



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0047976
(43) 공개일자 2010년05월11일

(51) Int. Cl.

H04L 9/08 (2006.01)

(21) 출원번호 10-2008-0106928

(22) 출원일자 2008년10월30일

심사청구일자 2008년10월30일

(71) 출원인

경희대학교 산학협력단

경기도 용인시 기흥구 서천동 1 경희대학교 국제 캠퍼스내

(72) 발명자

이승룡

경기 성남시 분당구 구미동 250 삼환빌라 102동 102호

이영구

경기 수원시 영통구 영통동 1024-14 경희유니빌 706호

고찬트룡

경기도 용인시 기흥구 서천동 1번지 경희대학교 전자정보과

(74) 대리인

김삼수

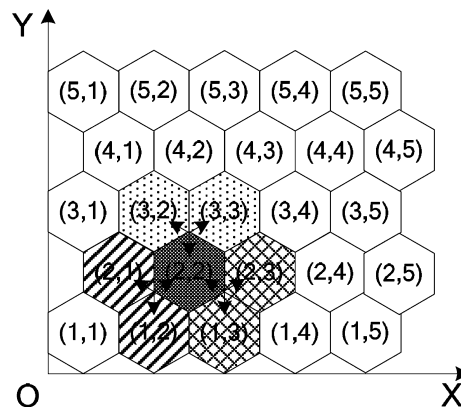
전체 청구항 수 : 총 9 항

(54) 전개 지식을 이용하는 센서 네트워크에서의 그룹-기반 키 관리 기법

(57) 요약

키 설정은 무선 센서 네트워크에서 특히, 주로 불리한 환경에서 전개될 때 인증 및 암호화의 중요한 역할을 담당한다. 전력의 엄격한 제한 때문에, 효과적인 키 설정 프로토콜을 프로세싱, 저장 및 설계하는 것은 사소한 태스크가 아니다. 전형적인 공용 키 암호 기법과 비교하여, 키 사전분배 메커니즘을 갖는 대칭형 키 암호 기법은 큰 스케일의 무선 센서 네트워크에 더 적당하다. 종래 솔루션 중 대부분은 실행 및 보안 능력들에서 몇 가지 문제점을 갖는다. 본 발명에서는 네트워크 연결성, 훼손된 노드에 대한 복원력, 메모리 요구 및 전송 에너지에 관하여 이점을 갖기 위한 사전 전개 지식(pre-deployment knowledge)을 이용하는 새로운 키 사전분배 모델을 제안한다.

대표도 - 도1



특허청구의 범위

청구항 1

이번 다항식을 생성하여 각 클러스터내의 센서 노드들로 분배하는 제1단계;

상기 센서 노드들이 특정 정보를 포함하는 메시지를 브로드캐스트하고, 이웃 노드들과 공통 공유 키-공간을 찾아 페어와이즈 키를 연산하는 제2단계

를 포함하는 것을 특징으로 하는 전개 지식을 이용하는 센서 네트워크에서의 그룹-기반 키 관리 기법.

청구항 2

제 1항에 있어서, 상기 제1단계에서

상기 클러스터는 이웃하는 센서 노드들의 그룹들의 세트이며, 그룹은 1-클러스터, 2-클러스터, 3-클러스터에 속하는 것을 특징으로 하는 전개 지식을 이용하는 센서 네트워크에서의 그룹-기반 키 관리 기법.

청구항 3

제 2항에 있어서, 특정 그룹을 (i, j)라 할 때,

상기 1-클러스터는 (i, j), (i+1, j), (i+1, j+1)로 이루어져 있고, 2-클러스터는 (i, j), (i, j-1), (i-1, j)로 이루어져 있으며 3-클러스터는 (i, j), (i-1, j+1), (i, j+1)로 이루어진 것을 특징으로 하는 전개 지식을 이용하는 센서 네트워크에서의 그룹-기반 키 관리 기법.

청구항 4

제 2항에 있어서,

상기 그룹은 세 개의 셀로 이루어져 있으며 모든 셀은 세 개의 그룹에 속하는 것을 특징으로 하는 전개 지식을 이용하는 센서 네트워크에서의 그룹-기반 키 관리 기법.

청구항 5

제 4항에 있어서,

각 셀은 세 개의 클러스터에 속하고, 상기 모든 센서 노드들은 3개의 이번 다항식을 저장하며, 각 그룹은 각 클러스터와 공통 키-공간을 공유하는지 체크하여 만일 공유하지 않으면 새로운 이번 다항식을 생성하여 센서 노드들로 분배하는 것을 특징으로 하는 전개 지식을 이용하는 센서 네트워크에서의 그룹-기반 키 관리 기법.

청구항 6

제 1항에 있어서, 상기 제2단계에서

상기 특정 정보는 노드의 ID와 운반하는 키-공간의 ID들을 포함하는 전개 지식을 이용하는 센서 네트워크에서의 그룹-기반 키 관리 기법.

청구항 7

제 1항에 있어서,

새로운 센서 노드가 추가될 때는 새로운 센서 노드로만 이번 다항식을 분배하는 것을 특징으로 하는 전개 지식을 이용하는 센서 네트워크에서의 그룹-기반 키 관리 기법.

청구항 8

제 1항에 있어서,

각 센서 노드들은 적어도 하나의 이번 다항식을 공유하는 훼손된 이웃 센서 노드들의 ID를 저장하고, 이 수가 일정량 이상이면 같은 이번 다항식을 공유하는 훼손되지 않은 센서 노드들이 해당 이번 다항식과 관련된 훼손 노드들을 제거하는 것을 특징으로 하는 전개 지식을 이용하는 센서 네트워크에서의 그룹-기반 키 관리 기법.

청구항 9

제 1항에 있어서,

상기 이번 다항식은 육각형 그리드로 분할된 특정 영역 상에서 제한된 수의 센서 노드들에 분배되는 것을 특징으로 하는 전개 지식을 이용하는 센서 네트워크에서의 그룹-기반 키 관리 기법.

명세서

발명의 상세한 설명

기술 분야

[0001] 본 발명은 센서 네트워크에서 전개 지식을 이용하는 그룹-기반 키 관리 기법에 관한 것이다.

배경 기술

[0002] 센서 네트워크는 홈 보안 모니터링, 군 경찰, 타겟 트래킹 등과 같은 다수의 어플리케이션들을 갖는다. 전형적인 센서 네트워크는 보통 많은 수의 작은 디바이스들로 이루어져 있다. 각 디바이스들은 센서 노드들이고, 제한된 배터리 전력 및 데이터 프로세싱 능력을 갖고 종종 단거리 무선 신호에 의해 각각의 다른 노드들과 통신한다. 많은 어플리케이션에서, 센서 노드들은 종종 정보를 인식, 수집하기 위해 특정 영역 상으로 랜덤하게 확산된다.

