(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0098933
(43) 공개일자 2009년09월18일

(51) Int. Cl.
H04L 12/26 (2006.01) *H04L 12/22* (2006.01)
(21) 출원번호 10-2008-0024115
(22) 출원일자 2008년03월15일
심사청구일자 2008년03월15일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가1 고려대학교 내
(72) 발명자
이동훈
경기 고양시 일산동구 정발산동 밤가시마을 901동 201호
조관태
서울 성북구 안암동5가 고려대학교 정보보호대학원 140호
(뒷면에 계속)
(74) 대리인
현종철

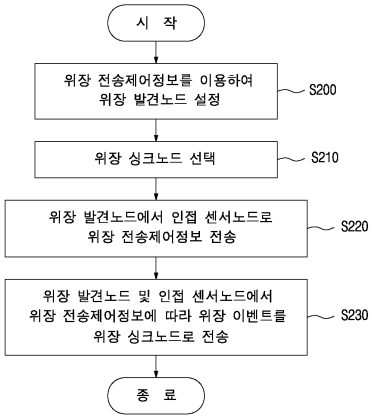
전체 청구항 수 : 총 20 항

(54) 무선센서네트워크에서의 위치 프라이버시 보호 방법과 이를이용한 무선센서네트워크 시스템 및 기록매체

(57) 요 약

본 발명은 무선센서네트워크에서의 위치 프라이버시 보호 기술에 관한 것으로서, 본 발명에 따른 무선센서네트워크에서의 위치 프라이버시 보호 방법은 이벤트를 감지한 센서노드인 발견노드(discoverer node)가 상기 이벤트를 싱크노드(sink node)로 전송하는데 필요한 전송제어정보에 대응하는 위장 전송제어정보를 후보 센서노드(candidate sensor node)에 저장하여 상기 후보 센서노드를 위장 발견노드(faked discoverer node)로 설정하는 위장 발견노드 설정 단계; 및 상기 위장 발견노드에서 위장 이벤트를 전송하기 위해 위장 싱크노드(faked sink node)를 선택하여 상기 위장 전송제어정보에 따라 상기 위장 이벤트를 상기 위장 싱크노드로 전송하는 위장 이벤트 전송 단계를 포함하여, 발견노드 및 싱크노드의 위치 프라이버시 안정성을 동시에 제공하면서도 기존 기술에 비해 데이터 전송률을 현저히 향상시킨다는 이점을 제공한다.

대 표 도 - 도2



(72) 발명자

이화성

서울 동작구 사당1동 1050-11번지 302호

김용호

서울 중랑구 신내2동 신내8단지 화성아파트 802동 1001호

특허청구의 범위

청구항 1

무선센서네트워크에서 위치 프라이버시를 보호하는 방법에 있어서,

이벤트를 감지한 센서노드인 발견노드(discoverer node)가 상기 이벤트를 싱크노드(sink node)로 전송하는데 필요한 전송제어정보에 대응하는 위장 전송제어정보를 후보 센서노드(candidate sensor node)에 저장하여 상기 후보 센서노드를 위장 발견노드(faked discoverer node)로 설정하는 위장 발견노드 설정 단계; 및

상기 위장 발견노드에서 위장 이벤트를 전송하기 위해 위장 싱크노드(faked sink node)를 선택하여 상기 위장 전송제어정보에 따라 상기 위장 이벤트를 상기 위장 싱크노드로 전송하는 위장 이벤트 전송 단계를 포함하는 무선센서네트워크에서의 위치 프라이버시 보호 방법.

청구항 2

제1항에 있어서,

상기 전송제어정보는, 상기 발견노드에서 상기 이벤트를 상기 싱크노드로 전송하는데 필요한 이벤트 전송 시작시간, 이벤트 전송 지속시간 및 상기 발견노드의 전송 주기에 관한 정보를 포함하는 것을 특징으로 하는 무선센서네트워크에서의 위치 프라이버시 보호 방법.

청구항 3

제2항에 있어서,

상기 후보 센서노드에 저장되는 상기 위장 전송제어정보는, 상기 무선센서네트워크에 대한 공격자가 상기 발견노드에 의한 트래픽 변동과 상기 위장 발견노드에 의한 트래픽 변동을 구별할 수 없도록 하는 값을 지니는 정보인 것을 특징으로 하는 무선센서네트워크에서의 위치 프라이버시 보호 방법.

청구항 4

제2항에 있어서,

상기 후보 센서노드에 저장되는 상기 위장 전송제어정보는, 상기 전송제어정보에 포함되는 상기 이벤트 전송 시작시간과 동일한 값 또는 상기 이벤트 전송 시작시간보다 이른 값을 지니는 위장 이벤트 전송 시작시간에 관한 정보를 포함하는 것을 특징으로 하는 무선센서네트워크에서의 위치 프라이버시 보호 방법.

청구항 5

제1항에 있어서,

상기 무선센서네트워크에서의 위치 프라이버시 보호 방법은, 상기 위장 발견노드 설정 단계에 후에 상기 위장 발견노드에서 상기 위장 전송제어정보를 이웃 센서노드로 전송하여 상기 이웃 센서노드로 하여금 상기 위장 전송제어정보에 따라 위장 이벤트를 상기 위장 싱크노드로 전송하도록 하는 단계를 더 포함하는 것을 특징으로 하는 무선센서네트워크에서의 위치 프라이버시 보호 방법.

청구항 6

제1항에 있어서,

상기 무선센서네트워크가 이벤트 감지 기반 무선센서네트워크인 경우 상기 무선센서네트워크에서의 위치 프라이버시 보호 방법은, 상기 위장 발견노드 설정 단계 전에 상기 발견노드에서 상기 위장 전송제어정보를 생성하여 상기 후보 센서노드로 전송하는 위장 전송제어정보 전송 단계를 더 포함하는 것을 특징으로 하는 무선센서네트워크에서의 위치 프라이버시 보호 방법.

청구항 7

제6항에 있어서,

상기 위장 전송제어정보 전송 단계는, 상기 발견노드가 상기 무선센서네트워크의 전송 경로상 상기 싱크노드보

다 멀리 위치한 센서노드 중에서 상기 후보 센서노드를 선택하여 상기 위장 전송제어정보를 상기 후보 센서노드로 전송하는 단계인 것을 특징으로 하는 무선센서네트워크에서의 위치 프라이버시 보호 방법.

