보안의 위협에 노출될 수 있다는 문제점이 있다.



(그림 3) 네트워크 클러스터링 및 위치별 행렬 배분

본 연구에서는 이와 같은 단점을 개선하기 위해 육각형의 그룹으로 나누어 고유한 행렬을 배분하는 것은 Yu의 방식과 동일하되 그룹의 중심에 클러스터헤드를 두고 클러스터헤드가 노드의 배치 후 각 노드의 요청에 의해서만 클러스터 간 통신에 필요한 정보를 배분하는 구조를 갖도록 한다. 각 노드의 위치에 따라 다른 클러스터 내의 노드와의 pairwise 키 설정이 필요한 경우에만 클러스터헤드가 정보를 분배하여 불필요한 정보의 노출 가능성을 줄이고 이웃한 모든 노드와의 pairwise 키 설정이 가능하도록 하여 센서 네트워크 통신의 효율성을 높일 수 있으며 노드가 사전에 계획되었던 위치와 멀리 떨어져 배치되는 경우에도 클러스터헤드 간의 통신을 통해 새로운 위치에서의 기능을 수행할

수 있도록 하여 노드의 손실을 막을 수 있다는 장점을 갖는다. 또한 클러스터 경계 면에 위치하는 노드들을 위한 행렬을 공유하는 클러스터를 두 개로 제한하고 그 클러스터에서도 경계에 가까운 노드만이 이를 할당받음으로써 보안의 위협을 훨씬 줄일 수 있다. 뿐만 아니라 클러스터헤드를 둠으로써 일반적인 센서 네트워크 통신에 필요한 자료의 수집과 정제를 통해 베이스 스테이션에 전달되는 네트워크 내 처리(in-network processing)가 가능하다는 장점을 갖는다. 이는 효율적인 인증 및 라우팅의 기본 프레임워크를 제공할 수 있다.

센서 네트워크 필드는 (그림 3)에서와 같이 육각의 형태로 사전에 클러스터링되며 각 클러스터 내에는 클러스터헤드가 위치한다. 클러스터는 육각의 형태로 구축하여 이웃하는 클러스터의 수를 최소화하면서 동시에 이웃노드와의 인접 정도가 균일하게 될 수 있도록 한다. 삼각이나 사각의 형태는 이웃 클러스터의 수가 각각 12, 8로 더 많으며 이웃노드와 인접하는 노드의 비율이 위치마다 달라서 복잡해질 뿐만 아니라 안전성도 낮아진다. 각 클러스터에는 클러스터 내에서만 사용이 가능한 고유한 비밀 행렬 A가 할당되어 모든 노드에게 이 행렬로부터 하나의 열 정보가 배분되고, 클러스터 간 통신에 필요한 공통 키 계산을 위해 두 클러스터의 인접 위치에 사용될 공용의 비밀 행렬이 별도로 지정되어 이 정보가 위치에 따라 각 클러스터헤드에게 사전에 분배된다. 각 클러스터헤드는 6개의 공유 비밀 행렬로 부터의의 값들을 추가로 가지며 가장자리에 위치한 클러스터헤드의 경우 배치 방법에 따라 2개에서 4개까지의 공유 행렬 값을 갖는다. 클러스터헤드 간의 pairwise 키를 위한 또 다른 비밀 행렬의 값도 사전에 할당된다. 제안하는 메커니즘에서 사용되는 표기법은 <표 1>과 같다.

〈표 1〉 제안 메커니즘에서 사용되는 표기법

표기법	설명
SN_{Xi}	클러스터 X에 배치된 센서 노드 i
CH_Y	클러스터 Y에 배치된 클러스터헤드
A_X	클러스터 X에 할당된 고유의 행렬
B_{XY}	클러스터 X와 클러스터 Y의 인접 지역에서 사용될 공용 행렬
C	클러스터헤드 간의 pairwise 키를 생성하기위한 고유의 행렬
G	공개 행렬
$K_{CH_X\ CH_Y}$	클러스터헤드 CH_X와 CH_Y간의 pairwise 키
$K_{BS\ CH_X}$	베이스 스테이션과 클러스터헤드 CH_X 간의 pairwise 키
K_{ij}	센서 노드 i와 j 간의 pairwise 키

3.2.2.2. 사용되는 키

이웃 노드 간, 혹은 이웃 클러스터헤드 간에 사용되는 키와 이 키의 설정을 위해 사용되는 행렬은 다음과 같다.

