



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0105684
(43) 공개일자 2008년12월04일

(51) Int. Cl.

H04L 9/08 (2006.01) H04L 12/28 (2006.01)

(21) 출원번호 10-2007-0053580

(22) 출원일자 2007년05월31일

심사청구일자 2007년05월31일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

천지영

서울 성북구 안암동5가 고려대학교 정보보호대학원 138호

김용호

서울 성북구 안암동5가 고려대학교 정보보호대학원 140호

(뒷면에 계속)

(74) 대리인

현종철

전체 청구항 수 : 총 12 항

(54) 위치 기반의 보안키 사전 분배 방법, 위치 기반의 보안키 공유 방법, 및 위치 기반의 보안키 추가 방법

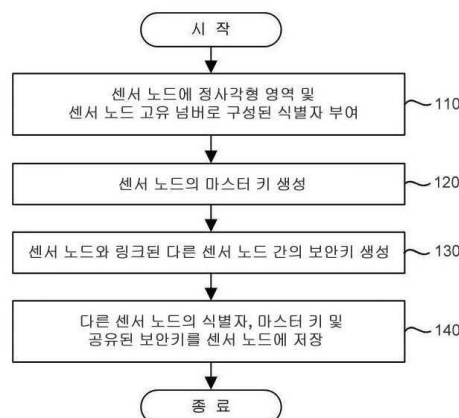
(57) 요약

위치 기반의 보안키 사전 분배 방법, 위치 기반의 보안키 공유 방법, 위치 기반의 보안키 추가 방법 및 이를 기록한 기록매체가 개시된다.

본 발명에 따른 위치 기반의 보안키 사전 분배 방법은, 복수의 센서 노드들이 배치될 위치를 정사각형 모양의 영역으로 분할하고, 상기 분할된 정사각형의 영역에 센서 노드를 배치한 후, 셋업 서버에서 상기 배치된 센서 노드에 상기 배치된 정사각형의 영역 및 상기 센서 노드 고유 넘버로 구성된 식별자를 부여하는 단계, 상기 식별자가 부여된 각각의 센서 노드에 상기 셋업 서버에서 상기 식별자를 기반으로 상기 센서 노드의 마스터 키를 생성하는 단계, 상기 마스터 키가 생성된 센서 노드에서 상기 센서 노드와 위치적으로 연관되어 링크되는 다른 센서 노드와의 보안키를 생성하는 단계, 및 상기 다른 센서 노드의 식별자, 마스터 키 및 공유된 보안키를 상기 센서 노드에 저장하는 단계를 포함한다.

본 발명에 의하면, 무선 센서 네트워크에서 위치기반의 보안키를 설정하여, 최소 비용으로 최대 이익을 얻기 위한 공격자의 선택적인 노드 포획을 고려한 안전한 보안키를 설정함으로써 센서 노드들 사이의 안전한 통신이 가능하고, 보안키 설립시 통신 및 계산량이 적고 메모리 요구량이 적어서 자원 제약적인 센서 네트워크에 적합하며 대규모 네트워크의 지원이 가능하고 안전하게 새로운 노드의 추가가 가능하고, 저전력으로 보안키의 생성 및 유지가 가능하며 보안이 중요하게 요구되는 응용환경에 쉽게 적용할 수 있는 효과가 있다.

대표도 - 도1



(72) 발명자

임종인

서울 종로구 내수동 95 삼성파크팰리스 101-901

이동훈

경기 고양시 일산동구 정발산동 밤가시마을 901동
201호

특허청구의 범위

청구항 1

복수의 센서 노드들이 배치될 위치를 정사각형 모양의 영역으로 분할하고, 상기 분할된 정사각형의 영역에 센서 노드를 배치한 후, 셋업 서버에서 상기 배치된 센서 노드에 상기 배치된 정사각형의 영역 및 상기 센서 노드 고유 번호로 구성된 식별자를 부여하는 단계;

상기 식별자가 부여된 각각의 센서 노드에 상기 셋업 서버에서 상기 식별자를 기반으로 상기 센서 노드의 마스터 키를 생성하는 단계;

상기 마스터 키가 생성된 센서 노드에서 상기 센서 노드와 위치적으로 연관되어 링크되는 다른 센서 노드와의 보안키를 생성하는 단계; 및

상기 다른 센서 노드의 식별자, 상기 센서 노드의 마스터 키 및 공유된 보안키를 상기 센서 노드에 저장하는 단계를 포함하는 위치 기반의 보안키 사전 분배 방법.

청구항 2

제 1 항에 있어서,

상기 보안키는,

의사 난수 함수 및 상기 보안키를 생성하고자 하는 센서 노드의 마스터 키를 이용하여 생성된 것을 특징으로 하는 위치 기반의 보안키 사전 분배 방법.

청구항 3

제 1 항에 있어서,

상기 다른 센서 노드는,

상기 센서 노드가 배치된 정사각형 영역 및 상기 센서 노드가 배치된 정사각형 영역과 수직으로 서로 접하는 정사각형 영역에 배치된 노드인 것을 특징으로 하는 위치 기반의 보안키 사전 분배 방법.

청구항 4

복수의 센서 노드들이 배치될 위치를 정사각형 모양의 영역으로 분할하고, 상기 분할된 정사각형의 영역에 센서 노드를 배치한 후, 셋업 서버에서 상기 배치된 센서 노드에 상기 배치된 정사각형의 영역 및 상기 센서 노드 고유 번호로 구성된 식별자를 부여하는 단계;

상기 식별자가 부여된 각각의 센서 노드에 셋업 서버에서 상기 식별자를 기반으로 상기 센서 노드의 마스터 키를 생성하는 단계;

상기 마스터 키가 생성된 센서 노드에서 상기 센서 노드와 위치적으로 연관되어 링크되는 다른 센서 노드와의 보안키를 생성하여 상기 보안키, 상기 다른 센서 노드의 식별자 및 상기 센서 노드의 마스터 키를 상기 센서 노드에 저장하는 단계; 및

상기 보안키, 식별자 및 마스터 키를 저장한 센서 노드를 센서 네트워크에 배치하고, 상기 센서 노드의 마스터 키에 따라 상기 센서 네트워크에 배치된 이웃 노드와 보안키를 공유하는 단계를 포함하는 위치 기반의 보안키 공유 방법.