청구항 8

제1항에 있어서,

상기 무선센서네트워크가 쿼리 기반 무선센서네트워크인 경우 상기 무선센서네트워크에서의 위치 프라이버시 보호 방법은, 상기 위장 발견노드 설정 단계 전에 상기 싱크노드에서 상기 위장 전송제어정보를 생성하여 상기 후보 센서노드로 전송하는 단계를 더 포함하는 것을 특징으로 하는 무선센서네트워크에서의 위치 프라이버시 보호 방법.

청구항 9

제1항에 있어서,

상기 무선센서네트워크가 주기 기반 무선센서네트워크인 경우 상기 무선센서네트워크에서의 위치 프라이버시 보호 방법은, 상기 위장 발견노드 설정 단계 전에 상기 싱크노드에서 상기 위장 전송제어정보를 생성하여 상기 후보 센서노드로 전송하는 위장 전송제어정보 전송 단계를 더 포함하고, 상기 무선센서네트워크의 전송 주기마다 상기 단계들을 반복하는 것을 특징으로 하는 무선센서네트워크에서의 위치 프라이버시 보호 방법.

청구항 10

제9항에 있어서,

상기 위장 전송제어정보 전송 단계는, 상기 싱크노드에서 상기 무선센서네트워크의 상기 전송 주기마다 새로운 후보 센서노드를 선택하여 상기 위장 전송제어정보를 상기 새로운 후보 센서노드로 전송하는 단계인 것을 특징으로 하는 무선센서네트워크에서의 위치 프라이버시 보호 방법.

청구항 11

제1항 내지 제10항 중 어느 한 항에 따른 무선센서네트워크에서의 위치 프라이버시 보호 방법을 상기 무선센서네트워크를 제어하는 컴퓨터 시스템에서 실행하기 위한 프로그램이 기록된 기록매체로서, 상기 컴퓨터 시스템이 판독할 수 있는 상기 기록매체.

청구항 12

이벤트를 감지한 센서노드인 발견노드(discoverer node) 및 싱크노드(sink node)의 위치 프라이버시를 보호하는 무선센서네트워크 시스템에 있어서,

상기 발견노드가 상기 이벤트를 상기 싱크노드로 전송하는데 필요한 전송제어정보에 대응하는 위장 전송제어정보를 저장하는 위장 발견노드(faked discoverer node); 및

상기 위장 발견노드로부터 위장 이벤트를 수신하는 위장 싱크노드(faked sink node)를 포함하고, 상기 위장 발견노드는 상기 무선센서네트워크 시스템에 포함되는 센서노드 중에서 상기 위장 싱크노드를 선택하여 상기 위장 전송제어정보에 따라 상기 위장 이벤트를 상기 위장 싱크노드로 전송하는 위치 프라이버시를 보호하는 무선센서네트워크 시스템.

청구항 13

제12항에 있어서,

상기 전송제어정보는, 상기 발견노드에서 상기 이벤트를 상기 싱크노드로 전송하는데 필요한 이벤트 전송 시작시간, 이벤트 전송 지속시간 및 상기 발견노드의 전송 주기에 관한 정보를 포함하는 것을 특징으로 하는 위치 프라이버시를 보호하는 무선센서네트워크 시스템.

청구항 14

제13항에 있어서,

상기 위장 발견노드에 저장되는 상기 위장 전송제어정보는, 상기 무선센서네트워크에 대한 공격자가 상기 발견

노드에 의한 트래픽 변동과 상기 위장 발견노드에 의한 트래픽 변동을 구별할 수 없도록 하는 값을 지니는 정보인 것을 특징으로 하는 위치 프라이버시를 보호하는 무선센서네트워크 시스템.

청구항 15

제13항에 있어서,

상기 위장 발견노드에 저장되는 상기 위장 전송제어정보는, 상기 전송제어정보에 포함되는 상기 이벤트 전송 시작시간과 동일한 값 또는 상기 이벤트 전송 시작시간보다 이른 값을 지니는 위장 이벤트 전송 시작시간에 관한 정보를 포함하는 것을 특징으로 하는 위치 프라이버시를 보호하는 무선센서네트워크 시스템.

청구항 16

제12항에 있어서,

상기 위장 발견노드는, 상기 위장 전송제어정보를 이웃 센서노드로 전송하여 상기 이웃 센서노드로 하여금 상기 위장 전송제어정보에 따라 위장 이벤트를 상기 위장 싱크노드로 전송하도록 하는 것을 특징으로 하는 위치 프라이버시를 보호하는 무선센서네트워크 시스템.

청구항 17

이벤트 감지 기반 무선센서네트워크에서 이벤트를 감지한 센서노드인 발견노드(discoverer node) 및 싱크노드(sink node)의 위치 프라이버시를 보호하는 무선센서네트워크 시스템에 있어서,

상기 발견노드가 상기 이벤트를 상기 싱크노드로 전송하는데 필요한 전송제어정보에 대응하는 위장 전송제어정보를 생성하여 전송하는 상기 발견노드;

상기 발견노드로부터 상기 위장 전송제어정보를 수신하여 저장하는 위장 발견노드(faked discoverer node); 및

상기 위장 발견노드로부터 위장 이벤트를 수신하는 위장 싱크노드(faked sink node)를 포함하고, 상기 위장 발견노드는 상기 이벤트 감지 기반 무선센서네트워크에 포함되는 센서노드 중에서 상기 위장 싱크노드를 선택하여 상기 위장 전송제어정보에 따라 상기 위장 이벤트를 상기 위장 싱크노드로 전송하는 위치 프라이버시를 보호하는 무선센서네트워크 시스템.

청구항 18

제17항에 있어서,

상기 발견노드는, 상기 이벤트 감지 기반 무선센서네트워크의 전송 경로상 상기 싱크노드보다 멀리 위치한 센서노드 중에서 상기 위장 발견노드를 선택하여 상기 위장 전송제어정보를 상기 위장 발견노드로 전송하는 것을 특징으로 하는 위치 프라이버시를 보호하는 무선센서네트워크 시스템.

청구항 19

쿼리 기반 무선센서네트워크에서 이벤트를 감지한 센서노드인 발견노드(discoverer node) 및 싱크노드(sink node)의 위치 프라이버시를 보호하는 무선센서네트워크 시스템에 있어서,

상기 발견노드가 상기 이벤트를 상기 싱크노드로 전송하는데 필요한 전송제어정보에 대응하는 위장 전송제어정보를 생성하여 전송하는 상기 싱크노드;

상기 싱크노드로부터 상기 위장 전송제어정보를 수신하여 저장하는 위장 발견노드(faked discoverer node); 및

상기 위장 발견노드로부터 위장 이벤트를 수신하는 위장 싱크노드(faked sink node)를 포함하고, 상기 위장 발견노드는 상기 쿼리 기반 무선센서네트워크에 포함되는 센서노드 중에서 상기 위장 싱크노드를 선택하여 상기 위장 전송제어정보에 따라 상기 위장 이벤트를 상기 위장 싱크노드로 전송하는 위치 프라이버시를 보호하는 무선센서네트워크 시스템.