[0003] 센서 네트워크를 위한 가장 기본적인 보안 요건 중 하나는 센서 노드들간에 메시지를 송신할 때 비밀성 및 무결성을 보증하는 것이다. 센서 네트워크가 개발되는 환경들은 보통 불리한 영역들이다. 이러한 공간들에서, 공격자들(attackers)은 메시지들을 도청하거나 센서 노드로 물리적 공격을 가하거나 또는 다른 통신 프로토콜로 논리적 공격을 이용하여 네트워크를 손상시킬 수 있다.

[0004] 그러므로, 상기 문제점들을 없애기 위해 센서 네트워크는 암호화 및 인증 서비스들이 필요하다. 리소스 제약으로 인하여, 효과적인 키 설정 메커니즘 구현은 사소한 태스크가 아니다. 최근의 타원곡선암호(elliptic curve cryptography:ECC)의 장점 이외에도 대칭형 키 알고리즘이 이러한 문제를 해결하기에 적합한 솔루션이다.

[0005] 랜덤 키 사전분배는 Eschenauer와 Gligor에 의해 처음 제안되었다. Chan, Perrig 및 Song은 q-composite과 랜덤 페어와이즈 키 사전분배로 개선시켰다. Du, Deng, Han, Varshney는 그들의 기법 내의 기본 랜덤 페어와이즈에 전개 지식(deployment knowledge)을 적용시켰다. Blundo의 접근법에 의지하는 다항식-기반 제안은 [11],[12],[13]에 있다. 키 행렬 기법들은 Blom의 솔루션 [6], 다중 공간 키 사전분배 기법 [7] 및 Du, Deng, Han, Varshney의 DHDV-D [9]로부터 개발되었다. 비록 몇몇의 모델들이 종래의 전개 지식을 활용했지만, 그 모델들은 여전히 이 정보의 이점을 얻지 못한다.

[0006] 본 발명에서는 보안 및 실행 질의(questions)를 개선시키기 위한 전개 지식(deployment knowledge)을 사용하는 무선 센서 네트워크를 위한 6방형의 그룹 기반 키 관리 모델(HGKM)을 소개한다. 전개 지식(deployment knowledge)의 이점으로, 우리는 육각형 그리드(hexagonal grid)내의 특정 영역 상에서 제한된 수의 센서 노드들에 다항식(polynomial) 정보를 분배한다. 그래서 그것은 적이 어떤 노드들을 훼손할 때 다항식을 노출할 확률을 감소시킬 것이다. 본 발명은 종래 솔루션들보다 나은 보안성을 갖는 것을 보여준다.

[0007] 본 발명은 다음과 같이 정리되었다. 섹션 2에서는 관련 논문을 간단히 기술한다. 다음 섹션 3은 Blundo의 다항식(polynomial) 키 사전분배 기술의 개요를 나타낸다. 섹션 4는 본 발명을 상세하게 나타낸다. 후에, 섹션 5에서 우리는 다른 것들과 비교해서 본 발명에 따른 기법의 분석 및 평가를 보인다. 마지막으로, 섹션 6에서는 앞으로의 연구 방향들을 지적하고 끝맺는다.

[0008] · 관련 논문

[0009] 첫 번째 기법은 Eschenauer과 Gligor에 의해 제안되었다. 이 시스템에서, 큰 키-풀(large key-pool)은 오프라

인에서 생성되고 각 센서는 키-풀(key-pool)로부터 키들의 랜덤 서브셋을 골라낸다. 통신 범위내에서 어떤 두 개의 노드들은 오직 그들이 공통 키를 공유할 때 서로 말할 수 있다. 네트워크내의 키-풀의 크기 및 센서 노드들의 수에 의해, 이 설계는 다른 연결성 및 복원력을 획득할 것이다. Chan, Perrig 및 Song은 후에 유사한 아이디어를 이용하는 접근법을 제안했다. 그러나 하나의 키로부터 어떤 $q > 1$ 키들까지의 키-링(key-ring)간에

공유 키들의 교차가 증가되었다. 이것은 q 의 값이 증가 됨에 따라 노드 캡처에 대항하는 네트워크 복원력은 향상됨을 보여준다.

[0010] Du, Deng, Han, Varshney는 전개 지식(deployment knowledge)을 적용하는 키 사전분배 모델을 제안했다. 그들의 설계에서는 완전한 네트워크가 그룹들로 나뉘었다. 각 그룹은 [4]와 같이 기본 랜덤 키 사전분배를 실행한다. 그룹의 키-풀은 수평 그룹의 키-풀을 갖는 α 키와 대각선 그룹의 키-풀을 갖는 β 키를 공유한다.

[0011] 키 행렬 솔루션은 Blom의 아이디어에 기초하였다. 그는 공통 공유 키를 연산할 수 있는 그룹 내의 어떤 멤버들의 쌍을 확실하게 생성하는 키 사전 분배 기법을 제시하였다. N 은 네트워크내의 센서 노드들의 수를 나타내고, G 는 유한 필드 상에 $(t+1) \times N$ 크기의 발생행렬이라 하고, D 는 F_q 내의 요소들을 갖는 $(t+1) \times (t+1)$ 의 비밀랜덤행렬이라 한다.

[0012] 행렬 G 와 D 로부터, 엔트리들이 노드들간에 페어와이즈 키들이 될 $N \times N$ 대칭형 K 를 구성한다. 행렬 K 는 $K = (D \cdot G)^T \cdot G$ 와 같다. 각 노드 i 는 개인 행렬 $A = (D \cdot G)^T$ 에 대응하는 행 i 를 저장한다. 만일 노드 i 가 노드 j 와 통신하기를 원한다면, 공용키 $K_{i,j}$ 를 얻기 위해 G 의 j 번째 열을 저장하고 있는 행 벡터의 내적을 계산한다.

[0013] Du, Deng, Han, Varshney의 다중공간(multiple-space) 키 사전분배는 센서 네트워크에 적용하기 위해 Eschenauer과 Gligor의 기본 랜덤 키 사전분배를 갖는 Blom의 방법과 결합된다. 이러한 접근은, 키 공간을 생성할 수 있는 각 튜플(tuple) $\langle D, G \rangle$ 의 세트를 나타낸다. 네트워크의 각 노드는 사전 생성된 공간인 ω 로부터 τ 공간까지 랜덤하게 저장된다. 확률에 기초하여 어떤 두 노드는 공통 비밀 키를 연산할 수 있는 공통 공간을 공유할 수 있다.

[0014] 이후, Du, Deng, Han, Varshney는 또한 [9]에서 제안된 DDHV-D 기법에 사전 전개 지식(pre-deployment knowledge)을 적용하였다. 그것은 [8]에서 전개 지식이 적용된 랜덤 사전분배 기법과 [7]의 다중 공간 키 사전분배의 결합이다. 모든 키-행렬 솔루션은 쓰레숄드 t -보안 속성을 갖는다. 그것은 공격자들에 의해 훼손되는 노드들이 t 보다 적으면 훼손되지 않은 노드들 간의 통신은 여전히 안전하다는 것을 의미한다. 다항식 키 생성의 기본 아이디어는 [10]에서의 Blundo 등에 의해 제안되었다. 그것은 페어와이즈 키를 얻기 위해 대칭형 다항식 평가법(symmetric polynomial evaluation)을 사용한다. 이 방법의 상세한 설명은 다음 섹션에서 기술될 것이다. 이 제안은 $t+1$ 노드 미만의 손상 속성은 다른 노드들의 키에 관한 어떤 정보도 나타내지 않는다는 특성으로 캡처된 노드에 대해서 t -collusion resistant하다.