- 동일 클러스터 내의 노드 간 : 하나의 클러스터에 포함될 노드에는 유일한 비밀 행렬 A_i가 할당되어 이웃 노드와 서로의 G의 행 값만 교환함으로써 pairwise 키를 계산할 수 있다. 특히 모든 일반 노드는 자신이 속한 클러스터의 클러스터헤드와 이웃하지 않은 경우라도 동일한 행렬로부터의 정보를 갖고 배치되므로 자신의 클러스터헤드와 pairwise 키를 설정할 수 있다.
- 서로 다른 클러스터에 포함되는 이웃 노드 간 : 서로 다른 클러스터에 포함되므로 사전에 분배받은 정보를 사용할 수 없으며 공용으로 사용되는 행렬 B_{ij}의 한 열과 G로부터의 한 행을 클러스터헤드에게 요청하여 pairwise 키를 계산한다.
- 클러스터헤드 간 : 클러스터헤드 간의 pairwise 키를 설정하기 위한 공통 행렬 C의 한 열과 G의 한 행을 사전에 할당받아 필요 시 계산하여 이웃한 클러스터헤드 뿐 아니라 이웃하지 않은 클러스터헤드와의 pairwise 키도 생성할 수 있다.
- 베이스 스테이션과 각 클러스터헤드 간 : 네트워크 필드에 배치되기 전, 모든 클러스터헤드는 베이스 스테이션과의 유일한 대칭키를 부여받는다.

3.2.2.3. Pairwise 키 설정 과정

pairwise 키를 설정하는 과정은 다음과 같은 단계로 이루어진다.

[1단계] 키 관련 정보 배분 : 노드를 배치하기 전 키 셋업 서버는 각 클러스터에 배치될 것으로 예상되는 노드에게 해당 클러스터에 할당된 A_i의 한 열과 G의 한 행을 배분한다. 클러스터헤드에게는 추가로 행렬 C의 한 열과 인접 클러스터와 공유하는 6개의 B 행렬의 원소들을 분배받으며 추가될 수 있는 멤버를 위한 여분의 열을 A_i로부터 분배받는다. 이 과정은 off-line 상에서 이루어지므로 보안상의 위협이 없다고 본다.

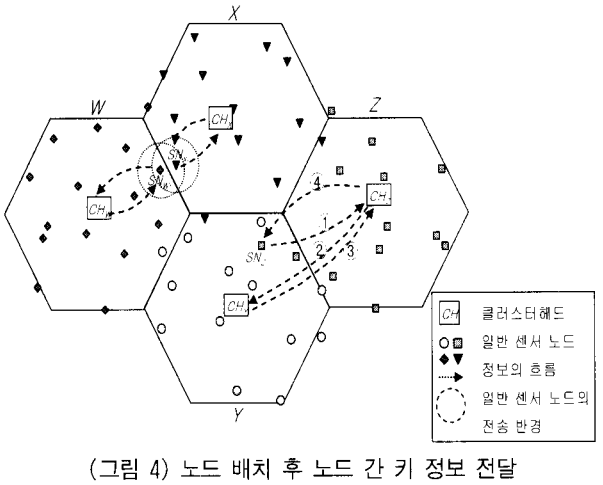
[2단계] 클러스터헤드를 중심으로 노드 배치 및 이웃 노드 파악 : 배치 중심에 클러스터헤드가 가까이 위치할 수 있도록 센서 노드를 배치한 후 모든 센서 노드들은 Hello 메시지를 교환하여 이웃 노드를 파악한다.

[3단계] Pairwise 키 설정 : 클러스터헤드 간, 그리고 이웃 노드 간에 사전에 분배받은 정보를 이용하여 이웃 노드 간 pairwise 키를 설정한다.