청구항 20

주기 기반 무선센서네트워크에서 이벤트를 감지한 센서노드인 발견노드(discoverer node) 및 싱크노드(sink node)의 위치 프라이버시를 보호하는 무선센서네트워크 시스템에 있어서,

상기 발견노드가 상기 이벤트를 상기 싱크노드로 전송하는데 필요한 전송제어정보에 대응하는 위장 전송제어정보를 생성하여 전송하는 상기 싱크노드;

상기 싱크노드로부터 상기 위장 전송제어정보를 수신하여 저장하는 위장 발견노드(faked discoverer node); 및

상기 위장 발견노드로부터 위장 이벤트를 수신하는 위장 싱크노드(faked sink node)를 포함하고, 상기 위장 발견노드는 상기 쿼리 기반 무선센서네트워크에 포함되는 센서노드 중에서 상기 위장 싱크노드를 선택하여 상기 위장 전송제어정보에 따라 상기 위장 이벤트를 상기 위장 싱크노드로 전송하고, 그리고 상기 싱크노드는 상기 주기 기반 무선센서네트워크의 전송 주기마다 새로운 위장 발견노드를 선택하여 상기 위장 전송제어정보를 상기 새로운 위장 발견노드로 전송하는 위치 프라이버시를 보호하는 무선센서네트워크 시스템.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 무선센서네트워크에서의 위치 프라이버시 보호 기술에 관한 것이며, 더욱 상세하게는 발견노드 및 싱크노드의 위치 프라이버시를 동시에 보호하고 데이터 전송률을 개선하는 무선센서네트워크에서의 위치 프라이버시 보호 방법과 이를 이용한 무선센서네트워크 시스템 및 기록매체에 관한 것이다.

배 경 기 술

<2> 무선센서네트워크(Wireless Sensor Network; WSN)란, 유비쿼터스 컴퓨팅(Ubiqutous Computing) 구현을 위한 기반 네트워크로서, 센싱과 통신 기능을 가지고 있는 소형 무선 송수신 장치인 센서노드(Sensor Node), 그리고 센서노드에서 센싱된 정보를 취합하거나 이벤트성 데이터를 외부로 연계하고 관련 센서 네트워크를 관리하는 싱크노드(Sink Node)로 구성되는 네트워크를 말한다. 무선센서네트워크는 기존의 네트워크와는 달리 의사소통을 목적으로 하는 것이 아니라 자동화된 원격 정보 수집을 기본 목적으로 하는 것이다. 무선센서네트워크는 유비쿼터스 환경의 핵심 기술로서 목표물 추적, 환경 감시, 교통정보 관리, 물류 관리 등 여러 응용 분야에 폭넓게 활용되고 있음은 물론 다양한 잠재적 응용 분야에 활용될 수 있다.

<3> 실제로, 정보통신부 정보통신인프라정책팀의 보고에 따르면, 유비쿼터스 센서네트워크(USN) 관련 세계시장은 2006년 6억불 정도의 수준에서 연평균 66퍼센트의 성장을 통해 2012년 약 128억불 규모로 성장할 것으로 전망하고 있으며, USN 관련 국내시장은 USN 서비스가 본격 도입되는 2008년부터 연평균 71퍼센트의 성장을 통해 2012년 2조 1천억원에 이를 것으로 전망하고 있다.

<4> 이러한 무선센서네트워크에 있어서, 프라이버시는 크게 내용 프라이버시(content privacy)와 전후관계 프라이버시(contextual privacy) 두 종류로 분류된다. 내용 프라이버시는 공격자가 무선센서네트워크상에서 송수신되는 데이터를 도청하고 상기 데이터를 공격자의 목적에 맞게 위조하는 것과 관련되어 있다. 전후관계 프라이버시는 공격자가 무선센서네트워크상에서 데이터의 트래픽 패턴 분석을 통해 이벤트를 최초로 감지한 센서노드인 발견노드 또는 싱크노드의 위치를 추적하는 것과 관련되어 있다.

<5> 무선센서네트워크에 있어서 네트워크 구축 목적이 주의(비밀)를 요하는 이벤트를 감지하는 것이라면 이벤트 발생지역의 위치정보가 공격자에게 노출되어서는 안 된다. 예컨대, 전쟁 시 중앙 통제실에서 아군의 배치 상황, 전투 부대의 이동 경로, 각 군수 물자의 위치 등을 파악하여 원활한 통제를 하기 위해 아군 지역에 센서노드를 배치했을 경우 이러한 일급비밀을 요하는 정보를 감지하는 발견노드의 위치정보가 적군에게 노출된다면 전쟁은 적군에게 유리한 상황에 놓이게 될 것이다. 따라서, 이벤트 발생지역의 위치정보를 노출하지 않기 위해서는 발견노드의 위치정보를 공격자로 하여금 쉽게 획득할 수 없도록 해야 한다.

<6> 또한, 싱크노드의 위치정보도 발견노드의 위치정보만큼 민감한 정보이므로 싱크노드의 위치정보 역시 공격자에게 노출되어서는 안 된다. 예컨대, 감지된 데이터들을 수집하는 싱크노드 역할을 하는 중앙 통제실의 위치정보도 적군에게 노출되지 말아야 한다. 만일 중앙 통제실의 위치정보를 노출시키지 않기 위해 병사가 직접 싱크노드를 지니고 센서노드가 배치된 지역에 투입되어 센서노드로부터 데이터를 수집할 경우 아군 병사의 위치정보가 적군에게 노출되어 위험한 상황에 빠질 수 있다. 그러므로, 발견노드와 싱크노드의 위치 프라이버시는 모두 보호되어야 할 필요가 있다.

<7> 최근 내용 프라이버시 보호와 관련하여서는 다양한 해결책들이 제안되어 왔다. 그러나 내용 프라이버시 보호를

위해 암호화와 인증을 거친 후에도 전후관계 프라이버시 보호와 관련된 문제는 여전히 존재한다. 왜냐하면, 전후관계의 프라이버시를 보호하기 위한 보안 기술에는 암호학이 크게 도움이 되지 않기 때문이다. 즉, 공격자는 송수신되는 패킷을 도청하여 이를 해석할 필요성이 있는 것이 아니라 단순히 패킷의 이동경로를 추적하거나 네트워크 트래픽을 분석하여 발견노드 혹은 싱크노드에 대한 위치정보만 획득하면 되기 때문이다.