청구항 5

제 4 항에 있어서,

상기 보안키는,

의사 난수 함수 및 상기 보안키를 생성하고자 하는 센서 노드의 마스터 키를 이용하여 생성되는 것을 특징으로 하는 위치 기반의 보안키 공유 방법.

청구항 6

제 4 항에 있어서,

상기 다른 센서 노드는,

상기 센서 노드가 배치된 정사각형 영역 및 상기 센서 노드가 배치된 정사각형 영역과 수직으로 서로 접하는 정사각형 영역에 배치된 노드인 것을 특징으로 하는 위치 기반의 보안키 공유 방법.

청구항 7

제 4 항에 있어서,

상기 센서 네트워크에 배치된 이웃 노드와 보안키를 공유하는 단계는,

상기 센서 네트워크에 배치된 다른 센서 노드에서 상기 다른 센서 노드가 저장하고 있는 식별자 목록을 브로드캐스팅하는 단계;

상기 브로드캐스팅된 식별자 목록에 상기 센서 노드의 식별자가 포함된 경우, 상기 센서 노드에서 자신의 마스터 키를 이용하여 상기 센서 노드와 상기 다른 센서 노드의 보안키를 연산하는 단계; 및

상기 센서 노드와 상기 다른 센서 노드에서 상기 연산된 보안키를 공유하는 단계를 포함하는 것을 특징으로 하는 위치 기반의 보안키 공유 방법.

청구항 8

제 4 항에 있어서,

상기 센서 네트워크에 배치된 이웃 노드와 보안키를 공유하는 단계는,

상기 센서 네트워크에 배치된 다른 센서 노드에서 상기 다른 센서 노드가 저장하고 있는 식별자 목록을 브로드캐스팅하는 단계; 및

상기 브로드캐스팅된 식별자 목록에 상기 센서 노드의 식별자가 포함되지 않은 경우, 상기 센서 노드의 이웃 노드 중 상기 다른 센서 노드와 보안키를 공유한 또 다른 센서 노드를 이용하여 상기 다른 센서 노드와 상기 센서 노드에서 보안키를 공유하는 단계를 포함하는 것을 특징으로 하는 위치 기반의 보안키 공유 방법.

청구항 9

복수의 센서 노드들이 배치될 위치를 정사각형 모양의 영역으로 분할하고, 상기 분할된 정사각형의 영역에 센서 노드를 배치한 후, 셋업 서버에서 상기 배치된 센서 노드에 상기 배치된 정사각형의 영역 및 상기 센서 노드 고유 번호로 구성된 식별자를 부여하는 단계;

상기 식별자가 부여된 각각의 센서 노드에 셋업 서버에서 상기 식별자를 기반으로 상기 센서 노드의 마스터 키를 생성하고, 상기 센서 노드와 위치적으로 연관되어 링크되는 다른 센서 노드와의 보안키, 상기 다른 센서 노드의 식별자 및 상기 센서 노드의 마스터 키를 저장하는 단계;

상기 센서 노드를 센서 네트워크에 배치하고, 상기 센서 노드에서 상기 센서 네트워크에 배치된 이웃 노드와 보안키를 공유하는 단계;

상기 센서 네트워크에 새로운 센서 노드가 추가하고자 하는 경우, 상기 셋업 서버에서 상기 새로운 센서 노드가 배치될 상기 정사각형 영역을 지정하고, 상기 지정된 정사각형 영역에 따라 상기 새로운 센서 노드의 식별자 및 마스터 키를 부여하는 단계;

상기 새로운 센서 노드에서 상기 지정된 정사각형 영역에 따라 상기 셋업 서버에 저장된 데이터베이스를 이용하여 상기 새로운 센서 노드와 위치적으로 연관되어 링크되는 센서 노드와의 보안키, 상기 식별자 및 마스터 키를 저장하는 단계; 및

상기 새로운 센서 노드를 상기 센서 네트워크에 배치하고, 상기 새로운 센서 노드의 마스터 키에 따라 상기 새로운 센서 노드와 이웃 노드간의 보안키를 설정하는 단계를 포함하는 위치 기반의 보안키 추가 방법.

청구항 10

제 9 항에 있어서,

상기 보안키는,

의사 난수 함수 및 상기 보안키를 설정하고자 하는 센서 노드 자신의 마스터 키를 이용하여 생성되는 것을 특징으로 하는 위치 기반의 보안키 추가 방법.

청구항 11

제 9 항에 있어서,

상기 다른 센서 노드는,

상기 센서 노드가 배치된 정사각형 영역 및 상기 센서 노드가 배치된 정사각형 영역과 수직으로 서로 접하는 정사각형 영역에 배치된 노드인 것을 특징으로 하는 위치 기반의 보안키 추가 방법.

