



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0053117
(43) 공개일자 2009년05월27일

(51) Int. Cl.

H04L 9/28 (2006.01) H04L 12/22 (2006.01)

(21) 출원번호 10-2007-0119786

(22) 출원일자 2007년11월22일

심사청구일자 2007년11월22일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

김용호

서울 성북구 안암동5가 고려대학교 정보보호대학원 140호

조관태

서울 성북구 안암동5가 고려대학교 정보보호대학원 140호

(뒷면에 계속)

(74) 대리인

현종철

전체 청구항 수 : 총 18 항

(54) 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법, 장치 및 이에 사용되는 컴퓨터 판독가능 기록매체

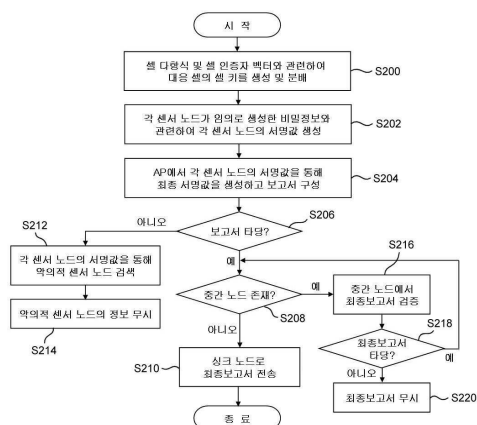
(57) 요약

본 발명은 센서필드의 셀마다 독립적인 셀 다항식 및 셀 인증자 벡터를 사용하는 센서 네트워크에서의 위조 데이터 삽입공격을 방지하는 방법, 장치, 및 컴퓨터 판독가능 기록매체에 관한 것이다.

본 발명에 따른 센서 네트워크에서의 위조 데이터 삽입공격을 방지하는 방법은, 센서필드를 구획하는 셀(cell)들에 각각 대응하는 셀 다항식 및 셀 인증자 벡터와 관련하여 상기 셀 다항식 및 상기 셀 인증자 벡터에 대응하는 셀의 셀 키를 생성하고 상기 셀 내의 센서 노드에 상기 셀 키를 분배하는 셀 키 분배 단계; 상기 셀에서 상기 셀 키를 분배받은 센서 노드가 이벤트를 발견하면 상기 이벤트를 발견한 상기 센서 노드 중에서 데이터 집합 노드(data aggregation node)를 선출하는 데이터 집합 노드 선출 단계; 상기 이벤트를 발견한 상기 센서 노드가 임의로 선택한 비밀정보를 통해 센서 노드 서명값을 생성하는 센서 노드 서명값 생성 단계;

상기 센서 노드 서명값을 통해 상기 데이터 집합 노드에서 최종 서명값을 생성하고 보고서를 구성하는 단계; 및 상기 보고서를 검증하여 상기 보고서가 정당하면 상기 보고서를 싱크 노드로 전송하는 검증 및 전송 단계를 포함한다.

대표도 - 도2



(72) 발명자

이화성

서울 성북구 안암동5가 고려대학교 정보보호대학원
140호

천지영

서울 성북구 안암동5가 고려대학교 정보보호대학원
138호

임종인

서울 종로구 내수동 95 삼성파크팰리스 101-901

이동훈

경기 고양시 일산동구 정발산동 밤가시마을 901동
201호

특허청구의 범위

청구항 1

센서 네트워크에서의 위조 데이터 삽입공격을 방지하는 방법에 있어서,

센서필드를 구획하는 셀(cell)들에 각각 대응하는 셀 다항식 및 셀 인증자 벡터와 관련하여 상기 셀 다항식 및 상기 셀 인증자 벡터에 대응하는 셀의 셀 키를 생성하고 상기 셀 내의 센서 노드에 상기 셀 키를 분배하는 셀 키 분배 단계;

상기 셀에서 상기 셀 키를 분배받은 센서 노드가 이벤트를 발견하면 상기 이벤트를 발견한 상기 센서 노드 중에서 데이터 집합 노드(data aggregation node)를 선출하는 데이터 집합 노드 선출 단계;

상기 이벤트를 발견한 상기 센서 노드가 임의로 선택한 비밀정보를 통해 센서 노드 서명값을 생성하는 센서 노드 서명값 생성 단계;

상기 센서 노드 서명값을 통해 상기 데이터 집합 노드에서 최종 서명값을 생성하고 보고서를 구성하는 단계; 및

상기 보고서를 검증하여 상기 보고서가 정당하면 상기 보고서를 싱크 노드로 전송하는 검증 및 전송 단계를 포함하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법.

청구항 2

제1항에 있어서, 상기 검증 및 전송 단계는,

상기 보고서를 검증하여 상기 보고서가 정당하지 않으면, 부당한 데이터를 전송한 센서 노드를 검색하여, 상기 검색된 센서 노드의 정보를 무시하는 검색 및 무시 단계를 더 포함하는 것을 특징으로 하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법.

청구항 3

제2항에 있어서, 상기 검색 및 무시 단계는,

상기 센서 노드 서명값을 검사함으로써 달성되는 것을 특징으로 하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 방법은,

상기 데이터 집합 노드와 상기 싱크 노드 사이에 중간 노드가 있는 경우, 상기 중간 노드에서 상기 보고서를 검증하여 상기 보고서가 정당하지 않으면 상기 보고서를 무시하는 단계를 더 포함하는 것을 특징으로 하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법.

청구항 5

제1항에 있어서, 상기 셀 키 분배 단계는,

범위 기반 셀 키 분배 방식에 의하는 단계인 것을 특징으로 하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법.

청구항 6

제1항에 있어서, 상기 셀 키 분배 단계는,

범위 제한 없는 셀 키 분배 방식에 의하는 단계인 것을 특징으로 하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법.

청구항 7

센서 네트워크에서의 위조 데이터 삽입공격을 방지하는 장치에 있어서,

상기 센서 네트워크에서의 위조 데이터 삽입공격 방지 장치는, 센서필드의 동일 셀 내에 위치하는 센서 노드들

을 포함하고, 각각의 셀에 대응하는 셀 다항식 및 셀 인증자 벡터와 관련하여 셀 키를 생성 및 분배하는 센서부;

상기 센서부 및 싱크 노드 사이에서 정보를 전달하는 중계부; 및

상기 센서부 및 상기 중계부의 동작을 제어하는 제어부를 포함하고,

상기 센서부의 상기 센서 노드는, 이벤트를 발견하는 경우 상기 이벤트를 발견한 센서 노드 중에서 데이터 집합 노드를 선출하고, 상기 이벤트를 발견한 상기 센서 노드가 위치한 셀에 대응하는 셀 다항식 및 셀 인증자 벡터와 관련하여 임의로 비밀정보를 선택하고, 그리고 상기 비밀정보를 통해 센서 노드 서명값 생성하고, 그리고,

상기 선출된 데이터 집합 노드는, 상기 센서 노드 서명값을 통해 최종 서명값을 생성하고, 상기 최종 서명값을 통해 보고서를 구성하고, 그리고 상기 보고서를 검증하여 정당하면 상기 보고서를 상기 싱크노드로 전송하는 것을 특징으로 하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 장치.