[0015] Liu 및 Ning는 상기 방법 및 [4]의 기본 랜덤 키 사전분배로부터 유래된 서브셋 할당 키 사전분배 모델을 소개하였다. 큰 키-풀을 생성하고 키-링을 만드는 대신, 이 기법은 큰 다항식 풀을 만들고 풀로부터 다항식의 서브셋이 각 노드로 할당된다. 그 후에 두 노드는 적어도 하나의 공통 다항식을 공유할 때 서로 통신할 수 있다. 이것은 이 솔루션이 [4]의 Eschenauer 및 Gligor의 모델과 비교해서 복원력이 증가됨을 보여준다. 게다가 사전 전개 지식(pre-deployment knowledge)을 사용하는 솔루션은 [12], [13]의 Liu 및 Ning의 클로셋 다항식 사전분배 기법(Closet Polynomials Predistribution Scheme:CPPS)과, [14]의 8-스퀘어 그리드-기반 다항식 사전분배(8-

square Grid-based Polynomial Predistribution)이다. 대부분의 솔루션은 여전히 실행 및 보안을 향상하기 위한 사전 전개 지식을 사용하는데 다소 제한이 있다.

[0016]

· Blundo's 키 사전분배 기법

[0017]

[10]의 Blundo의 기법은 t-보안 n-컨퍼런스에 대한 키 분배를 설정(establish)하기 위한 t-degree를 갖는 n 변 수 다항식을 사용한다. 두 엔티티간에 페어와이즈 키가 적용되고, 키 사전분배 서버는 한정된 필드 F_q 에

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

이변 t-degree 다항식 $f(x, y)$ 를 랜덤하게 생성하며 여기서 q 는 암호 키를 수용할 수 있을 만큼 충분히 큰 프라임 넘버이다. 함수 $f(x, y)$ 는 $f(x, y) = f(y, x)$ 인 대칭형 의미이다. 유니크한 정수 ID i 를 갖는 각 노드는 다항식 $f(x, y)$ 로부터 $f(i, y)$ 의 정보를 로드한다. 그리 고나서 어떤 두 개의 노드들 i 와 j 는 노드 i 에서 $k_{ij} = f(i, j)$ 와 노드 j 에서 $k_{ji} = f(j, i)$ 를 연산할 수 있다. 대칭형 속성으로 인하여 우리는 $k_{ij} = k_{ji}$ 를 갖는다. 그리하여 두 노드는 공통 페어와이즈 키를 갖는다.

[0018]

각 노드는 $t+1$ 계수들을 가져야하고, 각 계수들은 $\log_2 q$ 비트를 소요한다. 그래서 이 모델에서 각 노드 에 대한 메모리 저장 요구는 $(t+1)\log_2 q$ 비트이다. [6]의 분석은 이 기법이 무조건적으로 안전하고, t-collusion을 방지함을 보인다. 이것은 t 노드들 이상으로 훼손되지 않는 한, 공격자는 어떤 두 개의 노드들간 의 페어와이즈 키에 관해 아무것도 알지 못하는 것을 의미한다.

[0019]

이 기본적인 제안은 키를 저장하기 위한 메모리 오버헤드로 인하여 센서 네트워크에 직접적으로 적용할 수 없다. 메모리의 사이즈는 네트워크의 사이즈에 기하급수적으로 의존한다. 그래서 그것은 오직 이 모델만을 사용 하는 센서 노드와 같은 각 리소스-제한 장치에 유용하지 않다. 우리는 사전 전개 지식(pre-deployment knowledge)를 사용함에 의한 이 문제에 초점을 맞추고, 기댓값(expected) 위치 지식이 적용되는 다른 다항식 기 반 기법들보다 더 많은 이점을 가질 것임을 보여줄 것이다.

발명의 내용

해결 하고자하는 과제

[0020]

본 발명은 네트워크 연결성, 훼손된 노드에 대한 복원력, 메모리 요구 및 전송 에너지에 관하여 이점을 갖는 사 전 전개 지식(pre-deployment knowledge)을 이용하는 그룹-기반 키 관리 기법을 제공하는 것을 목적으로 한다.

과제 해결수단

[0021]

본 발명에 따른 전개 지식을 이용하는 센서 네트워크에서의 그룹-기반 키 관리 기법은 이번 다항식을 생성하여 각 클러스터내의 센서 노드들로 분배하는 제1단계와 상기 센서 노드들이 특정 정보를 포함하는 메시지를 브로드 캐스트하고, 이웃 노드들과 공통 공유 키-공간을 찾아 페어와이즈 키를 연산하는 제2단계를 포함한다. 이때, 상 기 제1단계에서 상기 클러스터는 이웃하는 센서 노드들의 그룹들의 세트이며, 그룹은 1-클러스터, 2-클러스터,

3-클러스터에 속하는 것이 바람직하다.

[0022] 또한, 특정 그룹을 (i, j) 라 할 때, 상기 1-클러스터는 (i, j) , $(i+1, j)$, $(i+1, j+1)$ 로 이루어져 있고, 2-클러스터는 (i, j) , $(i, j-1)$, $(i-1, j)$ 로 이루어져 있으며 3-클러스터는 (i, j) , $(i-1, j+1)$, $(i, j+1)$ 로 이루어진다.

[0023] 또한, 상기 그룹은 세 개의 셀로 이루어져 있으며 모든 셀은 세 개의 그룹에 속하고, 각 셀은 세 개의 클러스터에 속하고, 상기 모든 센서 노드들은 3개의 이번 다항식을 저장하며, 각 그룹은 각 클러스터와 공통 키-공간을 공유하는지 체크하여 만일 공유하지 않으면 새로운 이번 다항식을 생성하여 센서 노드들로 분배하는 것이 바람직하다.

[0024] 상기 제2단계에서 상기 특정 정보는 노드의 ID와 운반하는 키-공간의 ID들을 포함하고, 새로운 센서 노드가 추가될 때는 새로운 센서 노드로만 이번 다항식을 분배하는 것이 바람직하다. 또한, 각 센서 노드들은 적어도 하나의 이번 다항식을 공유하는 훼손된 이웃 센서 노드들의 ID를 저장하고, 이 수가 일정량 이상이면 같은 이번 다항식을 공유하는 훼손되지 않은 센서 노드들이 해당 이번 다항식과 관련된 훼손 노드들을 제거하는 것이 바람직하다. 여기서, 상기 이번 다항식은 육각형 그리드로 분할된 특정 영역 상에서 제한된 수의 센서 노드들에 분배된다.