<8> 한편, 무선센서네트워크의 센서노드들은 다른 무선 장치들, 예컨대 PDA나 핸드폰 등과는 달리 물리적인 보호가 부족한 공개지역에 넓게 배치되기 때문에 상기 다른 무선 장치들보다 도청이나 네트워크 트래픽 분석 공격에 취약하다는 문제점이 있다. 예를 들면, 미국의 버클리 대학에서 개발한 센서노드인 MICA 제품은 스펙트럼 분석기(spectrum analyzer)에 의해 쉽게 네트워크 토폴로지(network topology)를 노출한다. 따라서, 공격자는 큰 어려움 없이 센서노드들 간의 패킷 경로를 추적할 수 있으며 전체 네트워크 트래픽을 분석할 수 있다.

<9> 이와 같은 상황에서, 최근 무선센서네트워크에서의 위치 프라이버시 보호 기술에 대한 관심이 빠르게 증가하고 있다. 이에 따라 위치 프라이버시 보호 기술에 관한 연구들이 소개되고는 있지만, 내용 프라이버시 관련 연구에 비해서 아직 미흡한 실정이다.

<10> 일반 네트워크상의 위치 프라이버시 보호 기술에 있어서, 양파 라우팅(M. Reed, et al. "Anonymous Connections and Onion Routing", IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 482C494 1998. 참조) 기술은 사용자들이 익명으로 인터넷을 사용할 수 있는 기능을 제공하는 기술이다. 양파 라우팅은 가상 경로를 설정하여 공격자의 네트워크 트래픽 분석 공격으로부터 사용자 또는 서버의 위치 프라이버시 보호를 제공한다. 그러나 양파 라우팅은 높은 계산 오버헤드 및 통신 오버헤드로 인해 자원 제약적인 무선센서네트워크 환경에 적용하기 곤란하다는 문제점이 있다. 또한, 자원 제약적인 무선센서네트워크 환경에서 위치 프라이버시 보호를 위해 별도의 장치를 추가하는 것은 바람직한 방법이 아니다.

<11> 무선센서네트워크에서 발견노드의 위치 프라이버시를 보호하기 위해 제안된 라우팅 기술로는 팬텀 라우팅 방법이 있다(P. Kamat, et al, "Enhancing Source-Location in Sensor Network Routing", Proc. of 25th IEEE International Conference on Distributed Computing Systems(IDCS), 2005. 참조). 팬텀 라우팅 방법은 공격자가 발견노드의 위치 추적을 할 수 없도록 랜덤-워크 기술과 플러딩 기술을 사용한다. 그러나 팬텀 라우팅 방법은 발견노드의 위치 프라이버시에 대한 안전성이 향상되는 면은 있지만 여전히 트래픽 경로가 발견노드로 집중된다는 문제점이 있다.

<12> 또한, 무선센서네트워크에서 싱크노드의 위치 프라이버시를 보호하기 위해 최근 제안된 기술로서 LPR(Location Privacy Routing) 방법이 있다(Y. Jian, et al "Protecting Receiver-Location Privacy in Wireless Sensor Networks", Proc. of 26th IEEE International Conference on Computer Communications (INFOCOM), 2007. 참조). LPR 방식은 근거리 리스트와 원거리 리스트를 이용하여 공격자로부터 싱크노드의 위치 프라이버시를 보호한다. 그러나 LPR 방식은 발견노드가 원거리 리스트에 등재되어 있는 이웃 노드를 택할 경우 싱크노드로 전송되어야만 하는 패킷이 싱크노드로 전송되지 않는다는 문제점이 있다. 또한, LPR 방식 역시 싱크노드로 트래픽이 다소 집중된다는 문제점이 있다. 또한, LPR 방식도 팬텀 라우팅과 마찬가지로 발견노드와 싱크노드의 위치 프라이버시 보호를 동시에 제공할 수 없다는 문제점이 있다.

<13> 현재까지 발견노드 및 싱크노드 양자의 위치 프라이버시 정보를 동시에 보호하는 연구는 아직 소개된바 없다. 또한 기존의 위치 프라이버시 보호 방법은 발견노드가 감지한 데이터를 전송함에 있어서 전송률의 감소를 초래한다는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

<14> 따라서, 본 발명이 이루고자 하는 첫 번째 기술적 과제는, 자원 제약적인 무선센서네트워크에서 데이터 전송률의 감소없이 발견노드 및 싱크노드의 위치 프라이버시를 동시에 보호하는 무선센서네트워크에서의 위치 프라이버시 보호 방법을 제공하는 것이다.

<15> 본 발명이 이루고자 하는 두 번째 기술적 과제는, 상기 무선센서네트워크에서의 위치 프라이버시 보호 방법을 이용하는 무선센서네트워크 시스템을 제공하는 것이다.

<16> 본 발명이 이루고자 하는 세 번째 기술적 과제는, 상기 무선센서네트워크에서의 위치 프라이버시 보호 방법을 무선센서네트워크를 제어하는 컴퓨터 시스템에서 수행하기 위한 프로그램이 기록된 기록매체를 제공하는

것이다.

과제 해결수단

<17> 상기와 같은 첫 번째 기술적 과제를 해결하기 위하여 본 발명은, 무선센서네트워크에서 위치 프라이버시를 보호하는 방법에 있어서, 이벤트를 감지한 센서노드인 발견노드(discoverer node)가 상기 이벤트를 싱크노드(sink node)로 전송하는데 필요한 전송제어정보에 대응하는 위장 전송제어정보를 후보 센서노드(candidate sensor node)에 저장하여 상기 후보 센서노드를 위장 발견노드(faked discoverer node)로 설정하는 위장 발견노드 설정 단계; 및 상기 위장 발견노드에서 위장 이벤트를 전송하기 위해 위장 싱크노드(faked sink node)를 선택하여 상기 위장 전송제어정보에 따라 상기 위장 이벤트를 상기 위장 싱크노드로 전송하는 위장 이벤트 전송 단계를 포함하는 무선센서네트워크에서의 위치 프라이버시 보호 방법을 제공한다.

<18> 본 발명의 일 실시에 따르면, 상기 전송제어정보는, 상기 발견노드에서 상기 이벤트를 상기 싱크노드로 전송하는데 필요한 이벤트 전송 시작시간, 이벤트 전송 지속시간 및 상기 발견노드의 전송 주기에 관한 정보를 포함한다.