청구항 8

제7항에 있어서, 상기 선출된 데이터 집합 노드는,

상기 보고서를 검증하여 상기 보고서가 정당하지 않으면, 부당한 데이터를 전송한 센서 노드를 검색하여, 상기 검색된 센서 노드의 정보를 무시하는 것을 특징으로 하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 장치.

청구항 9

제8항에 있어서, 상기 선출된 데이터 집합 노드는,

상기 센서 노드 서명값을 검사하여 상기 부당 데이터 전송 센서 노드를 검색하는 것을 특징으로 하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 장치.

청구항 10

제7항 내지 제9항 중 어느 한 항에 있어서, 상기 중계부는,

상기 데이터 집합 노드와 상기 싱크 노드 사이에 위치하는 중간 노드를 포함하고, 상기 중간 노드는 상기 보고서를 검증하여 상기 보고서가 정당하지 않으면 상기 보고서를 무시하는 것을 특징으로 하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 장치.

청구항 11

제7항에 있어서, 상기 센서부는,

범위 기반 셀 키 분배 방식에 의하여 셀 키를 생성 및 분배하는 것을 특징으로 하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 장치.

청구항 12

제7항에 있어서, 상기 센서부는,

범위 제한 없는 셀 키 분배 방식에 의하여 셀 키를 생성 및 분배하는 것을 특징으로 하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 장치.

청구항 13

센서 네트워크를 제어하는 컴퓨터가 판독할 수 있는 컴퓨터 판독가능 기록매체에 있어서,

상기 컴퓨터 판독가능 기록매체에 센서 네트워크에서의 위조 데이터 삽입공격 방지 프로그램이 기록되어 있고, 상기 프로그램은,

센서필드를 구획하는 셀(cell)들에 각각 대응하는 셀 다항식 및 셀 인증자 벡터와 관련하여 상기 셀 다항식 및 상기 셀 인증자 벡터에 대응하는 셀의 셀 키를 생성하도록 하고 상기 셀 내의 센서 노드에 상기 셀 키를 분배하도록 하는 셀키 분배 코드;

상기 셀에서 상기 셀 키를 분배받은 센서 노드가 이벤트를 발견하면 상기 이벤트를 발견한 상기 센서 노드 중에서 데이터 집합 노드(data aggregation node)를 선출하도록 하는 데이터 집합 노드 선출 코드;

상기 이벤트를 발견한 상기 센서 노드가 임의로 선택한 비밀정보를 통해 센서 노드 서명값을 생성하도록 하는 센서 노드 서명값 생성 코드;

상기 센서 노드 서명값을 통해 상기 데이터 집합 노드에서 최종 서명값을 생성하고 보고서를 구성하도록 하는 코드; 및

상기 보고서를 검증하여 상기 보고서가 정당하면 상기 보고서를 싱크 노드로 전송하도록 하는 검증 및 전송 코드를 포함하는 컴퓨터 판독가능 기록매체.

청구항 14

제13항에 있어서, 상기 검증 및 전송 코드는,

상기 보고서를 검증하여 상기 보고서가 정당하지 않으면, 부당한 데이터를 전송한 센서 노드를 검색하여, 상기 검색된 센서 노드의 정보를 무시하도록 하는 검색 및 무시 코드를 더 포함하는 것을 특징으로 하는 컴퓨터 판독가능 기록매체.

청구항 15

제14항에 있어서, 상기 검색 및 무시 코드는,

상기 센서 노드 서명값 검사를 통해 상기 부당한 데이터를 전송한 상기 센서 코드를 검색하도록 하는 코드를 포함하는 것을 특징으로 하는 컴퓨터 판독가능 기록매체.

청구항 16

제13항 내지 제15항 중 어느 한 항에 있어서, 상기 컴퓨터 판독가능 기록매체는,

상기 데이터 집합 노드와 상기 싱크 노드 사이에 중간 노드가 있는 경우, 상기 중간 노드에서 상기 보고서를 검증하여 상기 보고서가 정당하지 않으면 상기 보고서를 무시하도록 하는 코드를 더 포함하는 것을 특징으로 하는 컴퓨터 판독가능 기록매체.

청구항 17

제13항에 있어서, 상기 셀 키 분배 코드는,

범위 기반 셀 키 분배 방식을 이용하는 코드인 것을 특징으로 하는 컴퓨터 판독가능 기록매체.

청구항 18

제13항에 있어서, 상기 셀 키 분배 코드는,

범위 제한 없는 셀 키 분배 방식을 이용하는 코드인 것을 특징으로 하는 컴퓨터 판독가능 기록매체.

명세서

발명의 상세한 설명

기술 분야

<1> 본 발명은 센서 네트워크에서 위조 데이터 삽입공격을 방지하는 방법 및 장치와 이에 사용되는 컴퓨터 판독가능 기록매체에 관한 것이며, 더 상세하게는 센서필드의 셀마다 독립적인 셀 다항식 및 셀 인증자 벡터를 사용하는 센서 네트워크에서의 위조 데이터 삽입공격을 방지하는 방법, 장치, 및 컴퓨터 판독가능 기록매체에 관한 것이다.

배경 기술

<2> 무선 센서 네트워크는 유비쿼터스 컴퓨팅 구현을 위한 기반 네트워크로 초경량, 초전력의 많은 센서 노드(sensor node)들로 구성된 무선 네트워크이다. 무선 센서 네트워크의 센서 노드들은 무작위로 배치되기 때문에

물리적 공격에 의해 쉽게 노출될 수 있다. 예를 들어 공격자는 센서 노드를 획득함으로써 그 메모리 안에 있는 비밀 정보를 얻을 수 있다.

<3> 상기와 같은 공격은 위조된 데이터의 삽입으로 인한 잘못된 정보를 전달할 수 있을 뿐만 아니라, 센서 노드가 싱크(sink)로 정보를 전달하는 경로 내에 있는 센서 노드들의 자원고갈을 야기할 수도 있다. 그러므로 위조된 데이터가 싱크노드에 도착하기 전에 가능한 일찍 이러한 위조된 데이터를 발견해야 한다. 위조된 데이터의 파급을 줄이기 위해 몇 가지 방법이 제안되어 왔다. 상기 방법들은 위조된 데이터를 발견하기 위해 여러 개의 센서 노드들이 투표를 통해 그 데이터가 위조되었는지 아닌지 결정한다. 그렇지만 상기 방법들은 두 가지 단점을 지니고 있다. 첫 번째 단점은 필터링 능력을 높이기 위해 각 센서 노드들은 많은 키를 저장해야 한다는 것이다. 두 번째 단점은 상기 방법들은 이웃 노드들 중 미리 정의된 값인 t 개 이상의 센서 노드들이 공격자에 의해 공격당했을 때 위조된 데이터의 삽입을 발견할 수 없다는 것이다.