효과

[0025] 본 발명은 가우시안 분배와 함께 사전 전개 지식의 이점을 갖는 실제 다항식-기반 키 사전분배 접근법을 사용함으로써, 네트워크 연결성과 통신 오버헤드, 메모리 요구 등에서 보다 많은 이점을 갖고, 공격에 훼손된 노드들에 대한 보안성이 강화되는 효과가 있다.

발명의 실시를 위한 구체적인 내용

[0026] 이하, 첨부된 도면을 참조하여 본 발명의 실시 예에 따른 전개 지식을 이용하는 센서 네트워크에서의 그룹-기반 키 관리 기법을 상세히 설명한다.

[0027] · 제안된 키 사전분배 모델

[0028] 본 발명에 따른 기법을 보이기 전에, Blundo의 기법에서 t -degree 이번 다항식 $f(x, y)$ 가 생성될 수 있는 모든 키들의 세트만큼 키-공간을 정의한다. 키-공간에서 키들의 수는 키-공간 사이즈를 나타낸다. 만일 그것이 $f(x, y)$ 로부터 생성되는 정보를 운반한다면 노드가 키-공간을 고른다고 가정한다. 공통 키-공간을 고르는 어떤 두 노드는 항상 그들의 페어와이즈 키를 연산한다.

[0029] 본 발명은 전체적으로 두 개의 단계를 갖는다. 키 사전분배, 다이렉트 키 설정(establishment). 키 사전분배 단계는 전개(deployment)전에 각 센서 노드로 신뢰 정보를 프리로드하기 위해 수행된다. 후에 셋업하고, 두 개의 센서 노드들이 만일 적어도 하나의 공통 키-공간을 공유한다면 노드들간의 다이렉트 키를 설정할 수 있다. 우선 처음에 우리는 센서 네트워크의 전개(deployment) 모델을 다룰 것이다.

[0030] · 6방향 그리드-기반 전개(deployment) 모델

[0031] 본 발명에서, 타겟 영역은 6방향 그리드로 분할된다. 이 형상은 원에 최적의 접근을 제공하고, 연속적인 필드 상에 반복될 수 있는 세 개의 형상 즉, 삼각형, 사각형 육각형 중 다른 두 개의 형상보다 큰 영역을 포함한다. 또한, 육각형은 사각형의 8개 또는 삼각형의 12개의 비교하여 최소(6개)의 이웃하는 셀을 갖는다. 센서 노드들은 셀들상에서 그룹들로 분할되고 분배된다. 이 모델은 비행기를 이용하여 차례차례로 그룹들을 드롭아웃하는 것처럼 각 그룹의 센서 노드들이 함께 운반되어 예상되는 인접 그룹들이 현장에서 서로 인접할 가능성이 높아서

실제 상황에서 효과적이다.

[0032] 보통, 센서 노드들의 배열은 어떤 확률 분배 함수(pdf 함수)에 의존한다. 타겟 전개(deployment) 영역이 $X \times Y$ 크기를 갖는 이차원이라고 가정하자. 이차원 영역 상에 $i = 1, \dots, N$ 인 노드 i 의 위치에 대한 pdf는 $f_i(x, y)$ 이다. 여기서 $x \in [0, X]$ 이고, $y \in [0, Y]$ 이다. N 개의 센서 노드들은 G 개의 같은 크기의 그룹으로 나뉜다. pdf는 [11],[12],[13],[14]에서와 같이 균등 분배가 될 수 있거나 [7],[8],[9]에서의 가우시안 분배와 같이 더 실제적일 수 있다. 본 발명에서 우리는 그룹 G_i 에 대해 아래와 같은 입체 가우시안 분배를 사용한다.

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

[0034] 여기서 (x, y) 는 그룹 G_i 에서 노드의 좌표이고, 그룹의 전개 포인트는 (x_i, y_i) 이며 σ 는 분배의 표준편차이다. σ 의 값은 주로 센서 그룹들을 드롭아웃할 때의 평면의 높이에 의존한다. 셀에서, 분배 함수는 비 균등이고, 우리는 전체 분배가 거의 균등함을 얻기 위해 전개 포인트들 간의 적절한 거리를 선택할 수 있다. 6방향 그룹-기반 전개 모델은 도 1에 나타내었다.

[0035] 본 발명의 구조를 설명하기 전에, 우리는 클러스터가 이웃하는 그룹들의 세트임을 정의한다. 그룹은 1-클러스터, 2-클러스터, 3-클러스터의 세 가지 타입의 클러스터에 속한다. 어떤 그룹 (i, j) 의 관점에서 1-클러스터는 이 그룹과 두 개의 그룹 $(i+1, j)$ 및 $(i+1, j+1)$ 로 이루어져 있다. 2-클러스터는 그룹 (i, j) 와 두 개의 그룹 $(i, j-1)$ 및 $(i-1, j)$ 로 이루어져 있다. 3-클러스터는 그룹 (i, j) 와 두 개의 그룹 $(i-1, j+1)$ 및 $(i, j+1)$ 로 이루어져 있다. 예를 들어, 도 1에서 그룹 (2, 2)로부터 그룹 (3, 2) 및 (3, 3)은 1-클러스터(2, 2)에 속한다. 그룹 (2, 1) 및 그룹 (1, 2)는 2-클러스터(2, 2)에 속하고, 3-클러스터(2, 2)는 그룹 (2, 3) 및 그룹 (1, 3)으로 이루어져 있다. 그러므로, 각 그룹은 세 개의 셀로 이루어져 있고, 모든 셀은 세 개의 그룹에 속한다.

[0036] · 다이렉트 키 설정 단계

[0037] 셋업 후에, 각 노드는 그것의 이웃 노드들과 일정한 키-공간을 공유하는지 아닌지를 발견해야한다. 이를 위해 각 노드는 아래의 정보를 포함하는 메시지를 브로드캐스트한다. : (1) 노드의 ID, (2) 운반하는 키-공간 ID들.

[0038] 노드 A와 B가 이웃하고 있고, 각각 ID가 N_a 및 N_b 라고 가정하자. 그들은 서로 상기 브로드캐스트 메시지를 수신한다. 만일 그들이 공통 공유 키-공간 f_c 를 찾는다면, 그들은 Blundo의 기법에서 보인 바와 같이 페어 와이즈 키를 연산할 수 있다. : 노드 N_a 는 키 $K_{A,B} = f_c(N_a, N_b)$ 를 연산한다. 노드 N_b 는

$K_{B,A} = f_c(N_b, N_a)$ 를 연산한다. 이번 다항식 f_c 의 대칭 속성으로 인하여 우리는 $K_{A,B} = K_{B,A}$ 를 갖는다. 이 키는 노드 A 와 노드 B 사이의 비밀 페어와이즈 키로 사용된다.