[4단계] 클러스터헤드에게 관련 정보 요청 : 각 센서 노드는 자신의 이웃에 다른 클러스터에 포함된 센서 노드가 있는 경우, 필요한 정보를 자신의 클러스터헤드에게 요청하고 클러스터헤드는 이 정보를 안전하게 각 센서 노드에게 전달한다. 이를 위해 클러스터헤드는 클러스터 내에 포함된 모든 센서 노드에게 자신의 공개 행렬 G의 행 값을 브로드캐스트하며 이 값을 이용해 센서 노드는 자신과 클러스터헤드간의 pairwise 키를 생성한다. 센서 노드가 클러스터헤드에게 정보를 요청할 때 이 키 값을 이용해 데이터를 암호화하며 데이터 내에 자신의 공개 행렬의 행값을 같이 보낸다. 클러스터헤드가 요청된 정보를 센서 노드에게 보낼 때는 계산한 pairwise 키로 암호화하여 전달하는데, 정보 요청을 받을 때와 정보를 보낼 때 라우팅 경로가 설정되지 않은 상태이므로 하나의 클러스터 내에서의 브로드캐스트 방식을 이용한다. (그림 4)에서 노드 SN_{X_i}와 SN_{W_j}는 서로 다른 클러스터의 멤버이나 서로의 전송 영역 내에 존재하여 pairwise 키

를 설정해야하므로 필요한 키정보를 각각의 클러스터헤드 (CH_X, CH_W)에게 요청하고 클러스터헤드는 이 정보를 요청한 멤버 노드와의 pairwise 키로 암호화하여 전송한다.

센서 노드가 예상 위치를 벗어나 배치되는 경우, 즉, 클러스터 Z의 경우를 보면 클러스터헤드 CH_Z가 멤버 노드의 이웃에 위치한 노드의 정보의 비율을 판단했을 때 SN_{Z_i}와 같이 센서 노드가 원래의 클러스터 영역 Z를 완전히 벗어났다고 판단될 경우, 원래의 클러스터헤드 CH_Z는 이 노드가 위치한 새로운 클러스터헤드에게 새로운 멤버를 받아들일 것과 관련 키정보를 요청하고 이를 SN_{Z_i}에게 전달하여 해당 클러스터 내에서 작동할 수 있도록 한다. 이 때 정보는 키를 바로 계산할 수 있는 값이므로 기밀성을 유지하기 위해 pairwise 키를 이용하여 암호화된 형태로 전달된다. 이 과정이 (그림 4)에 나타나있다.



(그림 4) 노드 배치 후 노드 간 키 정보 전달

① SN_{Z_i}는 원래의 클러스터헤드 CH_Z에게 자신의 이웃 노드 정보를 암호화하여 전송

$SN_{Z_i} \rightarrow CH_Z : Enc_{K_{SN_{Z_i}} CH_Z}$(자신의 id, 이웃 노드의 id 리스트)

② CH_Z는 자신의 멤버 SN_{Z_i}의 이웃 노드 중 다른 클러스터 멤버의 비율이 임계값 이상인 경우 그 클러스터에 노드가 배치된 것으로 판단하고 해당 클러스터 CH_Y에게 필요한 정보 요청

$CH_Z \rightarrow CH_Y$: Request(클러스터 id, SN_{Z_i})||MAC (Request (클러스터 id, SN_{Z_i}))

③ CH_Y는 행렬 A_Y의 한 열과 G의 한 행을 자신과 CH_Z의 pairwise 키로 암호화하여 CH_Z에게 전송

$CH_Y \rightarrow CH_Z : Enc_{K_{CH_Y CH_Z}}$($A_Y$의 한 열, G의 한 행)

④ CH_Z는 전달된 정보를 자신과 SN_{Z_i}와의 pairwise 키로 암호화하여 SN_{Z_i}에게 전송하고 SN_{Z_i}는 이를 복호화 함으로써 새로운 클러스터 Y의 멤버로 동작하는데 필요한 키 정보 확보

$CH_Z \rightarrow SN_{Z_i} : E_{K_{CH_Z SN_{Z_i}}}$($A_Y$의 한 열, G의 한 행)