<4> 최근 Zhang이 위조된 데이터를 발견하고 위조된 데이터를 무시할 수 있는 위치 기반 임계값 보증(Location-based Threshold Endorsement; LTE) 방법을 제안하였다(Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," vol. 24, no. 2, pp. 247-260, IEEE JSAC, Special Issue on Security in Wireless Ad Hoc Networks, Feb. 2006. 참조). LTE 방법에서 합법적인 데이터를 보고하기 위해서는 t 개 이상의 인증된 센서 노드들에 의해 공동 서명을 받아야 한다. 기존의 방법들과 비교해 볼 때, LTE 방법은 원거리에 있는 싱크노드에 데이터를 전송하기 위해 요구되는 통신 에너지를 효과적으로 줄임과 동시에 필터링 능력을 높였다는 것이 특징이다. LTE 방법이 통신 에너지를 효과적으로 줄일 수 있게 된 가장 큰 이유는 기존의 방법들처럼 대칭키 기반 방법이 아닌 공개키 기반 방법을 적용했기 때문이다. 요구되는 계산 에너지는 증가하지만 반면에 요구되는 통신 에너지를 현저히 줄일 수 있기 때문에 전체적으로 보았을 때 무선 센서 네트워크의 수명을 연장시킬 수 있다는 점이 큰 장점이다. 하지만 LTE 방법은 치명적인 약점을 지니고 있다. LTE 방법은 필터링 능력을 높이기 위해 셀 서명을 할 때, 각 노드에 공동으로 할당된 키를 사용한다. 어떠한 셀이라도 이벤트가 발생하였을 경우 이벤트를 발견한 노드들 사이에서 선출된 데이터 집합 노드(data aggregation point; AP)는 데이터를 보고하기 위해 서명값을 생성한다. 그렇지만 LTE 방법을 한번 실행한 후에는 일반적으로 AP는 셀 키와 셀 서명 키를 생성하는 데 필수적인 비밀 정보들의 일부분을 획득할 수 있게 된다. 따라서 LTE 방법에서 의도하지 않았지만 하나의 셀에 대한 정보의 일부분이 공격자에게 노출되고 이로 인해 또 다른 셀의 안전성 또한 위협받게 된다.

발명의 내용

해결 하고자 하는 과제

- <5> 따라서, 본 발명이 해결하고자 하는 첫 번째 기술적 과제는, 필터링 능력의 손실없이 센서필드의 셀들의 독립적인 안정성을 보장하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법을 제공하는 것이다.
- <6> 본 발명이 해결하고자 하는 두 번째 기술적 과제는, 필터링 능력의 손실없이 센서필드의 셀들의 독립적인 안정성을 보장하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 장치를 제공하는 것이다.
- <7> 본 발명이 해결하고자 하는 세 번째 기술적 과제는, 본 발명에 따른 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법을 수행할 수 있는 프로그램을 기록한 컴퓨터 판독가능 기록매체를 제공하는 것이다.

과제 해결수단

- <8> 상기와 같은 첫 번째 기술적 과제를 해결하기 위하여, 센서 네트워크에서의 위조 데이터 삽입공격을 방지하는 방법으로서, 센서필드를 구획하는 셀(cell)들에 각각 대응하는 셀 다항식 및 셀 인증자 벡터와 관련하여 상기 셀 다항식 및 상기 셀 인증자 벡터에 대응하는 셀의 셀 키를 생성하고 상기 셀 내의 센서 노드에 상기 셀 키를 분배하는 셀 키 분배 단계; 상기 셀에서 상기 셀 키를 분배받은 센서 노드가 이벤트를 발견하면 상기 이벤트를 발견한 상기 센서 노드 중에서 데이터 집합 노드(data aggregation node)를 선출하는 데이터 집합 노드 선출 단계; 상기 이벤트를 발견한 상기 센서 노드가 임의로 선택한 비밀정보를 통해 센서 노드 서명값을 생성하는 센서 노드 서명값 생성 단계; 상기 센서 노드 서명값을 통해 상기 데이터 집합 노드에서 최종 서명값을 생성하고 보고서를 구성하는 단계; 및 상기 보고서를 검증하여 상기 보고서가 정당하면 상기 보고서를 싱크 노드로 전송하는 검증 및 전송 단계를 포함하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법을 제공한다.
- <9> 본 발명의 일 실시예에 따르면, 상기 검증 및 전송 단계는 상기 보고서를 검증하여 상기 보고서가 정당하지 않으면, 부당한 데이터를 전송한 센서 노드를 검색하여, 상기 검색된 센서 노드의 정보를 무시하는 검색 및 무시

단계를 더 포함할 수 있다.

- <10> 본 발명의 일 실시예에 따르면, 상기 검색 및 무시 단계는 상기 센서 노드 서명값을 검사함으로써 달성될 수 있다.
- <11> 본 발명의 일 실시예에 따르면, 상기 방법은 상기 데이터 집합 노드와 상기 싱크 노드 사이에 중간 노드가 있는 경우, 상기 중간 노드에서 상기 보고서를 검증하여 상기 보고서가 정당하지 않으면 상기 보고서를 무시하는 단계를 더 포함할 수 있다.
- <12> 상기와 같은 두 번째 기술적 과제를 해결하기 위하여, 센서 네트워크에서의 위조 데이터 삽입공격을 방지하는 장치로서, 상기 센서 네트워크에서의 위조 데이터 삽입공격 방지 장치는, 센서필드의 동일 셀 내에 위치하는 센서 노드들을 포함하고, 각각의 셀에 대응하는 셀 다항식 및 셀 인증자 벡터와 관련하여 셀 키를 생성 및 분배하는 센서부; 상기 센서부 및 싱크 노드 사이에서 정보를 전달하는 중계부; 및 상기 센서부 및 상기 중계부의 동작을 제어하는 제어부를 포함하고, 상기 센서부의 상기 센서 노드는, 이벤트를 발견하는 경우 상기 이벤트를 발견한 센서 노드 중에서 데이터 집합 노드를 선출하고, 상기 이벤트를 발견한 상기 센서 노드가 위치한 셀에 대응하는 셀 다항식 및 셀 인증자 벡터와 관련하여 임의로 비밀정보를 선택하고, 그리고 상기 비밀정보를 통해 센서 노드 서명값을 생성하고, 그리고 상기 선출된 데이터 집합 노드는, 상기 센서 노드 서명값을 통해 최종 서명값을 생성하고, 상기 최종 서명값을 통해 보고서를 구성하고, 그리고 상기 보고서를 검증하여 정당하면 상기 보고서를 상기 싱크노드로 전송하는 센서 네트워크에서의 위조 데이터 삽입공격 방지 장치를 제공한다.
- <13> 본 발명의 일 실시예에 따르면, 상기 선출된 데이터 집합 노드는 상기 보고서를 검증하여 상기 보고서가 정당하지 않으면, 부당한 데이터를 전송한 센서 노드를 검색하여, 상기 검색된 센서 노드의 정보를 무시할 수 있다.
- <14> 본 발명의 일 실시예에 따르면, 상기 선출된 데이터 집합 노드는 상기 센서 노드 서명값을 검사하여 상기 부당 데이터 전송 센서 노드를 검색할 수 있다.
- <15> 본 발명의 일 실시예에 따르면, 상기 중계부는 상기 데이터 집합 노드와 상기 싱크 노드 사이에 위치하는 중간 노드를 포함하고, 상기 중간 노드는 상기 보고서를 검증하여 상기 보고서가 정당하지 않으면 상기 보고서를 무시할 수 있다.
- <16> 상기와 같은 세 번째 기술적 과제를 해결하기 위하여, 센서 네트워크를 제어하는 컴퓨터가 판독할 수 있는 컴퓨터 판독가능 기록매체로서, 본 발명에 따른 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법을 상기 컴퓨터에서 실행시키기 위한 프로그램 코드를 기록한 컴퓨터로 판독가능 기록 매체가 제공된다.