[0039] 상기 단계 후에, 센서 네트워크는 아래와 같은 키 그래프 $G(V, E)$ 를 형성한다. V 가 모든 센서 노드에 동등한 꼭지점 세트이고, E 는 네트워크내의 안전한 링크와 같은 에지들의 세트인 키 그래프 $G(V, E)$ 를 정의한다. 어떤 두 개의 꼭지점 u 와 v 간의 에지가 존재하는 필요충분조건 : (1) u, v 가 각각 전송 범위 내에 있다. (2) 둘 다 페어와이즈 키를 수립할 수 있음을 의미하는 공통 공유 키-공간 ID를 갖는다.

[0040] · 센서 추가 및 철회(revocation)

[0041] 새로운 센서를 추가하기 위해서는, 키 셋업 서버는 사전분배 단계와 유사하게 오직 새로운 노드로 관련 다항식 공유를 사전분배 할 필요가 있다. 키-공간의 사이즈가 제한되어 있으므로, 더 많은 센서들이 더해지면 그 셀에서의 보안은 낮아진다. 철회(revocation) 방법은 또한 간단하다. 각 센서 노드는 오직 자신과 적어도 하나의 이번 다항식을 공유하는 훼손된 센서들의 블랙리스트 ID들을 저장할 필요가 있다. 만일 같은 다항식을 공유하는 훼손된 노드들이 k 이상이면, 이 다항식을 갖는 훼손되지 않은 노드들은 이 다항식과 모든 관련 훼손 노드들을 제거한다.

[0042] · 분석

[0043] 우리는 아래의 측정에 관하여 논의한다.

[0044] - 네트워크 연결성 : 로컬 연결성 및 글로벌 연결성을 포함. 로컬 연결성은 노드가 그들의 전송 범위 내에서 이웃하는 노드들과 연결할 수 있는 확률이다. 글로벌 연결성은 전체 네트워크의 사이즈에 대한 최종 키 그래프 G 에서 가장 큰 격리된 연결 컴포넌트를 형성하는 센서 노드들 수의 비율이다.

[0045] - 통신 오버헤드 : 본 발명에서 통신 연결에 노드가 필요로 하는 에너지이다.

[0046] - 메모리 오버헤드 : 본 발명에서 노드에서 키 요소들을 저장하기 위한 메모리 요구이다.

[0047] - 캡처된 노드에 대한 복원력 : 노드들을 훼손시키는 공격이 나머지 네트워크에 미치는 영향을 추정하였다.

[0048] 이 분석에서 우리는 적들이 이번 다항식을 발견할 수 있는 확률을 구한다. 이는 이 다항식으로부터 얻어진 키로 암호화된 모든 보안 연결을 적들이 밝혀낼 수 있음을 의미한다.

[0049] · 시스템 구성

[0050] 본 발명에서의 시뮬레이션 및 수적인 분석을 위해 표 2의 구성을 사용한다.

[0051]

부호	값	부호설명
N	10,000	네트워크 내의 노드의 수
S	1000×1000(m ²)	네트워크 전개 영역
r	40m	통신 범위
M	200 keys	키 요소들을 저장하기 위한 노드의 메모리 크기
σ	50m	가우시안 분배의 표준 편차

[0052] <표 2> 시뮬레이션 구성

[0053] 본 발명에서는 노드 전개가 식(1)의 pdf 함수를 갖는 이차원 가우시안 분배를 따른다고 가정한다.

[0054] · 네트워크 연결성

[0055] $d = a \times \sigma$ 는 두 개의 이웃하는 셀들의 두 전개(deployment) 포인트들 간의 거리를 나타낸다. 이 값은 네트워크내의 로컬 연결성 및 글로벌 연결성에 대해서 영향을 미친다. 만일 전개(deployment) 분배가 가우시안 분배에 따른다면, 그룹의 99.87%의 센서 노드들이 전개 포인트로부터 3σ 범위 내에 존재한다. 그러므로, 만일 값 d 가 6σ 보다 매우 크면, 그룹 내의 거의 모든 노드들이 그들의 셀 영역 내에 존재하고, 그들의 이웃하는 노드들 역시 같은 셀 내에 존재한다.

[0056] 이런 경우, 로컬 연결성은 매우 높지만 네트워크는 전적으로 격리된 컴포넌트로 분할되고, 이는 글로벌 연결성은 매우 낮다는 것을 의미한다. 값 d 가 더 작은 경우, 로컬 연결성은 낮아질 것이지만 글로벌 연결성은 높다. 그래서, d 의 적절한 값을 선택하는 것은 네트워크 연결성에 영향을 미친다. 이 시뮬레이션에서, 우리는 a 에 따라 d 의 값을 다르게 변경한다. 이와 함께, 로컬 연결성 및 글로벌 연결성의 비율은 또한 도 2에 나타난 바와 같이 다양한 값을 갖는다.

[0057]

a	로컬 연결성	글로벌 연결성
0.4	0.0787	0.6546
0.6	0.1577	0.9290
0.8	0.2524	0.9704
1.0	0.3643	0.9921
1.5	0.6036	0.9990
2.0	0.7720	0.9994
2.5	0.8617	0.9998
3.0	0.9226	0.9999
3.5	0.9555	0.9999
4.0	0.9657	1

[0058] <표 3> 시뮬레이션 결과

[0059] 두 개의 이웃하는 셀의 두 전개 포인트들 간의 거리가 너무 낮을 때($a = 0.4; 0.6; 0.8; 1.0$), 어떤 노드 A 에는 그것의 주변에 분포된 이웃하지 않는 셀들의 많은 노드들이 있다. 이 노드들은 노드 A 와 어떤 키-공간을 공유하지 않는다. 그래서 로컬 연결성 및 글로벌 연결성은 감소한다. 표 3으로부터 본 발명의 전개 포인트 거리들의 적절한 값을 선택할 때 높은 로컬 및 글로벌 연결성을 얻음을 보기가 쉽다. $a = 1.5$ 값을 갖는 글로벌 연결성은 0.9990이고, 이는 네트워크 내에서 오직 0.01% 수의 노드들만을 낭비함을 의미한다.

[0060] · 통신 및 메모리 오버헤드

[0061] 무선 센서 네트워크의 프로토콜을 설계함에 있어 긴 생존시간(lived time)은 중요한 목표이다. 본 발명은 이웃하는 노드들 간의 공통 키-공간을 발견하는데 필요한 브로드캐스트 데이터 요구를 최소화했다. 본 발명의 1-홉 브로드캐스트 메시지 길이는 $\text{sizeof}(\text{nodeID}) + 3 \times \text{sizeof}(\text{key-spaceID})$ 이다. [4], [5]내의 다른 모델과 비교해서, 키 디스커버리 단계 내의 브로드캐스트 메시지들은 높은 연결성을 획득하기 위해 수백의 키를 포함한다. [13]의 CPPS를 갖는 브로드캐스트 메시지의 길이는 $\text{sizeof}(\text{nodeID}) + 5 \times \text{sizeof}(\text{polynomialID})$ 이고, 본 발명보다 높다.