<19> 본 발명의 일 실시에 따르면, 상기 후보 센서노드에 저장되는 상기 위장 전송제어정보는, 상기 무선센서네트워크에 대한 공격자가 상기 발견노드에 의한 트래픽 변동과 상기 위장 발견노드에 의한 트래픽 변동을 구별할 수 없도록 하는 값을 지니는 정보이다.

<20> 본 발명의 일 실시에 따르면, 상기 후보 센서노드에 저장되는 상기 위장 전송제어정보는, 상기 전송제어정보에 포함되는 상기 이벤트 전송 시작시간과 동일한 값 또는 상기 이벤트 전송 시작시간보다 이른 값을 지니는 위장 이벤트 전송 시작시간에 관한 정보를 포함한다.

<21> 본 발명의 일 실시에 따르면, 상기 무선센서네트워크에서의 위치 프라이버시 보호 방법은, 상기 위장 발견노드 설정 단계에 후에 상기 위장 발견노드에서 상기 위장 전송제어정보를 이웃 센서노드로 전송하여 상기 이웃 센서노드로 하여금 상기 위장 전송제어정보에 따라 위장 이벤트를 상기 위장 싱크노드로 전송하도록 하는 단계를 더 포함한다.

<22> 본 발명의 일 실시에 따르면, 상기 무선센서네트워크가 이벤트 감지 기반 무선센서네트워크인 경우 상기 무선센서네트워크에서의 위치 프라이버시 보호 방법은, 상기 위장 발견노드 설정 단계 전에 상기 발견노드에서 상기 위장 전송제어정보를 생성하여 상기 후보 센서노드로 전송하는 위장 전송제어정보 전송 단계를 더 포함한다.

<23> 본 발명의 일 실시에 따르면, 상기 무선센서네트워크가 이벤트 감지 기반 무선센서네트워크인 경우 상기 위장 전송제어정보 전송 단계는, 상기 발견노드가 상기 무선센서네트워크의 전송 경로상 상기 싱크노드보다 멀리 위치한 센서노드 중에서 상기 후보 센서노드를 선택하여 상기 위장 전송제어정보를 상기 후보 센서노드로 전송하는 단계이다.

<24> 본 발명의 일 실시에 따르면, 상기 무선센서네트워크가 쿼리 기반 무선센서네트워크인 경우 상기 무선센서네트워크에서의 위치 프라이버시 보호 방법은, 상기 위장 발견노드 설정 단계 전에 상기 싱크노드에서 상기 위장 전송제어정보를 생성하여 상기 후보 센서노드로 전송하는 단계를 더 포함한다.

<25> 본 발명의 일 실시에 따르면, 상기 무선센서네트워크가 주기 기반 무선센서네트워크인 경우 상기 무선센서네트워크에서의 위치 프라이버시 보호 방법은, 상기 위장 발견노드 설정 단계 전에 상기 싱크노드에서 상기 위장 전송제어정보를 생성하여 상기 후보 센서노드로 전송하는 위장 전송제어정보 전송 단계를 더 포함하고, 상기 무선센서네트워크의 전송 주기마다 상기 단계들을 반복한다.

<26> 본 발명의 일 실시에 따르면, 상기 무선센서네트워크가 주기 기반 무선센서네트워크인 경우 상기 위장 전송제어정보 전송 단계는, 상기 싱크노드에서 상기 무선센서네트워크의 상기 전송 주기마다 새로운 후보 센서노드를 선택하여 상기 위장 전송제어정보를 상기 새로운 후보 센서노드로 전송하는 단계이다.

<27> 상기와 같은 두 번째 기술적 과제를 해결하기 위하여 본 발명은, 이벤트를 감지한 센서노드인 발견노드(discoverer node) 및 싱크노드(sink node)의 위치 프라이버시를 보호하는 무선센서네트워크 시스템에 있어서, 상기 발견노드가 상기 이벤트를 상기 싱크노드로 전송하는데 필요한 전송제어정보에 대응하는 위장 전송제어정보를 저장하는 위장 발견노드(faked discoverer node); 및 상기 위장 발견노드로부터 위장 이벤트를 수신하는 위장 싱크노드(faked sink node)를 포함하고, 상기 위장 발견노드는 상기 무선센서네트워크 시스템에 포함되는 센서노드 중에서 상기 위장 싱크노드를 선택하여 상기 위장 전송제어정보에 따라 상기 위장 이벤트를 상기 위장

싱크노드로 전송하는 위치 프라이버시를 보호하는 무선센서네트워크 시스템을 제공한다.

<28> 상기와 같은 두 번째 기술적 과제를 해결하기 위하여 본 발명은, 이벤트 감지 기반 무선센서네트워크에서 이벤트를 감지한 센서노드인 발견노드(discoverer node) 및 싱크노드(sink node)의 위치 프라이버시를 보호하는 무선센서네트워크 시스템에 있어서, 상기 발견노드가 상기 이벤트를 상기 싱크노드로 전송하는데 필요한 전송제어정보에 대응하는 위장 전송제어정보를 생성하여 전송하는 상기 발견노드; 상기 발견노드로부터 상기 위장 전송제어정보를 수신하여 저장하는 위장 발견노드(faked discoverer node); 및 상기 위장 발견노드로부터 위장 이벤트를 수신하는 위장 싱크노드(faked sink node)를 포함하고, 상기 위장 발견노드는 상기 이벤트 감지 기반 무선센서네트워크에 포함되는 센서노드 중에서 상기 위장 싱크노드를 선택하여 상기 위장 전송제어정보에 따라 상기 위장 이벤트를 상기 위장 싱크노드로 전송하는 위치 프라이버시를 보호하는 무선센서네트워크 시스템을 제공한다.

<29> 상기와 같은 두 번째 기술적 과제를 해결하기 위하여 본 발명은, 쿼리 기반 무선센서네트워크에서 이벤트를 감지한 센서노드인 발견노드(discoverer node) 및 싱크노드(sink node)의 위치 프라이버시를 보호하는 무선센서네트워크 시스템에 있어서, 상기 발견노드가 상기 이벤트를 상기 싱크노드로 전송하는데 필요한 전송제어정보에 대응하는 위장 전송제어정보를 생성하여 전송하는 상기 싱크노드; 상기 싱크노드로부터 상기 위장 전송제어정보를 수신하여 저장하는 위장 발견노드(faked discoverer node); 및 상기 위장 발견노드로부터 위장 이벤트를 수신하는 위장 싱크노드(faked sink node)를 포함하고, 상기 위장 발견노드는 상기 쿼리 기반 무선센서네트워크에 포함되는 센서노드 중에서 상기 위장 싱크노드를 선택하여 상기 위장 전송제어정보에 따라 상기 위장 이벤트를 상기 위장 싱크노드로 전송하는 위치 프라이버시를 보호하는 무선센서네트워크 시스템을 제공한다.