효 과

- <17> 본 발명에 따른 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법, 장치 및 이에 사용되는 컴퓨터 판독가능 기록매체는 센서 네트워크의 데이터 필터링 능력을 향상시키고 센서필드의 각 셀에 독립적인 안정성을 보장하는 이점을 제공한다.

발명의 실시를 위한 구체적인 내용

- <18> 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명과 관련된 이론을 설명한다.
- <19> **바이리니어 그룹(Bilinear group) 및 페어링(Pairing)**
- <20> 두 개의 큰 소수 p, q 를 정의하고, G_1, G_2 는 q 를 프라임오더(prime order)로 하는 그룹이다. G_1 은 타원 곡선(elliptic curve) E/F_p 위에 있는 점들의 집합을 의미한다. G_2 는 적절한 a 에 대해 유한 필드 $F_{p^a}^*$ 의 곱셈 그룹의 서브 그룹을 의미한다. 페어링(Pairing)은 다음과 같은 특성을 가진 페어링 함수 $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 에 기반한다.
- <21> (1) Bilinearity : 모든 P 와 Q 에 대해 $P, Q \in G_1$ 과 $a, b \in \mathbb{Z}_q^*$ 을 만족할 때, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ 을 만족한다.
- <22> (2) Non-degenerancy : p 가 G_1 의 생성자일 때, $\hat{e}(P, P)$ 는 G_2 의 생성자이다.

<23> (3) Computability : 모든 P 와 Q 에 대해 $P, Q \in G_1$ 을 만족할 때, $\hat{e}(P, Q) \in G_2$ 을 계산하는데 효과적인 알고리즘이 존재한다.

<24> **ID 기반 공개키 암호**

<25> 전통적인 공개키 기반 암호(PKI)는 너무 복잡하고 느리며 많은 에너지 소모가 요구된다. 이러한 특성들은 무선 센서 네트워크에 적절하지 않기 때문에 대부분의 센서 키 연구는 대칭키 기반 암호에 관한 것이다. 대칭키 기반 방식은 적은 계산 오버헤드를 가지고 있는 반면에 대체적으로 많은 통신 오버헤드가 존재하거나 각 노드에게 상당한 메모리를 요구한다. 이러한 이유로 많은 연구자들은 최근에 센서 네트워크에서 실행 가능한 PKI를 연구하기 시작했다.

<26> 인증서 기반 시스템에서 사용자들은 인증기관으로부터 장기간 사용할 수 있는 인증서를 획득하여야 한다. 그리고 이 인증서는 그 사용자를 인증하기 위해 다른 사용자들에게 주어진다. 반면 ID 기반 시스템에서 사용자들은 이메일 같은 것을 통해 사용자의 공개 아이디를 알 수 있다. 그러므로 인증서 기반 시스템과는 달리 ID 기반 시스템에서는 인증서 전송이 필요하지가 않다. 무선 센서 네트워크에서 이러한 차이점은 네트워크의 수명에 있어서 커다란 영향을 준다. 왜냐하면 1 비트를 전송하는데 필요한 전송 에너지는 32 비트를 계산하는 데 필요한 에너지보다 훨씬 많은 에너지를 요구하기 때문이다. 에너지 소비에 관한 실험 결과, 계산에 요구되는 에너지는 전체 에너지 소비의 3%미만인 반면에 통신에 요구되는 에너지는 대략 97%정도이다.

<27> **위치 기반 키 관리 스킴**

<28> 위치 기반 키(LBK) 관리 스킴을 간단히 정리한다. 노드 배치에 앞서 다음과 같은 기능을 하는 믿을 수 있는 개체(trusted authority; TA)가 존재한다고 가정한다.

<29> (1) TA는 바이리니어 그룹 및 페어링에서 명시한 두 개의 그룹 G_1, G_2 그리고 페어링 함수를 설계한다.

<30> (2) TA는 두 개의 암호 해쉬 함수 H 와 h 를 선택한다. 단, 상기 해쉬 함수는 G_1 내의 0이 아닌 임의의 입력 값에 대해 일정한 길이의 출력 값과 맵핑시킨다.

<31> (3) TA는 네트워크 마스터 비밀 값으로 $k \in Z_q^*$ 을 만족하는 k 를 임의로 선택한다. W 가 G_1 의 무작위 생성원일 때, 상기 TA의 공개키 $W_{pub}=kW$ 을 만족한다.

<32> (4) 식별 정보 ID_A 를 가지고 있는 노드 A에 대해, TA는 ID 기반 키인 $IK_A=kH(ID_A)$ 을 계산한다.

<33> 각 센서 노드는 공개키 시스템의 매개 변수들($p, q, G_1, G_2, \hat{e}, H, h, W, W_{pub}$)과 ID 기반 키인 IK_A 를 배치 전에 미리 저장한다. 일단 센서 노드가 배치되면 각 센서 노드에 자기의 센서 노드의 위치 정보가 제공된다. Zhang은 상기 논문에서 이동 가능한 로봇과 주요지점을 사용하여 위치 정보를 제공하는 두 개의 센서 위치 기반 기술을 고려하였다. 위치 측정 후에 센서 노드 A는 센서 노드 B의 위치정보 I_A 와 $LK_A=kH(ID_A || I_A)$ 을 저장하게 된다. 마지막으로 상기 두 개의 센서 노드 A와 B는 하기 수학식 1과 같이 그들의 위치 정보와 ID 정보를 교환한 후에 공통키를 생성한다.