[0062] 키 요소를 저장하기 위한 메모리 사이즈는 다항식 $M = 3 \times (t + 1) \log_2 q \text{ (bits)}$ 로부터 얻어진다. 이 값은 다

항식을 공유하는 노드의 수와 함께 공격에 훼손된 노드에 대한 복원력에 영향을 미친다. 우리는 아래의 섹션에서 더욱 상세하게 논의할 것이다.

[0063]

· 노드 훼손에 대한 보안성

[0064]

센서 네트워크의 동작 환경은 항상 불리하기 때문에, 센서 노드들이 캡처되고 정보가 누설되기가 쉽다. 적들은 훼손된 노드들 내의 모든 페어와이즈 키들을 얻을 수 있다. 그러므로, 적들은 훼손된 노드들의 모든 링크와 훼손되지 않은 노드들 간의 다른 링크들을 포함하는 많은 보안 링크들을 부술 수 있다. 노드 캡처에 대한 복원력

이라는 점에서 우리의 모델을 평가하였다. 그것은 x 노드가 훼손되었을 때, 훼손되지 않은 센서 노드들 간의 다이렉트 키를 노출하는 것을 의미하는 다항식을 누설할 확률이 얼마나 되는지이다.

[0065]

[10]에서의 분석은 t-secure 속성을 갖는 다항식 기반 기법을 나타낸다. 만일 이번 다항식의 다항식 공유가 t 보다 많이 밝혀지지 않았다면, 적들은 이 다항식을 사용하여 수립된 훼손되지 않은 노드들의 페어와이즈 키를 알지 못할 것이다. 그러므로, 본 발명의 보안성은 같은 다항식을 공유하는 센서 노드들의 수의 평균에 의존하고, 센서 노드들의 수는 세 개의 이웃하는 육각형 셀들 내에 놓여질 것이라고 추정한다. 본 발명은 이전

의 섹션에서 전개(deployment) 모델을 설명하였다. 센서 노드 수의 평균을 나타내고 셀 N_c 내에 놓여질 것이라고 추정하고, 다항식을 공유하는 센서 노드 수의 평균은 다음에 의해 연산될 수 있다.

$$N_G = 3N_c = 3\omega S_c = \frac{3\sqrt{3}a^2\sigma^2\omega}{2} \quad (2)$$

[0066]

이 식에서 ω 는 센서 노드 밀도이다. 이전 섹션에서 설명된 바와 같이, 키 요소들을 저장하기 위한 메모리 요구는 $M = 3 \times (t + 1) \log_2 q \text{ (bits)}$ 이다. 따라서 이번 다항식의 차수는

$$t = \left\lceil \frac{M}{3} \right\rceil - 1 \quad (3)$$

[0068]

$N_G \leq t$ 를 만족하면, 본 발명은 노드 캡처에 대한 완벽한 저항을 갖는다. 달리 말해서, 센서의 훼손은 훼손되지 않은 센서들 간에 공유된 다이렉트 키를 훼손하지 않는다. [13]에서의 분석에 따라, 본 발명은 여기서 랜

덤 공격을 고려한다. 본 발명은 네트워크 내에서 센서 노드의 프랙션 P_c 가 공격자에 의해 훼손되었다고 가정

한다. 다항식을 공유하는 N_G 센서 노드들 사이에 t 센서 노드가 훼손될 확률은 다음에 의해 구해질 수 있다.

$$P_c(i) = \binom{N_G}{i} p_c^i (1 - p_c)^{N_G - i} \quad (4)$$

[0070]

그래서, 이번 다항식이 훼손되는 확률은 다음에 의해 연산될 수 있다.

$$P_c = 1 - \sum_{i=0}^t P_c(i) \quad (5)$$

[0072]

- [0073] 도 3에서 보는 바와 같이, 우리는 셀 사이즈가 큰 것을 의미하는, 보다 긴 거리는 노드 훼손 공격에 대한 복원력이 보다 공격받기 쉬움을 알 수 있다. 셀 사이즈가 크면, 키-공간을 공유하는 셀 내에 보다 많은 센서 노드들이 있고, 보안성을 더욱 낮게 하기 때문이다.
- [0074] 도 4에서 보는 바와 같이, 보다 많은 메모리는 네트워크의 복원력을 강화시킨다. 다항식의 차수가 높아지기 때문이다. [4],[5],[13]내의 다른 모델들과 비교하여 본 발명은 훼손된 노드에 대한 복원력에 의해 보다 좋은 보안성을 갖는다. 도 5에서 보는 바와 같이, 본 발명은 [12],[13]의 CPPS와 200개의 암호 키 스토리지를 갖는 [14]의 8-스퀘어 모델보다 좋은 보안성을 얻기 위해 단지 150개의 키 스토리지가 필요하다.
- [0075] 본 발명에서는 가우시안 분배와 함께 사전 전개 지식(pre-deployment knowledge)의 이점을 갖는 실제 다항식-기반 키 사전분배 접근법을 설명하였다. 우리는 이 모델이 실행(네트워크 연결성, 통신 오버헤드, 메모리 요구)의 모든 면에서 보다 많은 이점을 갖고, 공격에 훼손된 노드들에 대한 보안성을 갖는 것을 보였다. 본 발명의 앞으로의 연구는 메시지를 전파할 때의 프라이버시와 통신 에너지의 비용 감소, 인다이렉트 키 설정을 갖는 네트워크 연결성 분석의 문제점에 초점을 맞출 것이다.
- [0076] -인용문헌-
- [0077] [1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. "A survey on sensor networks" In *IEEE Commun. Mag.* Vol 40, Issue 8, August 2002.
- [0078] [2] A.D. Wood, and J.A. Stankovic, "Denial of service in sensor networks" In *IEEE Computer*. 54-62, October 2002.
- [0079] [3] C. Karlof, D. Wagner. "Secure routing in wireless sensor networks: attacks and countermeasures In *First IEEE International Workshop on Sensor Network Protocols and Applications*, May 2003.
- [0080] [4] L. Eschenauer, V. D. Gligor. "A key-management scheme for distributed sensor networks", In *Proceedings of the 9th ACM conference on Computer and communications security*, November 2002.
- [0081] [5] H. Chan, A. Perrig, D. Song. "Random key predistribution schemes for sensor networks" In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, May 2003.
- [0082] [6] R. Blom, "An optimal class of symmetric key generation systems" In *Proc of EUROCRYPT '84*, pp. 334-338, 1985.
- [0083] [7] W. Du, J. Deng, Y. S. Han, P. K. Varshney. "A pairwise key predistribution scheme for wireless sensor networks", In *Proceedings of the 10th ACM conference on Computer and communications security*, 2003.
- [0084] [8] W. Du; J. Deng; Y. S. Han; S. Chen; P.K Varshney. "A key management scheme for wireless sensor networks using deployment knowledge" In *23rd Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom '04)*, Hong Kong, China, March 21-25, 2004.
- [0085] [9] W. Du, J. Deng, Y. S. Han, P. Varshney. "A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge". In *IEEE Transactions on Dependable and Secure Computing*, Volume 3 , Issue 1(January 2006).
- [0086] [10] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung. "Perfect-secure key distribution of dynamic conferences" In *Advances in Cryptography - CRYPTO '92*, LNCS 740, pp. 471-486, 1993.
- [0087] [11] D. Liu, P.Ning. "Establishing pairwise keys in distributed sensor networks", In *ACM Transactions on Information and System Security*, February 2003.
- [0088] [12] D. Liu; P. Ning. "Location-based pairwise key establishments for static sensor networks" In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN '03)*, October

2003.