청구항 12

제 1 항 내지 제 11 항 중 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

- <7> 본 발명은 무선 센서 네트워크에서 키 설정 방법에 관한 것으로서, 더욱 상세하게는 센서 노드들 사이의 안전한 통신을 할 수 있는 센서 네트워크에서의 위치 기반의 보안키 사전 분배 방법, 위치 기반의 보안키 공유 방법, 위치 기반의 보안키 추가 방법 및 이를 기록한 기록매체에 관한 것이다.
- <8> 무선 센서 네트워크(Wireless sensor network)는 센서 노드들의 제한된 자원과 무선 통신을 이용한 데이터 전송 등으로 인하여 보안상의 많은 위험요소를 가지고 있다.
- <9> 따라서, 군사적인 목적으로 사용되는 경우 등과 같이 수집된 데이터의 보안이 중요한 환경에서는 센서 노드들 사이의 안전한 통신을 위한 보안키 설립이 필수적이다.
- <10> 무선 센서 네트워크는 에너지, 저장공간, 계산 및 통신 능력이 제한되어 있는 많은 수의 센서 노드들로 구성된다. 일반적인 네트워크와는 달리 무선 센서 네트워크에 있는 센서 노드들은 종종 물리적 공격에 취약한 환경에 배치될 수 있다. 이와 같이 센서 노드들은 에너지, 저장공간, 통신 및 계산 능력이 제한되어 있어서, 공개키 암호를 이용한 일반적인 키 설정방법을 적용하기 어렵다. 이러한 환경에서 공격자는 노드를 획득할 수 있고, 두 센서 노드들 사이의 데이터나 제어 정보를 도청하거나 변경할 수 있다. 이러한 공격은 전체 무선 센서 네트워크에 심각한 위협을 초래할 수 있다.
- <11> 이에 따라, 안전한 무선 센서 네트워크의 구성을 위해 기밀성 및 인증을 제공하는 보안 서비스는 중요한 요소로서, 센서 노드가 무선 센서 네트워크에 배치되기 전에 키 관련 정보를 모든 센서 노드들에게 분배하는 키 사전 분배 방법이 많은 관심을 받고 있다.
- <12> 센서 노드는 종종 물리적으로 안전하지 않은 환경에 배치될 수 있다. 이러한 환경에서 공격자는 센서 노드를 획득할 수 있으며, 이를 통해 센서 노드 내의 키를 포함하는 중요한 정보를 빼낼 수 있다. 이러한 이유로 무선 센서 네트워크에 적용하기 위한 키 사전 분배 방법의 가장 중요한 목적 중 하나는 센서 노드 획득 공격에 대한 완전한 장애 허용성을 가지는 방법을 제공하는 것이다. 완전한 장애 허용성이라 함은 획득된 센서 노드가 그 자신이 포함되지 않은 링크에 대해 어떠한 정보도 드러내지 않겠다는 것을 의미한다.
- <13> 이러한 장애 허용성을 가지는 키 사전 분배 방법은 지원 가능한 센서 네트워크의 크기가 엄격히 제한되며, D. Liu와 P. Ning이 ACM CCS 2003에서 제안한 'grid based key pre-distribution scheme'은 직접적인 보안키 설정을 위하여 많은 양의 모듈로 곱셈을 필요로 하므로 이러한 계산량은 자원 제약적인 센서 노드들에게 부담이 된다.
- <14> 한편, 위치 기반 기법 중 선택적인 노드 포획에 완전한 안정성을 보장하기 위하여 제안된 방법은 대칭행렬을 이

용하여 키를 사전 분배한 D. Huang 등의 그리드 그룹 배치(Grid Group Deployment:GGD) 방법이 있으나, 이 방법은 임계값(Threshold) 이하로 행렬의 행의 사용을 제한함으로써 선택적인 노드 포획에 대한 안정성을 보장하고, 이후 J. Lee 등이 제안한 멀티 레이어 그리드(Multi-layer Grids) 기법 또한 임계값 이하의 노드의 갯수에 대해서만 선택적인 노드 포획에 대한 안정성이 보장되는 문제점이 있으며, 전체 지원 가능한 노드의 수에 제한이 있다는 것은 새로운 노드의 추가에도 제한이 따르며, 네트워크의 확장성이 떨어지고, 대규모 네트워크의 지원이 어렵고, 보안키 설정시 필요한 모듈러 연산(modular operation)도 저전력의 센서 네트워크에 적합하지 않은 문제점이 있다.

발명이 이루고자 하는 기술적 과제

- <15> 따라서, 본 발명이 이루고자 하는 첫 번째 기술적 과제는 대규모 네트워크의 지원이 가능하면서 보안 키 설정을 위한 계산량이 적고, 선택적인 노드 포획에 완전한 안정성을 가지는 위치 기반의 보안키 사전 분배 방법을 제공하는 것이다.
- <16> 그리고, 본 발명이 이루고자 하는 두 번째 기술적 과제는, 상기 위치 기반의 보안키 사전 분배 방법을 이용한 위치 기반의 보안키 공유 방법을 제공하는 것이다.
- <17> 또한, 본 발명이 이루고자 하는 세 번째 기술적 과제는, 안전하게 새로운 노드의 추가할 수 있도록 상기 위치 기반의 보안키 사전 분배 방법을 이용한 위치 기반의 보안키 추가 방법을 제공하는 것이다..

발명의 구성 및 작용

- <18> 상기 첫 번째 기술적 과제를 달성하기 위하여 본 발명은,
- <19> 복수의 센서 노드들이 배치될 위치를 정사각형 모양의 영역으로 분할하고, 상기 분할된 정사각형의 영역에 센서 노드를 배치한 후, 셋업 서버에서 상기 배치된 센서 노드에 상기 배치된 정사각형의 영역 및 상기 센서 노드 고유 넘버로 구성된 식별자를 부여하는 단계, 상기 식별자가 부여된 각각의 센서 노드에 상기 셋업 서버에서 상기 식별자를 기반으로 상기 센서 노드의 마스터 키를 생성하는 단계, 상기 마스터 키가 생성된 센서 노드에서 상기 센서 노드와 위치적으로 연관되어 링크되는 다른 센서 노드와의 보안키를 생성하는 단계, 및 상기 다른 센서 노드의 식별자, 마스터 키 및 공유된 보안키를 상기 센서 노드에 저장하는 단계를 포함하는 위치 기반의 보안키 사전 분배 방법을 제공한다.
- <20> 상기 두 번째 기술적 과제를 달성하기 위하여 본 발명은,
- <21> 복수의 센서 노드들이 배치될 위치를 정사각형 모양의 영역으로 분할하고, 상기 분할된 정사각형의 영역에 센서 노드를 배치한 후, 셋업 서버에서 상기 배치된 센서 노드에 상기 배치된 정사각형의 영역 및 상기 센서 노드 고유 넘버로 구성된 식별자를 부여하는 단계, 상기 식별자가 부여된 각각의 센서 노드에 셋업 서버에서 상기 식별자를 기반으로 상기 센서 노드의 마스터 키를 생성하는 단계, 상기 마스터 키가 생성된 센서 노드에서 상기 센서 노드와 위치적으로 연관되어 링크되는 다른 센서 노드와의 보안키를 생성하여 상기 보안키, 상기 다른 센서 노드의 식별자 및 상기 센서 노드의 마스터 키를 상기 센서 노드에 저장하는 단계, 및 상기 보안키, 식별자 및 마스터 키를 저장한 센서 노드를 센서 네트워크에 배치하고, 상기 센서 노드의 마스터 키에 따라 상기 센서 네트워크에 배치된 이웃 노드와 보안키를 공유하는 단계를 포함하는 위치 기반의 보안키 공유 방법을 제공한다.
- <22> 상기 세 번째 기술적 과제를 달성하기 위하여 본 발명은,
- <23> 복수의 센서 노드들이 배치될 위치를 정사각형 모양의 영역으로 분할하고, 상기 분할된 정사각형의 영역에 센서 노드를 배치한 후, 셋업 서버에서 상기 배치된 센서 노드에 상기 배치된 정사각형의 영역 및 상기 센서 노드 고유 넘버로 구성된 식별자를 부여하는 단계, 상기 식별자가 부여된 각각의 센서 노드에 셋업 서버에서 상기 식별자를 기반으로 상기 센서 노드의 마스터 키를 생성하고, 상기 센서 노드와 위치적으로 연관되어 링크되는 다른 센서 노드와의 보안키, 상기 다른 센서 노드의 식별자 및 상기 센서 노드의 마스터 키를 저장하는 단계, 상기 센서 노드를 센서 네트워크에 배치하고, 상기 센서 노드에서 상기 센서 네트워크에 배치된 이웃 노드와 보안키를 공유하는 단계, 상기 센서 네트워크에 새로운 센서 노드가 추가하고자 하는 경우, 상기 셋업 서버에서 상기 새로운 센서 노드가 배치될 상기 정사각형 영역을 지정하고, 상기 지정된 정사각형 영역에 따라 상기 새로운 센서 노드의 식별자 및 마스터 키를 부여하는 단계, 상기 새로운 센서 노드에서 상기 지정된 정사각형 영역에 따라 상기 셋업 서버에 저장된 데이터베이스를 이용하여 상기 새로운 센서 노드와 위치적으로 연관되어 링크되는 센서 노드와의 보안키, 상기 식별자 및 마스터 키를 저장하는 단계, 및 상기 새로운 센서 노드를 상기 센서 네