수학식 1

$$\begin{aligned} K_{A,B} &= \hat{e}(LK_A, H(ID_B || I_B)) \\ &= \hat{e}(H(ID_A || I_A), kH(ID_B || I_B)) \\ &= \hat{e}(LK_B, H(ID_A || I_A)) = K_{B,A} \end{aligned}$$

<34> <35> 상기 수학식 1에서 " $||$ "는 "접합(concatenation)"을 의미한다.

<36> 이하, 본 발명의 기술적 과제의 해결 방안을 명확화하기 위해 첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 상세하게 설명하되 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다.

<37> 본 발명을 설명함에 있어서 관련된 공지기술 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불명료하게

할 수 있다고 판단되는 경우에는 그 상세한 설명은 생략할 것이다. 또한, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자 등의 의도 또는 관례 등에 따라 달라질 수 있을 것이다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

<38> 도 1에는 셀 단위로 구현된 센서필드가 도시되어 있다.

<39> r을 각 변의 길이로 하는 정사각형 모양의 M x N으로 센서필드(100)를 나눈 후, $1 \leq m \leq M$, $1 \leq n \leq N$ 을 만족하는 m, n에 대해 각 셀을 정수 쌍 <m,n>으로 이름 짓는다. $ID_{m,n}^i$ 은 셀 안에 있는 위치정보 $l_{m,n}^i$ 를 가진 i번째 노드를 나타낸다.

<40> 도 2에는 본 발명에 따른 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법에 관한 일례가 흐름도로 도시되어 있다.

<41> 도 3에는 본 발명에 따른 센서 네트워크에서의 위조 데이터 삽입공격 방지 장치에 관한 일례가 블록도로 도시되어 있다.

<42> 도 2 및 도 3을 참조하면, 센서필드(100)를 이루는 셀(cell)들 각각에 대응하는 셀 다항식 및 셀 인증자 벡터와 관련하여 상기 셀 다항식 및 상기 셀 인증자 벡터에 대응하는 셀의 셀 키를 생성하고 상기 셀 내의 센서 노드(302)에 상기 셀 키를 분배한다(S200). 기존의 방법과는 달리 하나의 다항식과 인증자 벡터가 아닌 각 셀 <m,

$$F_{m,n}(x) = \sum_{j=1}^t H(F_j \| m \| n) x^j \quad \text{과} \quad \text{셀 인증자 벡터} \quad V_{m,n} = \{v_{m,n}^{(j)} | 0 \leq j \leq t-1\}$$

n>에 대한 셀-다항식 을 정의한다. 상기 셀 다항식에서, F_j 는 G_1 에서 무작위로 선택한 계수이다. 상기 인증자 벡터 식에서, $v_{m,n}^{(j)} = \hat{e}(H(F_j \| m \| n), W)$ 이고, $v_{m,n}^{(0)} = \hat{e}(K_{m,n}, W)$ 이다. 셀 키를 공유하기 위해 다음 두 가지 방식이 사용될 수 있다.

<43> 범위 기반 셀 키 분배 방식

<44> 상기 방식은 이동 가능한 로봇이 공통 정보인 $K_{m,n}$ 을 분배하는 데 중요한 역할을 한다. 상기 방식은 상기 로봇이 (t-1)차 다항식 $F(x)$ 을 가지고 있다고 가정한다. 우선, 이동 가능 로봇은 셀 <m,n>에서 셀 다항식 $F_{m,n}(x)$, 셀 키 $K_{m,n} = kH(m \| n)$ 과 셀 인증자 벡터를 계산한다. 다음으로, 상기 이동 가능 로봇은 $K_{m,n}$ 과 센서 노드 식별정보인 $ID_{m,n}^i$ 을 사용하여 상기 센서 노드(302)의 공유 정보인 $K_{m,n}^i = F_{m,n}(ID_{m,n}^i \| l_{m,n}^i) + K_{m,n} \in G_1$ 을 계산한다. 마지막으로, 상기 이동 가능 로봇은 센서 노드 $ID_{m,n}^i$ (302)와의 공통키인 IK_a 을 사용하여 상기 $K_{m,n}^i$ 과 상기 셀 인증자 벡터를 상기 센서 노드 $ID_{m,n}^i$ (302)에게 안전하게 전송한다.

<45> $K_{m,n}$ 은 미리 정해진 값 t개 이상의 공유 정보로부터 다시 만들어질 수 있다. 반면, (t-1)개 이하의 공유 정보로부터는 만들어질 수 없다. 본 발명에서는 하기 수학식 2와 같은 방법으로 t차 선형 방정식에 의해 셀 키를 생성한다.

수학식 2

$$K_{m,n} = \sum_{i \in \Omega} \lambda_i K_{m,n}^i$$

<46> 상기 수학식 2에서, Ω 는 셀 안의 모든 센서 노드들의 t 오더 서브셋(t-order subset)이라고 정의하며,

$$\lambda_i = \prod_{j \in \Omega \setminus \{i\}} \frac{(ID_{m,n}^j \| l_{m,n}^j)}{(ID_{m,n}^j \| l_{m,n}^j - ID_{m,n}^i \| l_{m,n}^i)} \quad \text{이다.}$$

<48> 공격자의 노드 획득으로 인한 공유 정보 유출에 대한 방지와 노드 밀도는 트레이드오프 관계(trade off relation)이기 때문에 어느 성질이 더 중요한가에 따라 매개 변수 값 t를 결정해야 한다.

<49> 범위 제한 없는 셀 키 분배 방식

<50> 각 센서 노드(302)는 배치 전에 다항식 $F(x)$ 와 마스터 키 k 를 저장한다. 일단 각 노드의 LBK(Location Based Key)를 계산한 후에 노드 $ID_{m,n}^i$ 는 k 를 사용하여 $K_{m,n}$, 셀 다항식과 공유 정보인 $K_{m,n}^i$ 를 생성한다. 또한 셀 인증자 벡터를 계산한다. 상기 모든 과정을 마친 후에 상기 센서 노드(302)의 메모리에 저장되어 있는 상기 k , 상기 다항식 $F(x)$, 상기 셀 다항식 및 상기 셀 키 $K_{m,n}$ 를 안전하게 지워야 한다.