<30> 상기와 같은 두 번째 기술적 과제를 해결하기 위하여 본 발명은, 주기 기반 무선센서네트워크에서 이벤트를 감지한 센서노드인 발견노드(discoverer node) 및 싱크노드(sink node)의 위치 프라이버시를 보호하는 무선센서네트워크 시스템에 있어서, 상기 발견노드가 상기 이벤트를 상기 싱크노드로 전송하는데 필요한 전송제어정보에 대응하는 위장 전송제어정보를 생성하여 전송하는 상기 싱크노드; 상기 싱크노드로부터 상기 위장 전송제어정보를 수신하여 저장하는 위장 발견노드(faked discoverer node); 및 상기 위장 발견노드로부터 위장 이벤트를 수신하는 위장 싱크노드(faked sink node)를 포함하고, 상기 위장 발견노드는 상기 쿼리 기반 무선센서네트워크에 포함되는 센서노드 중에서 상기 위장 싱크노드를 선택하여 상기 위장 전송제어정보에 따라 상기 위장 이벤트를 상기 위장 싱크노드로 전송하고, 그리고 상기 싱크노드는 상기 주기 기반 무선센서네트워크의 전송 주기마다 새로운 위장 발견노드를 선택하여 상기 위장 전송제어정보를 상기 새로운 위장 발견노드로 전송하는 위치 프라이버시를 보호하는 무선센서네트워크 시스템을 제공한다.

<31> 상기와 같은 세 번째 기술적 과제를 해결하기 위하여 본 발명은, 상기 무선센서네트워크에서의 위치 프라이버시 보호 방법을 상기 무선센서네트워크를 제어하는 컴퓨터 시스템에서 실행하기 위한 프로그램이 기록된 기록매체로서, 상기 컴퓨터 시스템이 판독할 수 있는 상기 기록매체를 제공한다.

효 과

<32> 본 발명에 따른 무선센서네트워크에서의 위치 프라이버시 보호 방법과 이를 이용한 무선센서네트워크 시스템 및 기록매체는, 자원 제약적인 무선센서네트워크 환경에서 발견노드 및 싱크노드의 위치 프라이버시 안정성을 동시에 제공하면서도 기존 위치 프라이버시 보호 기술에 비해 데이터 전송률을 현저히 향상시킨다는 이점을 제공한다.

발명의 실시를 위한 구체적인 내용

<33> 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명의 개요 및 관련이론을 개괄적으로 설명한다.

<34> 본 발명은 무선센서네트워크에서 발견노드(dicoverer node) 및 싱크노드(sink node)에 대한 위치 프라이버시(location privacy)를 보호하기 위한 라우팅 알고리즘을 소개한다. 본 발명은 발견노드 및 싱크노드에 관한 위치정보를 공격자에게 노출하지 않기 위해 다수의 위장 발견노드(faked dicoverer node)와 위장 싱크노드(faked sink node)를 만들어 공격자가 실제 발견노드와 싱크노드의 위치를 추적하기 어렵게 만드는 기술이다. 상기 위장 발견노드는 이벤트가 자신의 주위에서 발생한 것처럼 꾸미기 위해 임의의 데이터(위장 이벤트)를 생성하여 상기 위장 싱크노드로 전송한다. 상기 위장 싱크노드의 수가 많을수록 공격자는 실제 발견노드와 싱크노드에 대한 위치정보를 획득하기 어려워진다. 즉, 본 발명에 따르면 무선센서네트워크에서 다양한 임의의 전송경로가 생

성되고 공격자는 이러한 전송경로가 발견노드 또는 싱크노드로 향하는 실제 전송 경로인지 아니면 위장된 전송 경로인지 구별할 수 없게 된다.

<35> 본 발명은 이벤트 전송 과정에 따라 그에 대응하는 라우팅 알고리즘의 일부 과정이 달라질 수 있기 때문에 무선센서네트워크의 유형을 고려하여 설명하여야 한다. 따라서, 본 명세서 전반에 걸쳐 무선센서네트워크는 아래와 같이 3가지 유형으로 분류하여 정의한다.

<36> **이벤트 감지 기반 무선센서네트워크**

<37> 이벤트 감지 기반 무선센서네트워크란 센서노드가 특정 이벤트를 감지하였을 때 또는 센서노드가 미리 정의된 임계값 이상 또는 이하의 값을 지니는 이벤트를 감지하였을 때 상기 센서노드가 감지된 이벤트에 관한 데이터를 싱크노드로 전송하는 유형의 무선센서네트워크를 말한다.

<38> 이벤트 감지 기반 무선센서네트워크는 주로 군사적 목적이나 환경 감시 목적 등으로 사용될 수 있다. 예컨대, 전쟁시 전장에 센서노드들을 설치하여 아군의 부대 배치, 군수 물자의 위치, 적군의 갑작스런 출현 등을 파악하는 데 사용할 수 있다. 또한, 산림, 들판 등에 감시가 필요한 범위 안에 센서노드를 설치하여 동물의 이동 경로 추적 또는 화재 방지 목적으로 사용될 수 있다.

<39> **쿼리 기반 무선센서네트워크**

<40> 쿼리 기반 무선센서네트워크란 싱크노드의 쿼리(query)에 따라 센서노드가 감지된 이벤트에 관한 데이터를 싱크노드로 전송하는 유형의 무선센서네트워크를 말한다.

<41> 쿼리 기반 무선센서네트워크의 경우 싱크노드가 각 지역에 배치된 센서노드의 위치 정보를 알고 있거나 각 지역의 대표 센서노드의 위치 정보를 미리 저장하고 있어야 한다. 싱크노드는 무선센서네트워크에서 감지된 데이터를 얻기를 원할 때마다 쿼리를 삽입한 패킷을 생성한 후, 해당 지역의 센서노드에게 패킷을 전송한다. 패킷을 수신한 센서노드는 상기 패킷에 삽입된 쿼리가 자신이 실행해야 하는 것인지를 판단하여, 자신이 실행해야 하는 것이라면 상기 쿼리를 수행한 후 감지된 데이터를 상기 쿼리에 맞게 처리하여 싱크노드로 전송한다. 만일 자신이 실행할 필요가 없으면 패킷을 다음 홉으로 전송한다.