트위크에 배치하고, 상기 새로운 센서 노드의 마스터 키에 따라 상기 새로운 센서 노드와 이웃 노드간의 보안키를 설정하는 단계를 포함하는 위치 기반의 보안키 추가 방법을 제공한다.

<24> 이하, 본 발명의 바람직한 실시예를 첨부도면에 의거하여 상세히 설명하기로 한다.

<25> 그러나, 다음에 예시하는 본 발명의 실시예는 여러 가지 다른 형태로 변형할 수 있으며, 본 발명의 범위가 다음에 상술하는 실시예에 한정되는 것은 아니다. 본 발명의 실시예는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 더욱 완전하게 설명하기 위하여 제공된다.

<26> 도 1은 본 발명의 일 실시예에 따른 위치 기반의 보안키 사전 분배 방법의 흐름도이고, 도 2는 도 1의 위치 기반의 보안키 사전 분배 방법에 적용되는 센서 노드들이 배치될 정사각형 영역의 지역을 도시한 것이고, 도 3은 도 1에 적용되는 센서 노드의 이웃 그룹의 집합을 도시한 것이다.

<27> 한편, 하기의 표 1은 아래에 상술할 기호에 대한 설명이다. 이는 상세한 설명의 전반에 공통적으로 적용되며, 실시형태에 따라 변형할 수 있음은 물론이다.

표 1

기호	설명
$A(i, j)$	센서 필드에 센서 노드가 배치될 분할된 단위 영역
$G(i, j)$	$A(i, j)$ 에 배치될 센서 노드의 그룹
$AG[G(i, j)]$	$G(i, j)$ 와 인접한 4개의 그룹의 집합, $\{G(i-1, j-1), G(i-1, j), G(i-1, j+1), G(i, j-1)\}$
$N_k^{i,j}$	그룹 $G(i, j)$ 에 속한 k번째 센서 노드의 식별자
m	동일 그룹에 속한 센서 노드와 보안키를 사전 배치한 보안키의 수
n	단위 그룹의 센서 노드의 수
$K_{N_k^{i,j}}$	노드 $N_k^{i,j}$ 의 마스터 키
p	이웃 노드와 보안키를 공유할 확률
$\mathcal{PRF}_k(N)$	마스터키가 k 인 센서 노드 N 의 의사 난수 함수값

<28>

<29> 도 1을 참조하면 우선, 복수의 센서 노드들이 배치될 지역을 정사각형 모양의 영역으로 분할하고, 상기 분할된 정사각형의 영역에 센서 노드를 배치한 후, 셋업 서버에서 상기 배치된 센서 노드에 상기 배치된 정사각형의 영역 및 상기 센서 노드 고유 넘버로 구성된 식별자를 부여한다(110 과정).

<30> 즉, 복수의 센서 노드들이 배치될 지역을 도 2에 도시된 바와 같이 $I \times J$ 개의 작은 정사각형 모양의 영역들로 나눈다. 그리고, 나누어진 정사각형 영역의 각각을 $A(i, j)$ ($1 \leq i \leq I, 1 \leq j \leq J$)라고 한다.

<31> 이 경우, 전체 센서 노드들의 수를 N 이라 하고, 상기 N 개의 센서 노드를 $I \times J$ 개의 그룹 $G(i, j)$ ($1 \leq i \leq I, 1 \leq j \leq J$)에 배치할 수 있다.

<32> 각각의 그룹 $G(i, j)$ 는 n 개의 센서 노드들로 구성되어 있고 영역 $A(i, j)$ 에 임의로 배치되어 질 수 있다.

<33> 그러면 셋업 서버(setup server)에서 각각의 센서 노드의 식별자를 상기 배치된 정사각형의 영역 및 상기 센서 노드 고유 넘버로 구성된 식별자를 부여한다.

<34> 그룹 $G(i,j)$ 에 있는 각각의 센서 노드의 식별자(Identifier:ID)는 $N_k^{i,j} = \{(i,j),k\} (k=1,...,n)$ 로 나타낼 수 있다. 이때, (i,j) 는 그룹의 식별자이고, k 는 각각의 그룹 안에 있는 센서 노드들에게 부여된 유일한 식별번호로 1에서 n 까지의 정수값을 가지게 된다.

<35> 그 다음, 상기 식별자가 부여된 각각의 센서 노드에 상기 셋업 서버에서 상기 식별자를 기반으로 상기 센서 노드의 마스터 키를 생성한다(120 과정).