<51> 다음으로, 센서부(300)의 센서필드(100)의 셀에서 상기 셀 키를 분배받은 센서 노드가 이벤트를 발견하면 상기 이벤트를 발견한 상기 센서 노드 중에서 데이터 집합 노드(data aggregation node; 304)를 선출한다. 상기 이벤트를 발견한 상기 센서 노드들 $ID_{m,n}^i$ (302)은 보고서(Λ)에 대한 서명값을 생성하기 위해 임의로 비밀정보(또는 비밀난수) $a_i \in Z_q^*$ 선택하고, 상기 센서 노드 $D_{m,n}^i$ (302)의 센서 노드 서명값을 생성하기 위한 중간값

$\theta_i = \hat{e}(W, W)^\alpha$ 계산한 후, 상기 중간값을 AP(304)에게 송신한다. 미리정한 값 t 개 이상의 데이터를 받은 후에 상기 AP(304)는 상기 데이터 사이에서 임의로 t 개를 선택한다. 상기 데이터를 보낸 상기 센서 노드(304)는

$$\theta = \prod_{i \in \Omega} \theta_i^{\lambda_i}$$

Ω 에 포함되어 있는 센서 노드이다. 다음으로 상기 AP(304)는 θ 를 계산하고 상기 θ 를 다른 센서 노드들에게 브로드캐스트 한다. 상기 θ 를 수신하는 즉시 각 센서 노드(302)는 보고서에 대한 센서 노드 서명값 $\gamma_{m,n}^i = h(\Lambda \parallel \theta) K_{m,n}^i + \alpha_i W$ 을 계산함으로써 보고서(Λ)에 대한 자신의 서명값을 생성한다(S202). 그리고 각 센서 노드(302)는 상기 AP(304)와 공유한 페어와이즈(pairwise) 키를 사용하여 상기 AP(304)에게 상기 센서 노드 서명값을 송신한다. 다음으로 상기 AP(304)는 보고서(Λ)에 대한 최종 서명값

$$\gamma_{m,n} = \sum_{i \in \Omega} \lambda_i \gamma_{m,n}^i$$

을 계산한다(S204). 상기 보고서(Λ)의 최종 서명값은 $(\gamma_{m,n}, h(\Lambda \parallel \theta))$ 이다. 따라서 상기 AP(304)에 의해 싱크(330)로 보내지는 최종 보고서 구성은 $\langle \Lambda, \gamma_{m,n}, h(\Lambda \parallel \theta) \rangle$ 가 된다.

<52> 일부 센서 노드가 손실되었다고 하더라도 상기 AP(304)는 $\gamma_{m,n}$ 을 유도한 후, $\hat{e}(\gamma_{m,n}, W) = (v_{m,n}^{(0)})^{h(\Lambda \parallel \theta)} \cdot \theta$ 을 검사함으로써 보고서의 신빙성을 검증할 수 있다(S206). 그 세 부 과정은 하기 수학식 3과 같다.

수학식 3

$$\begin{aligned} \hat{e}(\gamma_{m,n}, W) &= \hat{e}\left(\sum_{i \in \Omega} \lambda_i \gamma_{m,n}^i, W\right) \\ &= \hat{e}\left(\sum_{i \in \Omega} (\lambda_i K_{m,n}^i (\Lambda \parallel \theta) + \lambda_i \alpha_i W), W\right) \\ &= \hat{e}(h(\Lambda \parallel \theta) K_{m,n} + \sum_{i \in \Omega} \lambda_i \alpha_i W, W) \\ &= \hat{e}(K_{m,n}, W)^{h(\Lambda \parallel \theta)} \cdot \prod_{i \in \Omega} \hat{e}(W, W)^{\alpha_i \lambda_i} \\ &= (v_{m,n}^{(0)})^{h(\Lambda \parallel \theta)} \cdot \prod_{i \in \Omega} \theta_i^{\lambda_i} \\ &= (v_{m,n}^{(0)})^{h(\Lambda \parallel \theta)} \cdot \theta \end{aligned}$$

<53> 상기 검증을 통과하면 상기 AP(304)는 그 최종 보고서가 정당하다고 믿는다. 그리고 중계부(310) 내에 중간 노드(312)가 없다면, 상기 최종 보고서를 바로 싱크(330)로 보낸다(S210). 만일 상기 검증을 통과하지 못한다면 상기 AP(304)는 악의적인 센서 노드를 찾기 위해 하기 수학식 4와 같은 과정을 통해 각각의 센서 노드로부터 수신한 상기 센서 노드 서명값 $\gamma_{m,n}^i$ 을 검증한다(S202).

수학식 4

$$\begin{aligned} \hat{e}(\gamma_{m,n}^i, W) \\ = \prod_{j=0}^{t-1} (v_{m,n}^{(j)})^{(ID_{m,n}^i \| l_{m,n}^i)^j h(A\|\theta)} \cdot \theta_i \end{aligned}$$

<55>

<56> 상기 수학식 4의 세부과정은 하기 수학식 5와 같다.

수학식 5

$$\begin{aligned} \hat{e}(\gamma_{m,n}^i, W) \\ = \hat{e}(h(\lambda\|\theta)K_{m,n}^i + \alpha_i W, W) \\ = \hat{e}(K_{m,n}^i, W)^{h(A\|\theta)} \cdot \hat{e}(W, W)^{\alpha_i} \\ = \hat{e}(\sum_{j=1}^{t-1} H(F_j\|m\|n)(ID_{m,n}^i \| l_{m,n}^i)^j \\ + K_{m,n}, W)^{h(A\|\theta)} \cdot \theta_i \\ = \prod_{j=0}^{t-1} (v_{m,n}^{(j)})^{(ID_{m,n}^i \| l_{m,n}^i)^j h(A\|\theta)} \cdot \theta_i \end{aligned}$$

<57>

<58> 악의적인 센서 노드를 검색한 후, 상기 AP(304)는 상기 악의적인 센서 노드로부터 들어오는 정보를 무시할 수 있다(S214).

<59> 상기 AP(304) 및 상기 싱크 노드(330) 사이에 중간 노드(312)가 존재하면(S208), 상기 중간 노드(312)는 상기 최종 보고서를 수신할 때, 샘플링 확률이라 불리는 몇 개의 시스템 와이드(system-wide) 파라미터 p_s 에 의해 상기 최종 보고서를 검증한다(S216). 상기 중간 노드는 먼저 $H(A\|\theta')$ 를 계산한 후, 상기 최종 보고서를 검증한다. 상기 θ' 는 하기 수학식 6과 같다.

수학식 6

$$\theta' = \hat{e}(\gamma_{m,n}, W) \cdot \hat{e}(H(m\|n), -W_{pub})^{h(\lambda\|\theta)}$$

<60>

<61> 최종 보고서가 타당하면(S218), 하기 수학식 7을 만족시킨다.

수학식 7

$$\begin{aligned} \theta' &= \hat{e}(\gamma_{m,n}, W) \cdot \hat{e}(H(m\|n), W_{pub})^{-h(A\|\theta)} \\ &= \hat{e}(K_{m,n}, W)^{h(A\|\theta)} \cdot \prod_{i \in \Omega} \theta_i^{\lambda_i} \\ &\quad \cdot \hat{e}(K_{m,n}, W)^{-h(A\|\theta)} \\ &= \theta \end{aligned}$$

<62>

<63> 만일, $h(A\|\theta) = h(A\|\theta')$ 을 만족한다면 상기 중간 노드(312)는 그 최종 보고서를 다음 홉으로 보낸다(S218). 그렇지 않으면 그 최종 보고서는 위조된 것으로 판단하여 상기 중간 노드(312)에서 무시된다(S220). 다음 홉의 중간 노드에서 상기 단계(S216, S218, S220)를 반복할 수 있다.