<42> 쿼리 기반 무선센서네트워크는 기상청 등에 사용될 수 있다. 예컨대, 기상청에서 각 지역의 기온, 습도, 풍속, 강우량 등의 정보를 원할 때 그 목적에 적합한 쿼리를 삽입하여 패킷을 생성한 다음 상기 패킷을 각 지역에 배치된 센서노드로 전송하면 된다.

<43> **주기 기반 무선센서네트워크**

<44> 주기 기반 무선센서네트워크란 미리 정의된 시간이 경과할 때마다 각 센서노드가 감지된 데이터를 싱크노드로 전송하거나 계속적으로 수집된 데이터들을 미리 정의된 시간이 되었을 때 정해진 절차에 따라 처리한 후 싱크노드로 상기 처리된 데이터를 전송하는 유형의 무선센서네트워크를 말한다.

<45> 주기 기반 무선센서네트워크는 의학 분야 등에 사용될 수 있다. 예컨대, 심장 질환 환자의 몸에 센서를 부착하여 심장박동 수 등 의사가 환자의 건강을 위해 필요한 환자 정보를 주기적으로 보고받을 목적으로 사용된다. 센서노드에 의해 주기적으로 수집된 정보는 의사가 환자의 건강 상태를 체계적으로 관리하는데 사용될 수 있으며 이를 바탕으로 정확한 진단을 처방할 수 있다.

<46> 본 발명을 설명하기 위한 무선센서네트워크 환경은 다음과 같은 내용을 전제로 한다.

<47> 무선센서네트워크에서 싱크노드를 포함한 각 센서노드는 센서필드에 배치된 후, 각 센서노드와의 대략적인 거리를 알고 있다고 전제한다. 위성 항법 장치(Global Positioning System; GPS)와 같은 장치를 이용하여 대략적인 거리를 알 수 있으며 정확한 거리를 알고 있을 필요는 없다.

<48> 만일 GPS와 같은 장치가 없어도 각 센서노드는 비콘 메시지를 통하여 다른 센서노드와의 홉 수를 알 수 있다. 각 센서노드는 홉 수를 0으로 설정하여 비콘 메시지를 이웃 센서노드들에게 브로드캐스트한다. 상기 이웃 센서노드들은 홉 수를 1씩 늘리면서 다른 이웃 센서노드들에게 다시 브로드캐스트한다. 비콘 메시지가 더 이상 브로드캐스트할 이웃 센서노드가 없는 말단 센서노드까지 도달하면 상기 말단 센서노드들은 최초로 브로드캐스트한 센서노드로 자신의 아이디 및 홉 수가 계산된 비콘 메시지를 재전송한다. 각 센서노드는 자신(n_i)과 다른 센서노드(n_j)로부터 수신한 비콘 메시지의 홉 수를 획득하여 리스트 L_i에 추가한다. 무선센서네트워크 설립 초기에 비콘 메시지 브로드캐스트로 인한 통신 오버헤드가 커질 수 있다. 그러나 기존의 다른 방법들에 있어서 각 센서노

드로부터 싱크노드까지의 거리를 계산하기 위해 싱크노드가 이동할 때마다 비콘 브로드캐스트를 실행한 것과는 달리 본 발명은 최초 한번이면 계산된 거리를 재사용할 수 있어 싱크노드의 이동으로 인한 추가적인 통신 오버헤드나 시간 지연이 발생하지 않는다는 이점이 있다.

<49> 센서노드간의 통신은 암호화되어 있다고 전제한다. 즉, 기존의 여러 방법을 통해 각 센서노드 간 또는 센서노드와 싱크노드간의 통신은 모두 암호화가 이루어졌다고 전제한다. 그러므로 공격자가 송수신 패킷을 단순히 도청을 함으로써 얻을 수 있는 이득은 없다.

<50> 또한, 모든 센서노드 간에 대략적인 동기화를 전제한다. 모든 센서노드가 지니고 있는 타이머가 정확히 동일할 필요는 없으며 어느 정도 오차는 허용된다. 아래에서 다시 설명하겠지만, 각 센서노드 간의 대략적인 동기화가 필요한 이유는 본 발명에서 위장 이벤트 전송시간이 실제 이벤트 전송시간과 동일 또는 유사할 때 공격자가 실제 발견노드와 위장 발견노드를 구별하기 어렵기 때문이다.

<51> 이하, 본 발명의 기술적 과제의 해결 방안을 명확화하기 위해 첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 상세하게 설명한다. 다만, 본 발명을 설명함에 있어서 관련된 공지기술 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불명료하게 할 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다. 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.

<52> 도 1에는 본 발명에 따른 위치 프라이버시를 보호하는 무선센서네트워크 시스템의 일례가 도시되어 있다.

<53> 도 2에는 본 발명에 따른 무선센서네트워크에서의 위치 프라이버시 보호 방법의 일례가 흐름도로 도시되어 있다.

<54> 본 명세서에서 사용되는 기호의 정의는 하기 표 1과 같다.

표 1

<55>

기 호	정 의
Ω	정의된 인덱스의 집합
$\mathbb{N}=\{n_i \mid i\in\Omega\}$	$i(\in\Omega)$번째 센서 노드(n_i)의 집합 (모든 센서 노드의 집합)
s	싱크노드
$s'_i(\in N)$	i번째로 위장된 싱크노드
k	위장된 싱크노드의 수

$d(\in N)$	발견노드
$d'_i(\in N)$	i번째로 위장된 발견노드
$D'=\{d'_i \mid 0<i\le k, d'_i\in N\}$	위장된 발견노드의 집합
$L_i=\{dist(n_i,n_j) \mid n_j\in N\}$	노드 n_i가 노드 n_j와의 거리 또는 홉 수를 저장하는 리스트
A	노드 d 또는 노드 s를 포획하려는 공격자

<56>

$evnt$	발생한 이벤트
$evnt'_i$	i번째 위장된 이벤트 (임의의 값)
per_{evnt}	$evnt$를 감지한 노드 d의 전송주기
$per_{evnt'_i}$	노드 d'_i의 전송주기
$dura_{evnt}$	노드 d의 $evnt$ 전송지속시간
$dura_{evnt'_i}$	노드 d'_i의 $evnt'_i$ 전송지속시간
$time_{evnt}$	노드 d가 노드 s로 $evnt$를 전송하는 전송시작시간
$time_{evnt'_i}$	노드 d'_i가 노드 s'_i로 $evnt'_i$를 전송하는 전송시작시간

<57>

<58> 도 1 및 도 2를 참조하면, 본 발명에 따른 무선센서네트워크에서의 위치 프라이버시 보호 방법은, 우선 이벤트(evnt)를 감지한 센서노드인 발견노드(d; 100)가 상기 이벤트(evnt)를 싱크노드(s; 110)로 전송하는데 필요한 전송제어정보에 대응하는 위장 전송제어정보를, 위장 발견노드(d')로 사용될 후보 센서노드(candidate sensor node; 120)에 저장하여 상기 후보 센서노드를 위장 발견노드(d'; 120)로 설정한다(S200).