<36> 셋업 서버는 센서 노드들에게 키를 사전 분배하는데, 이는 각각의 센서 노드 $N_k^{i,j}$ 를 위한 마스터 키(Master Key)인 $K_{N_k^{i,j}}$ 를 생성한다. 마스터 키는 각 센서 노드만이 저장하고 있는 고유의 키로 자신의 마스터 키를 이용하여 후술할 보안키를 생성하고 이 보안키를 이용하여 이웃 노드와 데이터를 상호 송수신하게 된다.

<37> 그 다음, 상기 마스터 키가 생성된 센서 노드에서 상기 센서 노드와 위치적으로 연관되어 링크되는 다른 센서 노드와의 보안키를 생성한다(130 과정).

<38> 상기 분할된 영역 $A(i,j)$ 에 대응되는 센서 노드의 그룹을 $G(i,j)$ 라 할 때, 자신의 그룹이 속한 정사각형 영역과 위치적으로 연관되어 링크되는 다른 센서 노드와의 보안키를 생성한다.

<39> 여기서, 상기 정사각형 영역과 위치적으로 연관되어 링크되는 다른 센서 노드는 상기 센서 노드가 배치된 정사각형 영역과 수직으로 서로 접하는 정사각형 영역에 배치된 노드일 수 있다.

<40> 즉, 자신의 그룹이 속한 정사각형 영역과 상, 하, 좌, 우로 접하는 정사각형 영역에 속한 센서 노드의 그룹의 집합을 $AG[G(i,j)]$ 이라고 정의하면, 상기 도시된 도 3과 같이 $AG[G(i,j)] = \{G(i,j), G(i-1,j), G(i,j-1), G(i,j+1), G(i+1,j)\}$ 이 될 수 있다. 그룹 $G(i,j)$ 에 있는 각각의 센서 노드 $N_k^{i,j}$ 에 대해 셋업 서버는 그룹 $G(i',j') (\in AG[G(i,j)])$ 로부터 각각 m 개씩 센서 노드를 선택한다.

<41> 여기서 m 의 값은 한 그룹의 센서 노드의 수 n 과 센서 네트워크에서 미리 결정되는 단위 센서 노드가 이웃 노드와 연결될 확률 p 에 의해 정해질 수 있다.

<42> 이는 하기의 수학적 식 1로 표현되어 질 수 있다.

수학적 식 1

$$n = \frac{m}{p}$$

<43>

<44> 한편, 셋업 서버는 그룹 $G(i',j') (\in AG[G(i,j)])$ 로부터 각각 m 개씩 센서 노드를 선택하며, 식별자가 $N_t^{i',j'} (t = k+1(\bmod n), \dots, k+m(\bmod n))$ 인 센서 노드를 선택한 후 의사 난수 함수(Pseudo

Random Function:PRF)와 마스터 키를 이용하여 센서 노드 $N_k^{i,j}$ 와 $N_t^{i',j'}$ 사이의 보안키 $K_{N_k^{i,j}, N_t^{i',j'}}$ 를 하기의 수학적 식 2에 의해 연산한다.

수학식 2

$$K_{N_k^{i,j}, N_t^{i',j'}} = PRF_{K_{N_t^{i',j'}}}(N_k^{i,j})$$

<45>

<46> 여기서, $PRF_k(N)$ 의 의미는 마스터키가 k 인 노드 N 의 의사 난수 함수값을 연산하는 것이다.

<47>

마지막으로, 상기 다른 센서 노드의 식별자, 상기 센서 노드의 마스터 키 및 공유된 보안키를 상기 센서 노드에 저장한다(140 과정).

<48>

상기 이웃 그룹 $AG[G(i,j)]$ 에 있는 각각의 5개의 집합에 대하여 소정의 갯수 m 개씩 $5m$ 개의 보안키를 연산한 후 그룹 $G(i,j)$ ($1 \leq i \leq I, 1 \leq j \leq J$)에 있는 각각의 센서 노드 $N_k^{i,j}$ 에 대해 $5m$ 개의 센서 노드들과의 보안키와 상기 센서 노드 $N_k^{i,j}$ 와 보안키를 생성한 센서 노드 $N_t^{i',j'}$ 의 식별자 쌍($N_t^{i',j'}, K_{N_k^{i,j}, N_t^{i',j'}}$) ($t = k+1(\text{mod } n), \dots, k+m(\text{mod } n), G(i',j') \in AG[G(i,j)]$)과 센서 노드 자신의 마스터 키 $K_{N_k^{i,j}}$ 를 키 정보로 저장한다.

<49>

한편, 센서 노드 $N_k^{i,j}$ 는 $N_t^{i',j'}$ 와의 보안키를 사전에 저장하지만, $N_t^{i',j'}$ 는 자신의 마스터 키를 이용하여 보안키를 연산할 수 있으므로 상기 보안키를 사전에 저장하지 않는다.

<50>

따라서, $N_k^{i,j}$ 가 $5m$ 개의 보안키를 사전에 저장하지만 센서 노드 $N_t^{i',j'}$ ($t = k-1(\text{mod } n), \dots, k-m(\text{mod } n), G(i',j') \in AG[G(i,j)]$)와의 보안키를 저장하지 않고 실제로 연산할 수 있으므로, 실제로는 $10m$ 개의 보안키를 저장한 것과 동일한 결과를 얻을 수 있다.

<51>

도 4는 본 발명의 다른 실시예에 따른 위치 기반의 보안키 공유 방법의 흐름도이다.

<52>

도 4를 참조하면, 복수의 센서 노드들이 배치될 지역을 정사각형 모양의 영역으로 분할하고, 상기 분할된 정사각형의 영역에 센서 노드를 배치한 후, 셋업 서버에서 상기 배치된 센서 노드에 상기 배치된 정사각형의 영역 및 상기 센서 노드 고유 넘버로 구성된 식별자를 부여한다(410 과정)

<53>

그 다음, 상기 식별자가 부여된 각각의 센서 노드에 셋업 서버에서 상기 식별자를 기반으로 상기 센서 노드의 마스터 키를 생성한다(420 과정).