[0089] [13] D. Liu, P.Ning. "Improving Key Predistribution with Deployment Knowledge in Static Sensor Networks", In ACM Transactions on Sensor Networks, Vol. 1, No. 2, November 2005, pp. 204-239.

[0090] [14] Ngo Trong Canh, Tran Van Phuong, Young-Koo Lee, Sungyoung Lee, and Heejo Lee. "A Location-aware Key Predistribution Scheme for Distributed Wireless Sensor Networks," In The 15th IEEE International Conference on Networks (ICON '07), pp.188-193, 19-21 Nov. 2007.

도면의 간단한 설명

[0091] 도 1은 본 발명의 실시 예에 따른 그룹-기반 키 관리 기법에서 6방향 그룹-기반 전개 모델을 나타내는 도면이다.

[0092] 도 2는 본 발명의 실시 예에 따른 그룹-기반 키 관리 기법에서 전개 포인트 거리에 따른 네트워크 연결성을 나타내는 도면이다.

[0093] 도 3은 다른 전개 포인트 거리를 갖는 노드 훼손 공격에 대항하는 네트워크 복원력을 나타내는 도면이다.

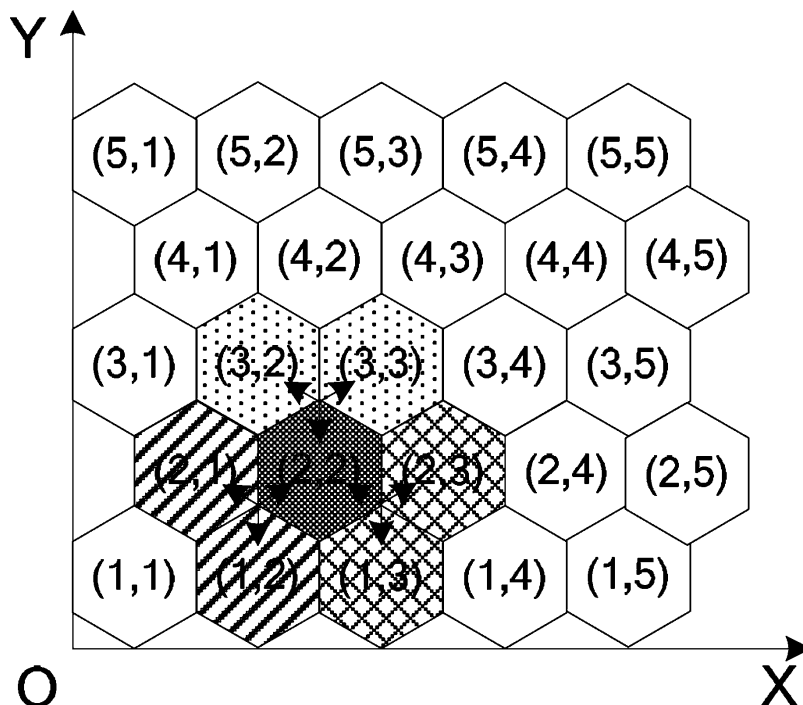
[0094] 도 4는 다른 메모리 사이즈를 갖는 노드 훼손 공격에 대항하는 네트워크 복원력을 나타내는 도면이다.

[0095] 도 5는 전개 포인트 거리가 1.5일 때, 통신 훼손의 프랙션(fraction) 비교를 나타내는 도면이다.

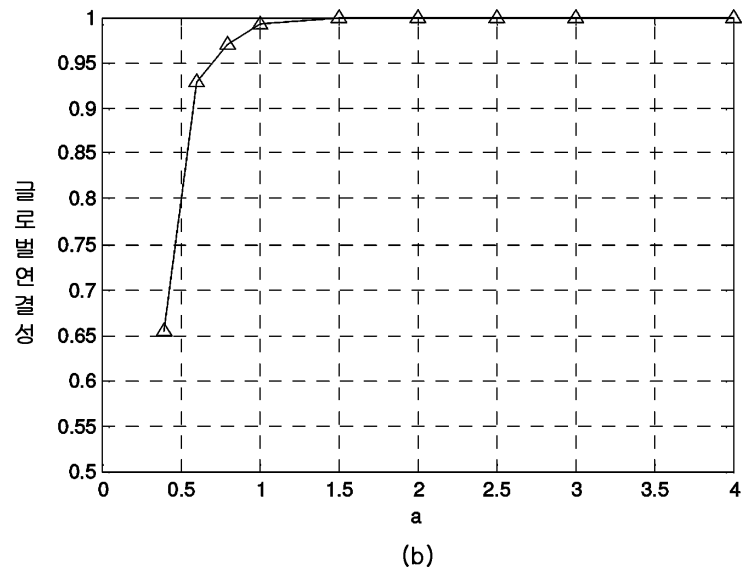
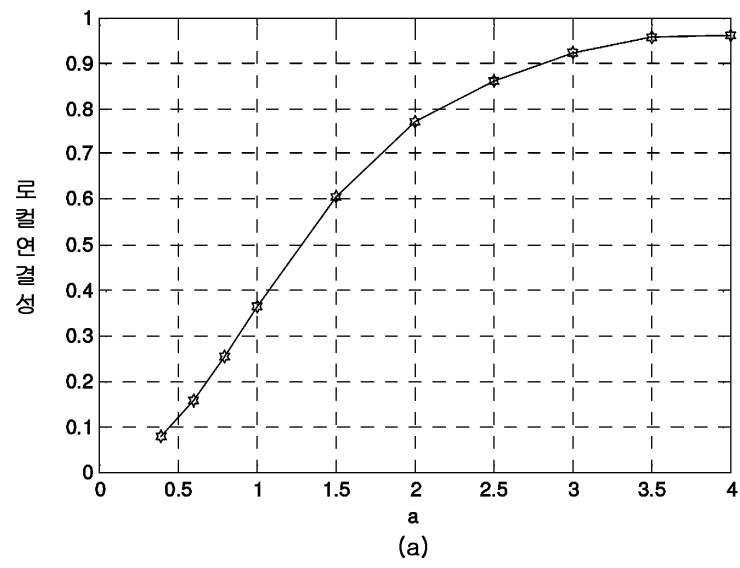
[0096] 도 6은 본 발명의 실시 예에 따른 다항식 사전분배 알고리즘을 나타내는 도면이다.