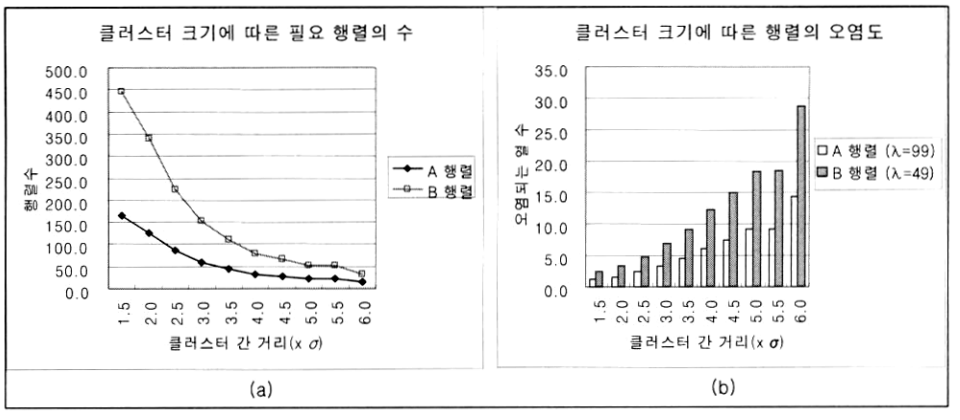
[5단계] 추가적 pairwise 키 설정 : 클러스터헤드로부터 분배받은 키정보를 이용하여 pairwise 키를 설정

4. 효율성 분석

4.1 안전성 분석

메커니즘의 효율성 분석을 위해 노드들이 필드에 일정하게 분포되어있다고 가정하였으나 실제로는 2차원 가우시안 분포를 모델로 하였으므로 배치중심을 위주로 조금 더 많은 노드들이 배치됨을 생각할 때 본 메커니즘을 실제로 적용하면 그 효율성은 더 높아진다. 제안 메커니즘의 효율성에 가장 큰 영향을 미치는 요소는 클러스터의 크기이다. 센서 노드의 전송 반경이 일정할 때 클러스터 크기가 크면 대부분의 노드가 해당 클러스터에 포함되고 또한 대부분 배치 중심에 좀 더 많은 노드가 위치하게 되므로 상대적으로 클러스터의 가장자리에 위치하여 다른 클러스터에 포함된 노드와 통신하는 경우의 수가 적어진다. 이는 결국 다른 클러스터 내의 노드와 pairwise 키를 설정해야하는 경우가 줄어드는 효과가 있으므로 클러스터가 필요한 키정보를 전달하는 확률, 이에 따른 키 설정의 비율을 낮추어 공유하는 행렬의 열 수를 줄이게 되고 이로 인한 키 노출과 공유 행렬 노출의 가능성을 낮춘다. 그러나 클러스터의 크기가 너무 커지면 하나의 클러스터 내에 너무 많은 센서 노드가 배치되어 자칫 전체 네트워크의 연결 가능성이 낮아질 수 있을 뿐 아니라 한 클러스터 내에서 비밀 행렬을 공유하는 노드수가 너무 많으면 λ 개 이상의 노드가 포획되는 경우 비밀 행렬이 노출되어 클러스터 전체가 위험에 빠질 가능성이 높아진다. 반면 클러스터 크기가 너무 작아지면 하나의 클러스터에 포함되는 노드의 수도 적어지고 많은 노드들이 다른 클러스터에 속한 노드들과 이웃하는 가능성이 높아져 공유 행렬의 열을 갖고 있는 노드 수가 늘어나고 이로 인한 보안상의 위협이 높아질 뿐더러 자신에게 사전에 할당되어있던 클러스터가 아닌 다른 클러스터에 위치할 가능성도 높아지므로 전체적인 효율성을 떨어뜨리는 결과를 낳는다. 또한 클러스터 크기가 너무 작아서 센서 반경이 이웃한 클러스터를 넘어서서 다른 클러스터 영역내의 노드와 이웃 노드의 관계가 형성이 되면 공통 행렬의 정보를 공유할 수 없어 pairwise 키 설정 자체가 불가능하다. <표 2>에서와 같은 환경 하에서 가우시안 분포를 따르면 99.87% 정도의 노드가 배치 중심 위치에서 3σ 내에 위치하게 된다. 그러므로 클러스터 중심 간의 최단 거리 l이 약 6σ 이상이 되면 센서 전송 반경이 이웃하지 않는 클러스터까지 미치지 않는다고 보장할 수 있다. 그러나 클러스터 크기가 너무 커지면 연결 가능성이 떨어지므로 이러한 tradeoff를 고려한 최적의 클러스터 크기를 찾는 것이 중요하다. 효율성 측정을 위해 본 논문에서 사용되는 파라미터 값은 다음과 같다.