<54>

그 다음, 상기 마스터 키가 생성된 센서 노드에서 상기 센서 노드와 위치적으로 연관되어 링크되는 다른 센서 노드와의 보안키, 상기 다른 센서 노드의 식별자 및 상기 센서 노드의 마스터 키를 저장한다(430 과정).

<55>

한편, 상기 410 과정 내지 430 과정은 전술한 바와 동일하므로, 중복된 상술은 생략하기로 한다.

<56>

마지막으로, 상기 보안키, 식별자 및 마스터 키를 저장한 센서 노드를 센서 네트워크에 배치하고, 상기 센서 노드의 마스터 키에 따라 상기 센서 네트워크에 배치된 이웃 노드와 보안키를 공유한다(440 과정).

<57>

이는, 상기 보안키, 식별자 및 마스터 키를 저장한 센서 노드들이 배치되고 난 후, 각각의 센서 노드들은 이웃 노드들과 보안키를 설립하게 된다.

<58>

각각의 센서 노드는 보안키를 가지고 있는 식별자의 목록을 브로드캐스팅(broadcasting)하는데 이웃 노드들로부터 보안키를 가지고 있는 센서 노드의 식별자 목록을 전송 받은 후, 만약 자신의 센서 노드의 식별자가 브로드캐스팅된 이웃 노드의 목록에 있다면 센서 노드 자신의 마스터 키를 이용하여 보안키를 연산하고, 연산된 보안

키를 이용하여 이웃 노드와 보안키를 공유하게 된다.

- <59> 만약, 센서 노드 자신의 식별자가 브로드캐스팅된 이웃 노드의 목록에 없다면 이미 브로드캐스팅한 센서 노드와 보안키를 설립한 다른 이웃 노드를 이용하여 보안키를 공유한다.
- <60> 상세히 살펴보면, 상기 센서 네트워크에 배치된 다른 센서 노드에서 상기 다른 센서 노드가 저장하고 있는 식별자 목록을 브로드캐스팅하면, 상기 브로드캐스팅된 식별자 목록에 상기 센서 노드의 식별자가 포함된 경우, 상기 센서 노드에서 자신의 마스터 키를 이용하여 상기 센서 노드와 상기 다른 센서 노드의 보안키를 연산한다.
- <61> 상기 센서 노드에서 자신의 마스터 키를 이용하여 상기 센서 노드와 상기 다른 센서 노드간의 보안키를 연산하는 방법은 상기의 수학식 2에 의할 수 있다.
- <62> 그런 다음, 상기 센서 노드와 상기 다른 센서 노드에서 상기 연산된 보안키를 공유하고, 공유된 보안키를 이용하여 상기 센서 노드와 상기 다른 센서 노드 사이에 데이터 교환이 이루어진다.
- <63> 한편, 상기 센서 네트워크에 배치된 다른 센서 노드에서 상기 다른 센서 노드가 저장하고 있는 식별자 목록을 브로드캐스팅하고, 상기 브로드캐스팅된 식별자 목록에 상기 센서 노드의 식별자가 포함되지 않은 경우, 상기 센서 노드의 이웃 노드 중 상기 다른 센서 노드와 보안키를 공유한 또 다른 센서 노드를 이용하여 상기 다른 센서 노드와 상기 센서 노드에서 보안키를 공유한다.
- <64> 이는 상기 센서 노드는 통상적으로 저장하고 있는 이웃 노드 리스트를 통하여 상기 이웃 노드 리스트 중에서 상기 브로드캐스팅한 센서 노드를 저장하고 있는지의 여부를 알 수 있다.
- <65> 따라서, 상기 센서 노드의 이웃 노드 중에서 상기 브로드캐스팅한 센서 노드와 보안키를 설립한 센서 노드가 존재하는 경우, 상기 센서 노드는 상기 이웃 노드와 보안키를 설립하고, 상기 이웃 노드를 통하여 브로드캐스팅한 센서 노드와 정보 데이터를 송수신할 수 있게 된다.
- <66> 도 5는 본 발명의 또 다른 실시예에 따른 위치 기반의 보안키 추가 방법의 흐름도이다.
- <67> 도 5를 참조하면, 우선, 복수의 센서 노드들이 배치될 지역을 정사각형 모양의 영역으로 분할하고, 상기 분할된 정사각형의 영역에 센서 노드를 배치한 후, 셋업 서버에서 상기 배치된 센서 노드에 상기 배치된 정사각형의 영역 및 상기 센서 노드 고유 넘버로 구성된 식별자를 부여한다(510 과정).
- <68> 그 다음, 상기 식별자가 부여된 각각의 센서 노드에 셋업 서버에서 상기 식별자를 기반으로 상기 센서 노드의 마스터 키를 생성하고, 상기 센서 노드와 위치적으로 연관되어 링크되는 다른 센서 노드와의 보안키, 상기 다른 센서 노드의 식별자 및 상기 센서 노드의 마스터 키를 저장한다(520 과정).
- <69> 그 다음, 상기 센서 노드를 센서 네트워크에 배치하고, 상기 센서 노드에서 상기 센서 네트워크에 배치된 이웃 노드와 보안키를 공유한다(530 과정).
- <70> 상기 510과정 내지 530과정은 상기 상술한 내용과 동일하므로, 중복된 상술은 생략하기로 한다.
- <71> 그 다음, 상기 센서 네트워크에 새로운 센서 노드가 추가하고자 하는 경우, 상기 셋업 서버에서 상기 새로운 센서 노드가 배치될 상기 정사각형 영역을 지정하고, 상기 지정된 정사각형 영역에 따라 상기 새로운 센서 노드의 식별자 및 마스터 키를 부여한다(540 과정).
- <72> 이는, 셋업 서버에서 이전에 센서 노드가 센서 네트워크에 배치되기 전의 센서 노드의 정사각형 영역에 배치된 그룹을 저장하므로, 이를 기반으로 새로운 센서 노드의 식별자 및 마스터 키를 부여한다.
- <73> 상기 새로운 센서 노드에서 상기 지정된 정사각형 영역에 따라 상기 셋업 서버에 저장된 데이터베이스를 이용하여 상기 새로운 센서 노드와 위치적으로 연관되어 링크되는 센서 노드와의 보안키, 상기 식별자 및 상기 새로운 센서 노드 자신의 마스터 키를 저장한다(550 과정).
- <74> 즉, 새로운 노드가 추가되어 질 때, 셋업 서버는 새로운 센서 노드가 속하게 될 그룹 $G(i,j)$ 를 정하고, 이를 통하여 상술한 $AG[G(i,j)]$ 를 구하게 된다. 이는 전술한 보안키 사전 분배 방법과 마찬가지로 $5m$ 개의 키를 사전 저장한다.
- <75> 마지막으로, 상기 새로운 센서 노드를 상기 센서 네트워크에 배치하고, 상기 새로운 센서 노드의 마스터 키에

따라 이웃 노드와 보안키를 설정한다(560 과정).