도면

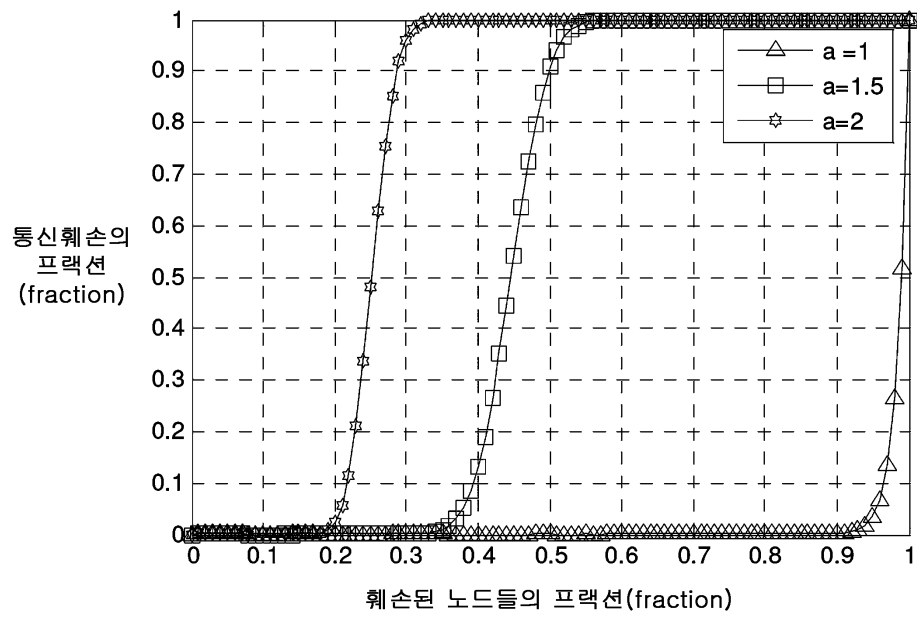
도면1



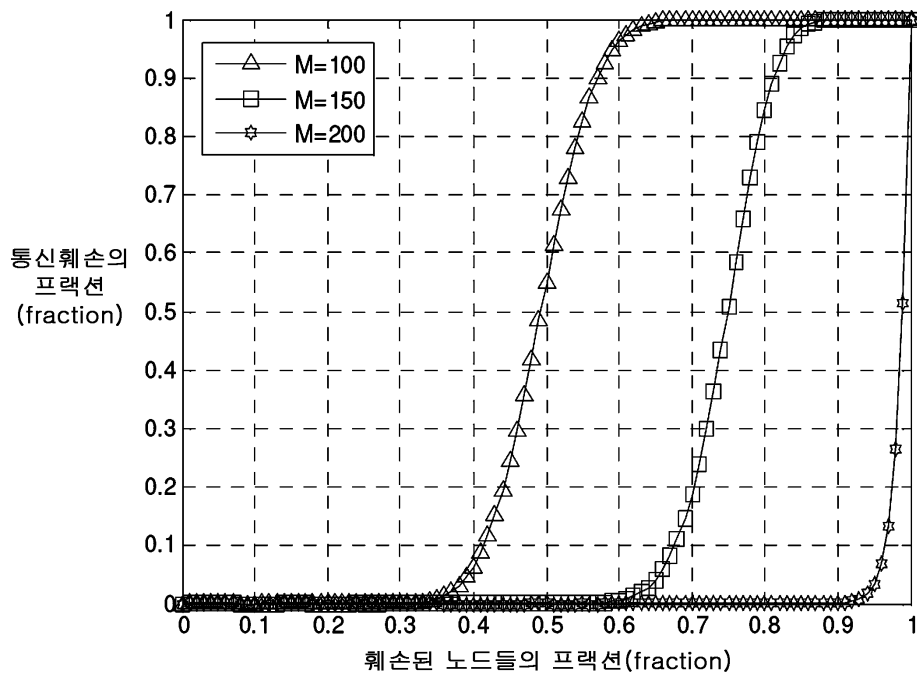
도면2



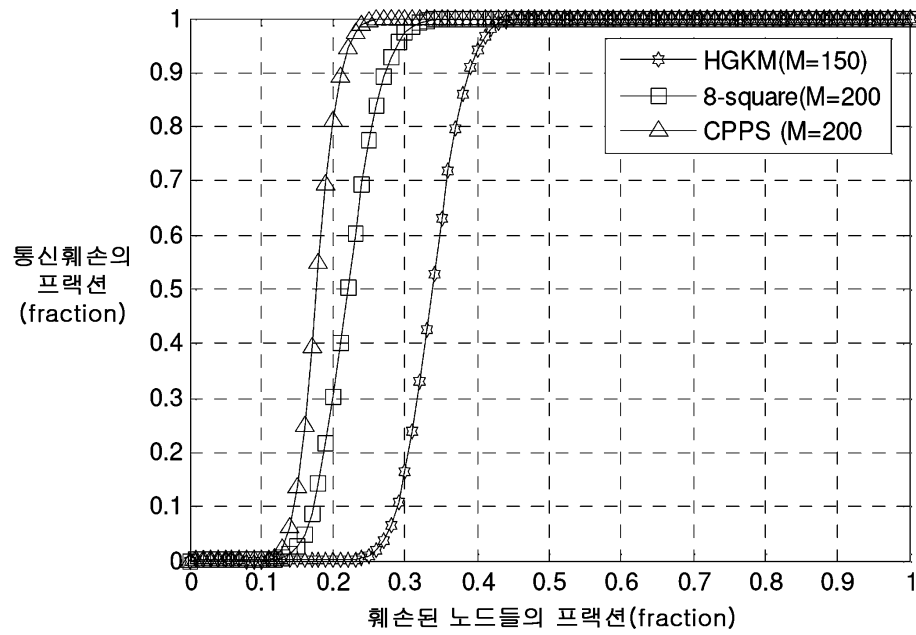
도면3



도면4



도면5



도면6

```

For each group  $G_{i,j}$  {
    For each group  $G_{u,v}$  in 1-cluster( $G_{i,j}$ ) {
        If not is_polynomial_sharing( $G_{u,v}$ ,  $G_{i,j}$ ) {
            Geneate a  $f(x,y)$ .
            Assign  $f(x,y)$  to 1-cluster( $G_{i,j}$ )
        }
    }
    For each group  $G_{u,v}$  in 2-cluster( $G_{i,j}$ ) {
        If not is_polynomial_sharing( $G_{u,v}$ ,  $G_{i,j}$ ) {
            Geneate a  $f(x,y)$ .
            Assign  $f(x,y)$  to 2-cluster( $G_{i,j}$ )
        }
    }
    For each group  $G_{u,v}$  in 3-cluster( $G_{i,j}$ ) {
        If not is_polynomial_sharing( $G_{u,v}$ ,  $G_{i,j}$ ) {
            Geneate a  $f(x,y)$ .
            Assign  $f(x,y)$  to 3-cluster( $G_{i,j}$ )
        }
    }
}
    
```