먼저 네트워크 연결 가능성(P_c)을 비교해 보면 메모리 크기를 100을 기준으로 했을 때 Du의 배치정보 스킴이 Eschenauer의 기본 스킴이나 Chan의 q-composit 스킴에 비해 더 성능이 높으며 Yu의 그룹 기반 스킴의 경우 파라미터 값에 따라 차이를 보이지만 6개의 이웃 클러스터 중 4개의 이웃 클러스터 내 노드와의 pairwise 키 설정을 함을 의미하는 w=4



(그림 5) (a)클러스터 크기에 따른 필요 행렬 및 (b)각 행렬의 오염된 열 수(C_n=200)

이상인 경우 가능성을 1까지 높일 수 있음을 알 수 있다. 제안 스킴은 이러한 제약 조건 없이도 P_c=1, 즉, 존재하는 모든 이웃 노드와의 pairwise 키 설정이 가능하다.

〈표 2〉 효율성 측정에 사용되는 파라미터

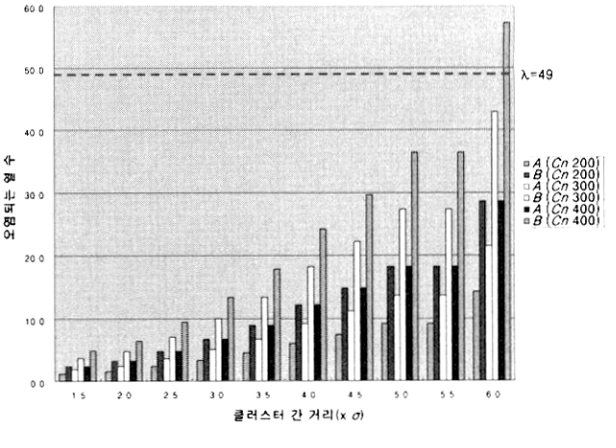
표기법	값	설명
N	10^4	센서 노드의 수
n	유동적	클러스터 수
n'	유동적	클러스터링 후 첫 번째 줄의 클러스터 개수
m	유동적	한 클러스터 내에서 클러스터 간 통신이 필요한 노드의 평균 수
r	40 m	일반 센서 노드의 전송 반경
M	100 또는 200	메모리 크기
σ	50 m	표준 편차
S	$10^3 * 10^3$ m^2	센서 네트워크 영역
Cn	200	전체 네트워크에서 오염된 노드 수
l	$a*\sigma$	클러스터 중심 간의 최단 거리

〈표 3〉 네트워크 연결 가능성 비교

메커니즘	P_c
q-composite 스킴(q=2, M=200)	0.9358
Eschenauer의 기본 스킴(M=100)	0.9867
Eschenauer의 기본 스킴(M=200)	0.9999
Du의 배치 정보 스킴(M=100)	0.9988
Yu의 그룹 기반 스킴(w=1~3, M=100)	0.9969~0.9999
Yu의 그룹 기반 스킴(w=4 이상, M=100)	1
제안 스킴(M=100)	1

다음으로 노드가 포획되어 보유한 키정보가 노출될 때 전체 네트워크에 미치는 영향을 살펴보면, 제안 메커니즘의 경우 (그림 3)에서 보는 바와 같이 공용 행렬 B를 공유하는 최대 클러스터 수는 2이다. 클러스터 경계 영역에 위치하지 않은 노드의 경우 A 행렬의 한 행만을 사전에 배분받으므로 $M = (\lambda+1)$이고, 배치 후 경계 영역임을 확인하고 추가로 클러스터헤드로부터 배분 받는 경우에도 필요한 총 메모리는 $M = (\lambda+1) * i$,(i=1,2)의 두 가지 경우에 해당하므로 λ값은 전자의 경우 99, 후자의 경우도 최악의 경우 32가 되어 하나의 행렬을 공유하는 노드들이 32개까지 포획되어야만 해당 행렬을 복구할 수 있어 보안성이 훨씬 높아진다. 동일 조건의 비교를 위하여 클러스터헤드 간 거리가 2σ인 경우 오염된 노드를 200이라고 했을 때 클러스터의 수는 약 128개이며 클러스터 당 오염된 노드의 수는 200/126 = 1.5이므로 이 노드들이 최대 2개씩의 행렬을 공유한다 해도 약 3이 되어 λ값에 훨씬 못 미치는 값이므로 B 행렬을 복구하여 키를 알아내는 것은 거의 불가능하다. 최악의 경우를 고려하여 클러스터헤드 간 거리 6σ, 즉, 클러스터 수가 14개라면 한 클러스터 당 오염된 노드 수는 200/14 = 14.29이며 이 노드가 모두 2개씩의 공유 행렬 정보를 가진다 해도 14.29 * 2 < 32 이다. 실제로는 경계 면에 위치하여 추가적인 행렬 정보를 필요로 하는 노드는 클러스터 내 전체 노드 수에 비해 훨씬 적으며 그 중에서도 두 개의 클러스터와 동시에 통신해야하는 노드는 극소수이므로 행렬 B는 안전하다.