- <76> 이미 형성되어 있는 센서 네트워크에 있는 센서 노드들은 새로 추가되는 노드와의 보안키를 가지고 있지 않으므로 새로운 노드가 이웃 노드와 보안키를 공유할 확률은 반으로 감소한다.
- <77> 그러나, 이미 형성된 네트워크는 모두 연결되어 있기 때문에 이미 연결된 이웃 노드들을 이용하여 사전 저장된 보안키가 없는 이웃 노드들과 보안키를 설립할 수 있다.
- <78> 만약, 센서 노드의 밀도가 낮은 그룹에 새로운 센서 노드가 추가된다면 그 그룹에 있는 노드의 수가 적으므로 거의 모든 센서 노드와의 보안키를 사전에 저장할 수 있게 된다.
- <79> 이와 같이, 필요시 센서 노드를 추가할 경우에, 공격자에게 물리적으로 노출되기 쉬운 환경에서, 공격자의 선택적인 노드 포획에 안전하게 된다.
- <80> 왜냐하면, 공격자가 선택적으로 노드를 포획한다 하더라도 포획된 노드에 저장된 보안키 연산에 사용된 마스터 키를 알 수 없으므로, 이를 통하여 다른 센서 노드와의 보안키를 설립할 수 없기 때문에 공격자의 선택적인 노드 포획이 있다 하더라도 정보의 유출을 차단할 수 있기 때문이다.
- <81> 그리고, 간단한 PRF 연산 한 번으로 보안키를 설립할 수 있으므로 센서 네트워크에서 보안키 설립에 있어 연산량도 감소하게 된다.
- <82> 도 6은 본 발명의 일 실시예에 따른 위치 기반의 보안키 사전 분배 방법과 종래의 방법에 의한 센서 노드가 저장하는 보안키의 수를 도시한 그래프이다.
- <83> 도 6을 참조하면, 종래의 보안키 분배 방법으로 알려진 EG-D 방법(610)과 GGD 방법(620)에 의한 단위 센서 노드의 보안키 저장 수와 본 발명의 일 실시예(630)에 따른 센서 노드의 보안키 저장수를 비교하면, 본 발명의 단위 센서 노드의 보안키 저장수가 EG-D 방법(610)과 GGD 방법(620)에 의한 단위 센서 노드의 보안키 저장 수의 50% 이하를 나타내고 있음을 알 수 있다.
- <84> 이는 상술한 바와 같이 $N_k^{i,j}$ 가 m개의 보안키를 사전에 저장하지만 센서 노드 $N_t^{i',j'}(t = k-1(\bmod n), \dots, k-m(\bmod n), G(i',j') \in AG[G(i,j))$ 와의 보안키를 저장하지 않고 실제로 연산할 수 있으므로, 실제로는 2m개의 보안키를 저장한 것과 동일한 효과를 얻을 수 있으므로 이는 당연한 결과라 하겠다.
- <85> 상기 도 6에서 알 수 있는 바와 같이 센서 노드가 상대적으로 적은 수의 보안키를 저장하고도 간단한 연산을 통하여 보안키를 설립할 수 있으므로, 센서 네트워크 망을 구성하는 센서 노드의 보안키 생성을 저전력으로 구현할 수 있다.
- <86> 본 발명은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터(정보 처리 기능을 갖는 장치를 모두 포함한다)가 읽을 수 있는 코드로서 구현하는 것이 가능하다.
- <87> 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광데이터 저장장치 등이 있다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.
- <88> 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사항에 의해 정해져야 할 것이다.

발명의 효과

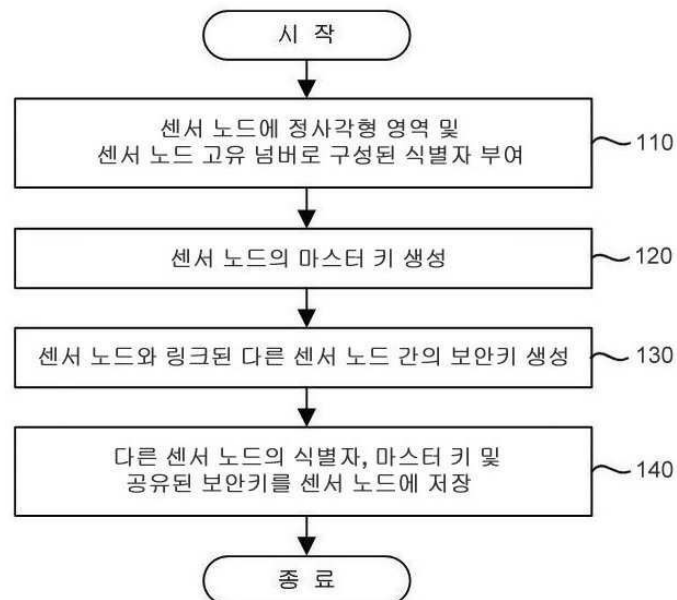
- <89> 상술한 바와 같이 본 발명에 의하면, 무선 센서 네트워크에서 위치기반의 보안키를 설정하여, 최소 비용으로 최대 이익을 얻기 위한 공격자의 선택적인 노드 포획을 고려한 안전한 보안키를 설정함으로써 센서 노드들 사이의 안전한 통신이 가능하고, 보안키 설립시 통신 및 계산량이 적고 메모리 요구량이 적어서 자원 제약적인 센서 네트워크에 적합하며 대규모 네트워크의 지원이 가능하고 안전하게 새로운 노드의 추가가 가능하고, 저전력으로 보안키의 생성 및 유지가 가능하며 보안이 중요하게 요구되는 응용환경에 쉽게 적용할 수 있는 효과가 있다.