<64> 도 4에는 홉 수에 따라 위조된 보고서를 발견할 확률이 그래프로 도시되어 있다. LTE의 취약점 때문에 LTE는 애초 의도한 필터링 능력을 보장하지 못한다. 본 발명에 따른 방법은 중간 노드가 확률 p_s 을 가지고 수신한 보고서

를 검증한다. 1 홉 이내에 위조된 보고서를 발견하고 상기 위조된 보고서를 무시할 기대 확률은 $1-(1-p_s)^1$ 과 같다. 예를 들어 $p_s=0.4$ 일 때, 5 홉 이내에 위조된 보고서를 발견할 확률은 92%이고, 10 홉 이내에 발견할 확률은 99%가 된다. p_s 값의 결정은 필요에 따라 계산 오버헤드와 필터링 능력 사이에서 적당한 값을 찾아야 한다. 그 두 성질은 트레이드오프 관계이기 때문이다. 많은 수의 위조된 데이터가 발견되었을 때, 추가적인 메모리 없이 값을 증가시킬 수 있다. 그렇지만 다른 기존의 보안 스킴들은 그 확률을 증가시키기 위해 각 노드에 배치 전에 미리 저장되는 키의 수를 증가시켜야 하므로 그에 따른 계산 오버헤드도 증가하게 된다. 기존의 스킴과 우리가 제안한 스킴의 이러한 차이점은 매우 중요하다. 그 이유는 제안된 스킴은 배치 전에 미리 저장되는 키의 수 증가 없이 라우팅 경로 상에서 충분한 필터링 능력을 발휘할 수 있기 때문이다.

<65> 본 발명에 따른 센서 네트워크에서의 위조 데이터 삽입공격 방지 장치는, 상기 센서 노드(302) 및 AP(304)등 센서필드의 동일 셀 내에 위치하는 센서 노드들을 포함하고, 각각의 셀에 대응하는 셀 다항식 및 셀 인증자 벡터와 관련하여 셀 키를 생성 및 분배하는 센서부(300), 상기 중간 노드(312)를 포함할 수 있는 중계부(310), 및 상기 센서부(300)와 상기 중계부(310)를 제어하는 제어부(320)를 포함할 수 있으며, 본 발명에 따른 상기 장치에 포함되는 상기 센서 노드(302), 상기 AP(304), 및 상기 중간 노드(304)는 상기 제어부(320)를 통해 위에서 설명한 바와 같이 동작한다.

<66> 본 발명에 따른 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법은 또한, 상기 센서 네트워크를 제어하는 컴퓨터가 판독할 수 있는 컴퓨터 판독가능 기록매체에 상기 컴퓨터가 읽을 수 있는 프로그램 코드로서 구현하는 것이 가능하다. 상기 컴퓨터 판독가능 기록매체는 상기 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다.

<67> 컴퓨터가 판독가능 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<68> 상술한 바와 같이, 본 발명에 따른 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법, 장치 및 이에 사용되는 컴퓨터 판독가능 기록매체는, 이벤트를 발견한 각 센서 노드가 임의로 비밀정보 α_i 를 선택하기 때문에 AP가 각 센서 노드의 α_i 를 알아낼 수 없다. AP가 $\gamma_{m,n}^i = h(A||\theta)K_{m,n}^i + \alpha_i W$ 와 $\gamma_{m,n} = h(A||\theta)K_{m,n} + \sum_{i \in \Omega} \lambda_i \alpha_i W$ 을 알아냈다고 하더라도, α_i 없이 $K_{m,n}^i$ 와 $K_{m,n}$ 을 결코 획득할 수 없다. 따라서 악의적인 AP로부터 영향을 받지않는 이점이 있다.

<69> 또한, 본 발명에 따르면, 모든 셀에 대해 별개의 셀-다항식을 사용한다. 예를 들어 공격자가 셀 $\langle m,n \rangle$ 에 대한 t 개의 공유 정보를 획득했다고 가정했을 때, 공격자가 t -가변 선형 방정식을 계산함으로써 $(t-1)$ 차 다항식 $F_{m,n}(x)$ 의 모든 계수 $\{H(F_j || m || n)\}$ 을 유도해낼 수 있다고 하더라도, 공격자는 다른 셀 $\langle m',n' \rangle$ 에 대한 어떠한 정보도 획득할 수 없다. H 가 단방향 성질을 지닌 암호학적 해쉬 함수이기 때문에 $H(F_j || m || n)$ 으로부터 $H(F_j || m' || n')$ 을 이끌어내는 것은 상당히 어렵다. 결과적으로 셀의 셀-다항식이 공격자에게 노출되었다 하더라도 다른 셀의 안전성에는 영향을 주지 못한다. 즉, 각 셀에 독립적인 안전성을 주는 이점이 있다.

<70> 이제까지 본 발명에 대하여 그 바람직한 실시예를 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다.

<71> 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 균등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면의 간단한 설명

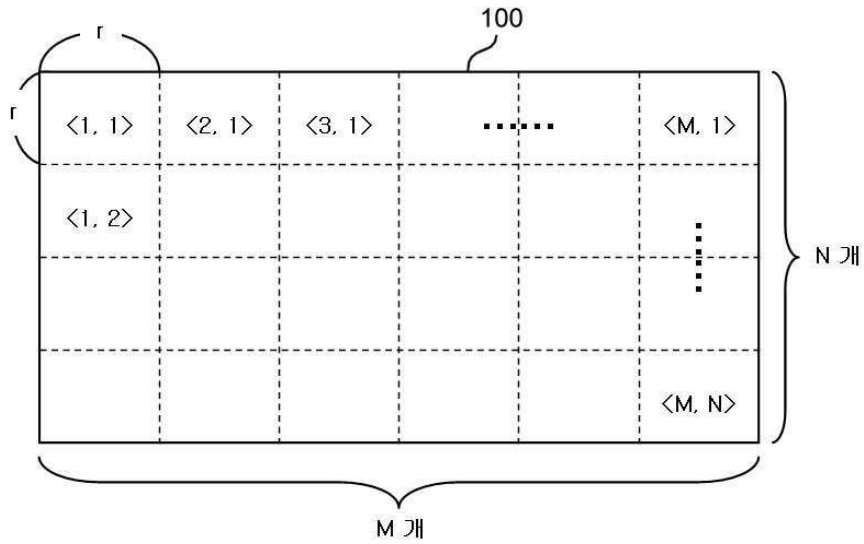
<72> 도 1은 셀로 구성된 센서필드의 일례를 나타낸 도면이다.

<73> 도 2는 본 발명에 따른 센서 네트워크에서의 위조 데이터 삽입공격 방지 방법의 일례에 관한 흐름도이다.