A 행렬의 안전성을 분석해 보면 A 행렬의 경우는 클러스터가 커지면 하나의 클러스터에 포함되는 노드수가 많아지고 평균 오염된 노드 수가 많아지므로 λ값이 일정할 때 클러스터 크기에 따라 행렬이 노출될 가능성이 높아진다. 역시 오염된 노드수가 200일 경우를 살펴보면 제안 메커니즘은 λ값이 99로 클러스터의 최소 개수 14개의 경우라도



(그림 6) 클러스터 크기에 따른 각 행렬의 오염된 열 수(C_n= 200,300,400)

평균 클러스터 당 오염된 노드 수는 200/14 ≈ 14.3이므로 이 노드들이 λ값에 훨씬 못 미쳐 행렬 A는 안전하다. (그림 5)는 클러스터 간 최단 거리를 $a*\sigma$라 할 때 a 값의 크기에 따른 필요 행렬의 수 및 전체 오염 노드가 200개 일 때의 행렬의 노출 위험성을 나타낸 것이다.

(그림 6)은 제안 메커니즘이 Cn이 400개 이상인 경우에 B의 행렬 내에 노출되는 열 수가 λ개 이상이 됨으로써 B 행렬로 인한 키 노출의 가능성이 생김을 보여준다. 그러나 A 행렬의 경우 λ값이 99로 매우 높아 여전히 행렬 자체는 매우 안전함을 알 수 있다.

4.2 이웃 노드와의 pairwise 키 설정확률

Yu 등이 제안한 방식은 네트워크 연결 가능성을 낮추지 않으면서 오염된 노드로 인한 보안의 위험성을 낮출 수 있다는 장점을 갖지만 공유 행렬의 보안을 유지하기 위해서는 이웃 노드간의 직접키 설정확률이 현저히 낮아질 수밖에 없다. 제안 메커니즘과의 비교를 위하여 같은 조건을 고려해 본다면 행렬 B를 공유하는 클러스터 수 $2(b=2)$, 한 클러스터 내의 노드가 갖는 공유 행렬의 정보 $2(w=2)$로 이웃한 6개의 클러스터 중 2개의 클러스터 내 노드와만 pairwise 키 설정이 가능하므로 제안 메커니즘의 1/3 수준이 되어 나머지 이웃 노드와의 pairwise 키를 설정하기 위해서는 경로키를 설정해야하는 오버헤드를 감수하거나 이웃한 노드로 직접 통신하지 못하고 우회하여 통신함으로써 통신의 효율성을 저하시킬 수밖에 없다. 본 연구의 가장 큰 장점 중 하나는 모든 이웃 노드와의 직접키 설정이 가능하다는 점이다.

4.3 오버헤드 분석

각 노드가 키 설정을 위해 사용하는 키정보는 <표 4>와 같다.

4.3.1 저장 오버헤드

센서 노드는 저장 공간의 제약이 심하므로 가능한 한 각 센서 노드가 사전에 분배받는 키정보를 줄여야한다. 제안 메커니즘은 클러스터헤드가 좀 더 많은 키정보를 가지고 배치되므로 일반 노드의 키 저장 부담이 훨씬 낮아진다. 클러스터헤드의 저장 공간은 $(\lambda+1)(m+a+2)$이다. m은 클러스터 간 통신이 필요한 노드 수이며 a는 자신의 영역 중심 쪽으로 들어온 다른 클러스터 멤버 노드의 수이고 클러스터 내 통신에 한 개의 열이, 클러스터헤드 간 통신을 위해 한 개의 열이 필요하다. 일반 센서 노드는 원래의 행렬 A의 한 열만 가지면 되므로 $(\lambda+1)$개의 저장 장소가 필요하며 경계 영역 노드는 A로부터 하나의 열과 다른 클러스터 멤버와 이웃하는 수가 1, 혹은 2일 수 있으므로 총 $(\lambda+1)*2$ 또는 $(\lambda+1)*3$이 필요하다.