도면의 간단한 설명

- <1> 도 1은 본 발명의 일 실시예에 따른 위치 기반의 보안키 사전 분배 방법의 흐름도이다.
- <2> 도 2는 도 1의 위치 기반의 보안키 사전 분배 방법에 적용되는 센서 노드들이 배치될 정사각형 영역의 지역을 도시한 것이다.
- <3> 도 3은 도 1에 적용되는 센서 노드의 이웃 그룹의 집합을 도시한 것이다.
- <4> 도 4는 본 발명의 다른 실시예에 따른 위치 기반의 보안키 공유 방법의 흐름도이다.
- <5> 도 5는 본 발명의 또 다른 실시예에 따른 위치 기반의 보안키 추가 방법의 흐름도이다.
- <6> 도 6은 본 발명의 일 실시예에 따른 위치 기반의 보안키 사전 분배 방법과 종래의 방법에 의한 센서 노드가 저장하는 보안키의 수를 도시한 그래프이다.

도면

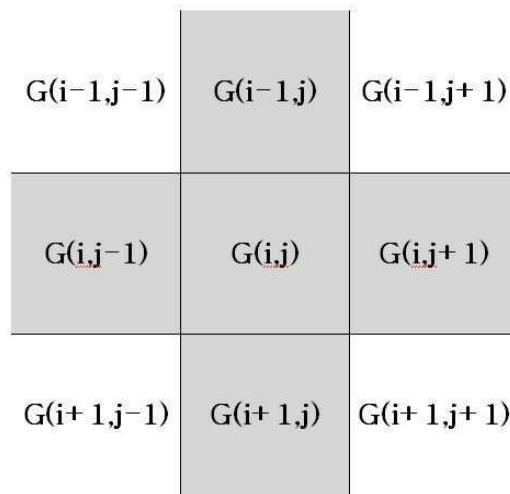
도면1



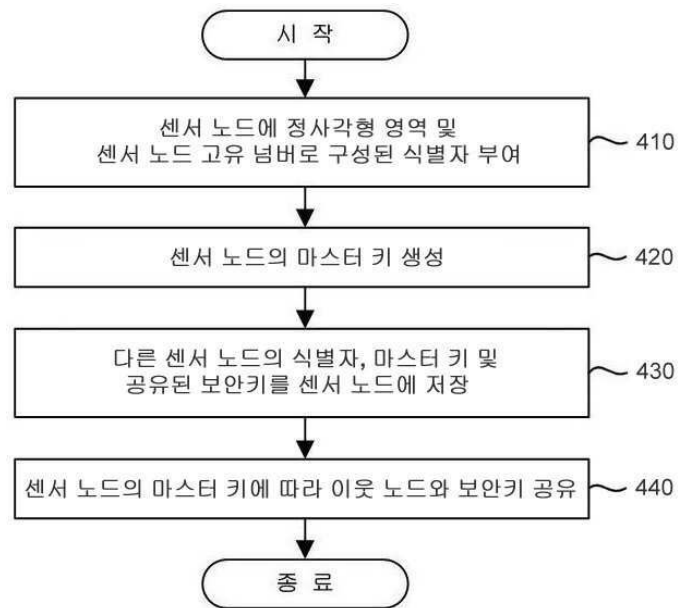
도면2

$A(1,1)$	$A(1,2)$	$A(1,3)$		$A(1,J)$
$A(2,1)$	$A(2,2)$	$A(2,3)$		$A(2,J)$
$A(3,1)$	$A(3,2)$	$A(3,3)$		$A(3,J)$
⋮	⋮	⋮	⋱	
$A(l,1)$	$A(l,2)$	$A(l,3)$		$A(l,J)$

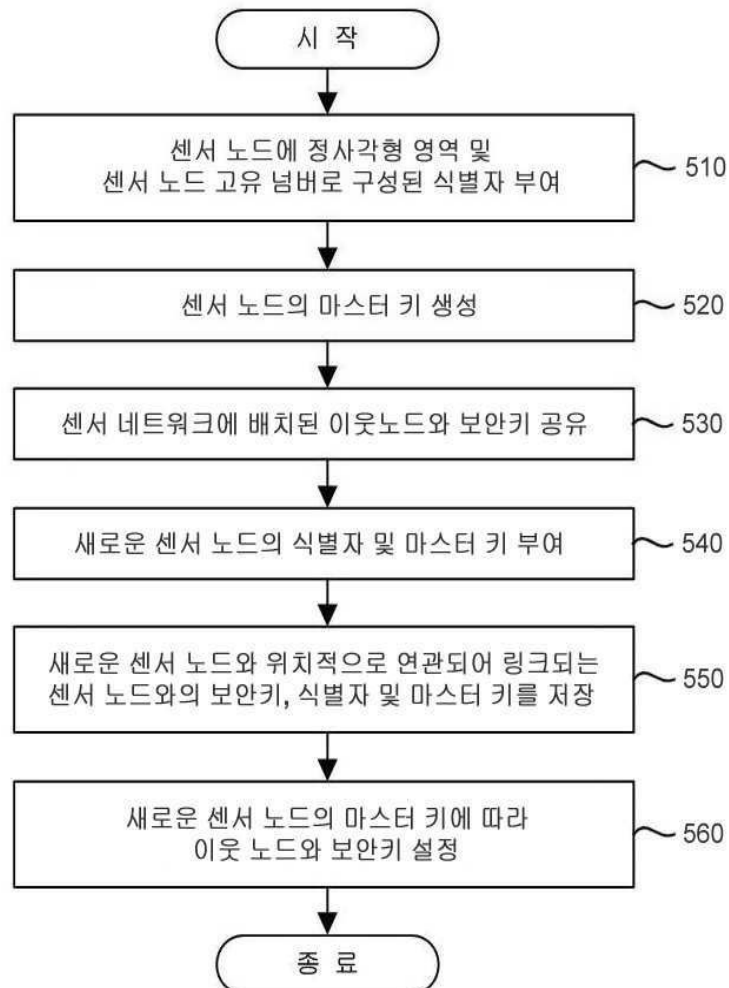
도면3



도면4



도면5



도면6