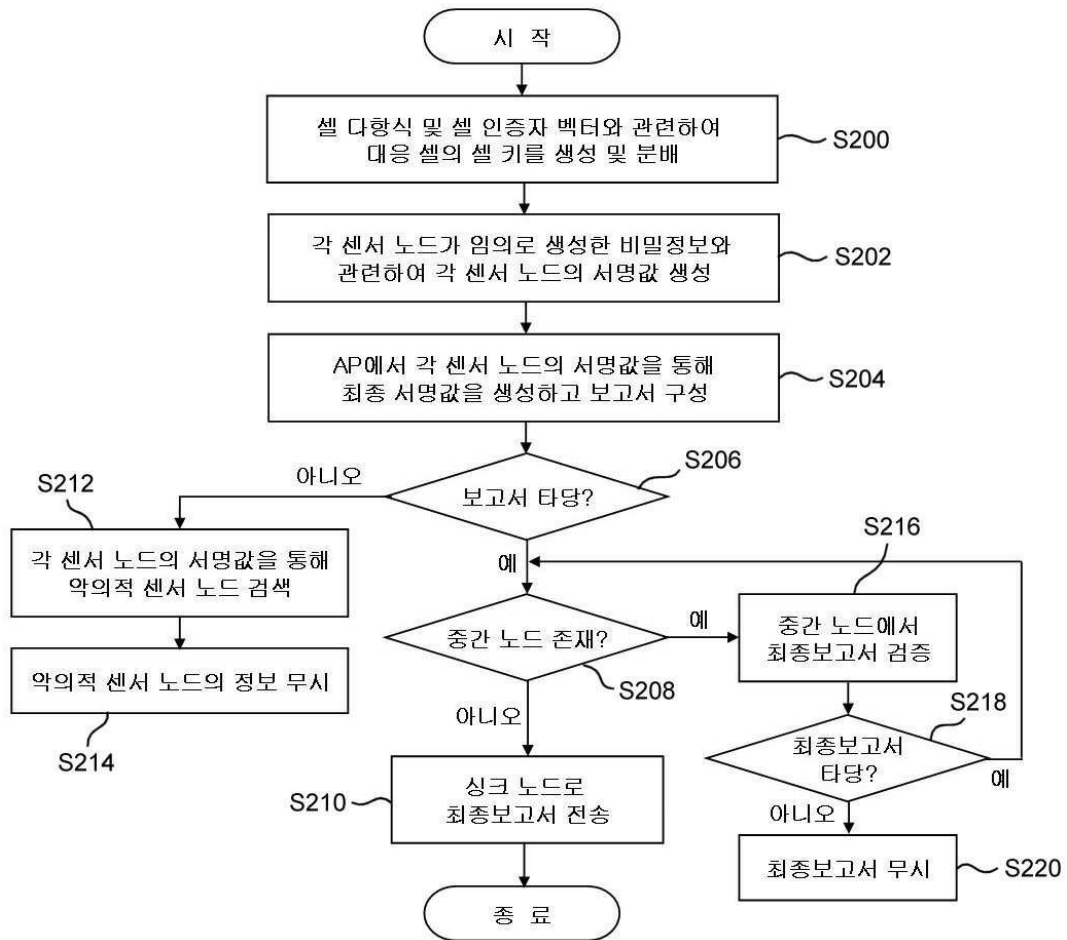
- <74> 도 3은 본 발명에 따른 센서 네트워크에서의 위조 데이터 삽입공격 방지 장치의 일례에 관한 블록도이다.
- <75> 도 4는 홉 수에 따라 위조된 보고서를 발견할 확률을 나타낸 그래프이다.

도면

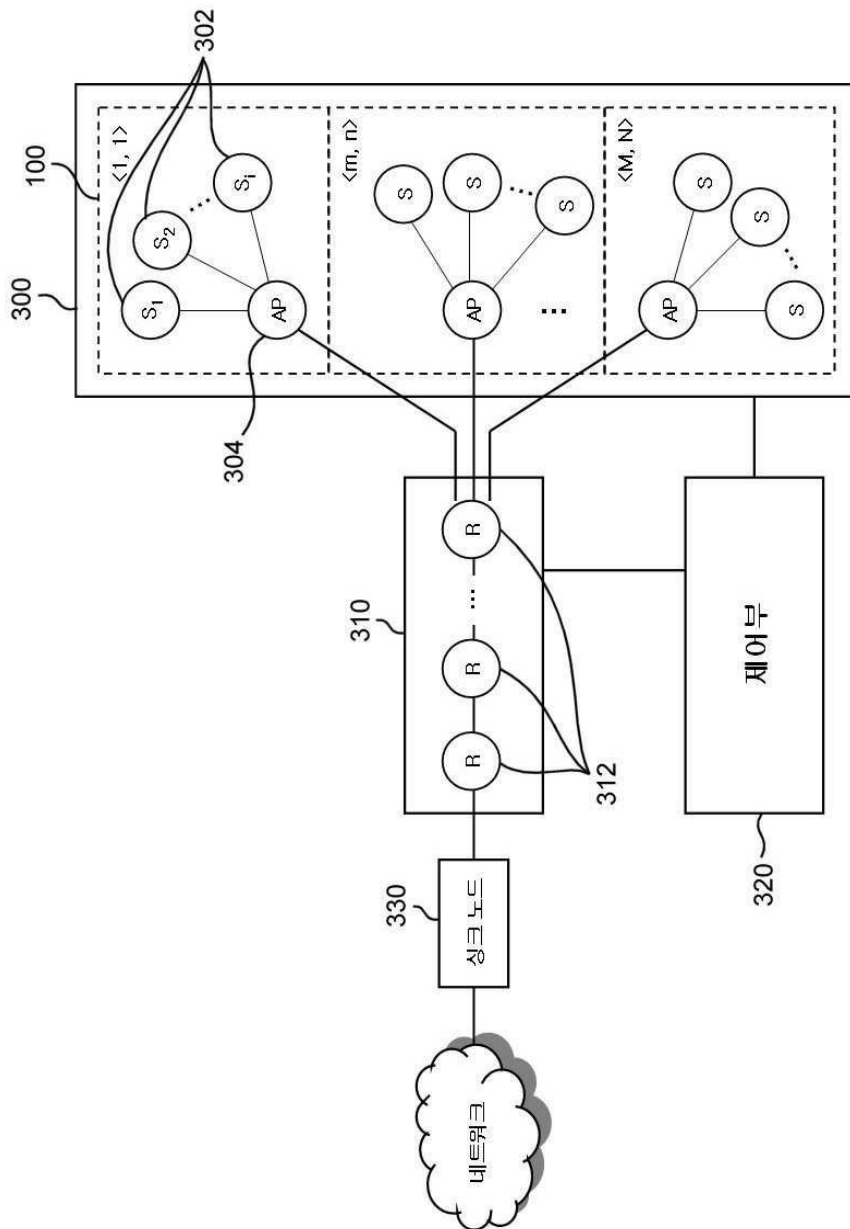
도면1



도면2



도면3



도면4