4.3.2 계산 오버헤드

클러스터 내 통신만 필요한 노드는 동일 클러스터 내 이웃 노드와의 키 계산만이 필요하므로 계산을 위한 에너지 소비는 매우 적다. 이 계산은 노드의 밀집도가 높을수록 점점 많아지고 낮을수록 적어진다. 클러스터헤드의 경우 이웃 노드의 수만큼의 키 계산에 추가로 클러스터헤드 간의 pairwise 키 계산이 필요하지만 이는 향후 인증이나 암호화에 반드시 필요하며 일반 노드에 비해 클러스터헤드가 갖는 에너지 수명이나 계산 능력을 고려해볼 때 그다지 크지 않은 오버헤드이다.

4.3.3 통신 오버헤드

센서 네트워크는 에너지 소비를 최소화하는 것이 네트워크 수명에 가장 중요한 요소이며 에너지 소비 측면에서 통신 오버헤드는 계산 오버헤드보다 훨씬 많은 에너지가 소비되므로 가능한 한 통신의 횟수를 줄이는 것이 매우 중요하다. 제안하는 메커니즘의 경우 클러스터의 중앙에 위치한 노드는 이웃 노드와의 Hello 메시지 교환 외에 키설정을 위한 별도의 통신이 필요치 않으며 클러스터 경계면에 위치한 노드가 필요한 행렬의 정보를 자신의 클러스터헤드에게 요청할 때와 요청한 정보를 받을 때 클러스터 내에서의 브로드캐스팅이 필요하며, 그 빈도가 매우 낮기는 하나 원래의 클러스터 영역을 벗어나 배치되는 노드의 경우 원래의 클러스터헤드와 새로운 위치의 새로운 클러스터헤드를 통하여 이루어지는 행렬 정보 교환 시에 부가적인 통신 오버헤드가 발생한다. Yu 등이 제안한 방식의 경우 기존 방식과 비교하여 네트워크 연결 가능성과 오염된 노드로 인한 네트워크 연결 가능성 저하를 고려하여 설정한 w의 값, 즉, 이웃 노드와의 직접 키 설정의 수는 1/3로 제한됨으로써 6개의 이웃 클러스터 중 2개의 이웃 클러스터들과만 직접키를 설정하게 됨으로써 나머지 부분은 경로키 설정이 부가적으로 필요하게 된다. 이 부분에서 추가적 통신 오버헤드가 발생할 뿐 아니라 경로키를 설정하기 위해 실제 키정보가 교환되므로 보안의 위험성이 훨씬 높아질 수밖에 없다. 제안 메커니즘은 이와 비슷하거나 더 적은 통신 오버헤드를 가지면서도 모든 이웃 노드와의 직접키 설정이 가능하며 보안성과 저장

〈표 5〉 키 계산에 필요한 행렬의 종류 및 할당 정보

	클러스터 중심 영역의 노드	클러스터 경계의 노드	클러스터헤드	필요한 총 행렬 개수
행렬 A	1개의 열	1개의 열	1개의 열+a (추가되는 멤버를 위한 정보)	n 개
행렬 B	-	1~2개의 열 (클러스터헤드로부터 전달받음)	6개 행렬로부터 총 m개의 열	약 $3*n-4*n'+1$개
행렬 C		-	1개의 열	1
배치후 전체 메모리 크기	$\lambda+1$	$(\lambda+1)*i$ $i=2,3$	$(\lambda+1)*(m+a+2)$	-

의 효율성을 훨씬 높이는 방식이라 할 수 있다.

5. 결 론

본 연구에서는 센서 네트워크의 보안을 위해 핵심이 되는 pairwise 키 설정에 있어서 효율성과 보안성을 높이기 위해 센서 네트워크 구조를 사전에 클러스터링하고 중심에 클러스터헤드를 둠으로써 이들을 통한 키 정보 전달 및 실제적인 배치 정보를 바탕으로 한 pairwise 키를 설정할 수 있는 방안을 제시하였다. 본 연구는 노드 배치가 가우시안 분포를 따르는 것으로 가정하였으나 만일 한번에 여러개가 아니라 한개씩 랜덤하게 뿌리는 경우에는 중심부의 밀집도가 가장자리와 동일하므로 그 효율성이 가우시안 분포의 경우보다는 조금 떨어지지만, 이 경우에도 클러스터간 통신이 필요치 않은 노드가 필요한 노드보다 더 많기 때문에 기존에 제안된 모든 노드들이 배치 후에 사용하지도 않을 키정보를 가지고 배치되는 경우보다 저장 오버헤드뿐 아니라 보안 수준에서도 더 효율적이다. 실험적 결과를 통하여 제안한 메커니즘은 클러스터헤드가 좀 더 많은 정보를 사전에 보유하고 전달함으로써 일반 센서 노드의 키정보 보유량을 더욱 줄여 노드 포획에 대항하는 저항성을 더욱 높이고 직접키 설정 확률을 획기적으로 높일 수 있음을 알 수 있다. 제안 메커니즘은 클러스터헤드의 경우 일반 노드에 비해 좀 더 많은 양의 정보가 사전에 분배되고 이 정보를 요청에 따라 전송해야하고 그럼으로써 이들에 대한 보안의 수준도 더 높여야한다는 추가적인 부담이 가해지지만 센서 네트워크의 특징 상 네트워크 내 처리(in-network processing)가 불가피하다는 사실을 고려했을 때 충분히 합리적인 구조이며 데이터 처리나 인증과의 연계 시 더욱 그 장점이 부각될 수 있다. 향후에는 제안한 메커니즘에 의해 설정된 노드가 pairwise 키와 클러스터헤드 간 pairwise 키를 이용한 효율적인 라우팅 및 인증 메커니즘에 관하여 연구를 진행할 예정이다.

참 고 문 헌

[1] D. W. Carman, P. S. Kruus, and B. J. Matt, "Constraints and approaches for distributed sensor network security," Technical report, NAI Labs, 2000.

[2] R. Blom "An optimal class of symmetric key generation systems. Advances in Cryptology," Proc. of EUROCRYPT 84, LNCS 209, pp.335~338, 1985.

[3] L. Eschenauer and V.D. Gligor, "A key management scheme for distributed sensor networks," Proc. of the 9th ACM CCS'02, pp.41~47, 2002.

[4] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," IEEE Symposium on Research in Security and Privacy, pp.197~213, 2003.

[5] W. Du, J. Deng, Y. S. Han, and P. Varshney, "A pairwise key pre distribution scheme for wireless sensor networks," Proc. of 10th ACM CCS'03, 2003.

[6] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," Proc. of 10th ACM CCS'03, pp.52~2003.

[7] 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.

[8] W. Du, J. Deng, Y. S. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," Proc. of IEEE INFOCOM'04, 2004.

[9] Z. Yu and Y. Guan, "A Robust Group based Key Management Scheme for Wireless Sensor Networks," IEEE Communications Society, WCNC 2005.

[10] Haowen Chan, Adrian Perrig, "PIKE: Peer Intermediaries for Key Establishment in Sensor Networks," Proc. of Infocom 2005.

[11] M. Chorzempa, J. M. Park and M. Eltoweissy, "SECK: Survivable and Efficient Keying in Wireless Sensor Networks," IEEE Workshop on Information Assurance in Wireless Sensor Networks, (WSNIA 2005).

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

채 기 준

e-mail : isdoh@ewhain.net
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, 센서네트워크, 홈 네트워크, 유비쿼터스 컴퓨팅

김 호 원

e-mail : kjchae@ewha.ac.kr
1993년 경북대학교 전자공학과(학사)
1995년 포항공과대학교 전자전기공학과 공학석사
1999년 포항공과대학교 전자전기공학과 공학박사
1998년~현재 한국전자통신연구원 정보보호연구단 RFID/USN 보안연구팀 팀장
2003년~2004년 Ruhr University Bochum, Germany, PostDoc.
연구분야 : 암호학 및 정보보호 이론, RFID 및 USN 정보보호 기술, 암호 프로세서 설계, VLSI 설계, embedded system 개발