<59> 상기 전송제어정보에는 상기 발견노드(100)에서 상기 이벤트(evnt)를 상기 싱크노드(110)로 전송하는데 필요한 이벤트 전송 시작시간($time_{evnt}$), 이벤트 전송 지속시간(dur_{evnt}) 및 상기 발견노드의 전송 주기(per_{evnt})에 관한 정보가 포함될 수 있다.

<60> 상기 전송제어정보에 대응하는 상기 위장 전송제어정보에는 상기 위장 발견노드(120)에서 위장 이벤트(evnt')를 위장 싱크노드(s'; 130)로 전송하는데 필요한 위장 이벤트 전송 시작시간($time_{evnt'}$), 위장 이벤트 전송 지속시간($dur_{evnt'}$) 및 상기 위장 발견노드의 전송 주기($per_{evnt'}$)에 관한 정보가 포함될 수 있다.

<61> 상기 무선센서네트워크에 대한 공격자(A)가 상기 발견노드와 상기 위장 발견노드를 구별할 수 없도록 상기 위장 전송제어정보가 지니는 값들을 상기 전송제어정보가 지니는 값들과 동일 또는 유사한 값으로 설정한다. 즉, 상기 공격자(A)가 상기 발견노드(100)에 의한 트래픽 변동과 상기 위장 발견노드(120)에 의한 트래픽 변동을 구별할 수 없도록 하는 값으로 설정한다. 특히, 상기 위장 전송제어정보의 상기 위장 이벤트 전송 시작시간($time_{evnt'}$)은 상기 전송제어정보의 상기 이벤트 전송 시작시간($time_{evnt}$)과 동일한 값 또는 이른 값으로 설정한다.

<62> 본 발명의 일 실시예에 있어서, 상기 무선센서네트워크가 이벤트 감지 기반 무선센서네트워크인 경우, 상기 발견노드(100)가 상기 후보 센서노드(120)를 선택하고 상기 위장 전송제어정보를 생성하여 상기 후보 센서노드(120)로 전송한다.

<63> 구체적으로 설명하면, 노드 n_1이 이벤트(evnt)를 최초로 발견한 발견노드(100)인 경우 상기 발견노드(100)는 상기 이벤트(evnt)를 상기 싱크노드(110)에 보고하기 전에 노드 간 거리 또는 홉 수를 저장한 리스트(L_1)를 검색하여 일정 거리 이상에 위치한 k개(예컨대, 3개)의 센서노드를 상기 위장 발견노드(d')로 사용될 후보 센서노드로서 임의로 선택한다. 그리고 상기 발견노드(100)는 상기 k개의 후보 센서노드의 아이디들(예컨대, n_{100}, n_{101}, n_{102})을 위장 발견노드 집합(D')으로서 저장한다. 상기 위장 발견노드 집합(D')은 하기 수학식 1과 같이 표현할 수 있다.

수학식 1

<64> $$D' = \{d'_i \mid d'_1 = n_{100}, d'_2 = n_{101}, d'_3 = n_{102}, 0 < i \leq k\}$$

<65> 그리고, 상기 발견노드(100)는 상기 위장 전송제어정보를 패킷에 넣어 상기 위장 발견노드 집합(D')에 속해 있는 각각의 후보 센서노드로 전송하여 상기 후보 센서노드로 하여금 상기 위장 전송제어정보를 저장하도록 함으

로써 상기 후보 센서노드를 위장 발견노드로서 설정한다. 이러한 과정에서 상기 발견노드(100)는 상기 무선센서네트워크의 전송 경로상 상기 싱크노드보다 멀리 위치한 센서노드 중에서 상기 후보 센서노드(120)를 선택하여 상기 위장 전송제어정보를 상기 후보 센서노드(120)로 전송할 수 있다. 무선센서네트워크상에서 위장 발견노드들이 넓게 분포하도록 함으로써 네트워크 트래픽을 분산시키기 위함이다.

<66> 본 발명의 일 실시예에 있어서, 상기 무선센서네트워크가 쿼리 기반 무선센서네트워크인 경우, 상기 발견노드(100)가 아닌 상기 싱크노드(110)가 상기 후보 센서노드(120)를 선택하고 상기 위장 전송제어정보를 생성하여 상기 후보 센서노드(120)로 전송한다.

<67> 본 발명의 일 실시예에 있어서, 상기 무선센서네트워크가 주기 기반 무선센서네트워크인 경우, 상기 발견노드(100)가 아닌 상기 싱크노드(110)가 상기 후보 센서노드(120)를 선택하고 상기 위장 전송제어정보를 생성하여 상기 후보 센서노드(120)로 전송한다. 그리고, 상기 싱크노드(110)는 전송 주기마다 새로운 후보 센서노드를 선택하여 상기 위장 전송제어정보를 상기 새로운 후보 센서노드로 전송한다. 주기 기반 무선센서네트워크의 경우 주기마다 새로운 위장 발견노드를 설정하는 것은, 일정한 네트워크 트래픽 패턴이 장시간 지속되면 공격자의 패킷 추적에 의해 싱크노드가 포획될 가능성이 커지므로 공격자에게 일정한 네트워크 트래픽 패턴을 제공하지 않기 위함이다.

<68> 그 다음, 상기 위장 발견노드(120)에서 위장 이벤트를 전송하기 위해 위장 싱크노드(faked sink node; 130)를 선택한다(S210).

<69> 구체적으로 설명하면, 상기 위장 전송제어정보를 저장한 상기 위장 발견노드(120; d'_1, d'_2 또는 d'_3)는 센서노드 간 거리 또는 홉 수를 정장하는 리스트(L_{100}, L_{101} 또는 L_{102})에서 소정의 거리 이상에 있는 센서노드를 위장 싱크노드(130; s'_1, s'_2 또는 s'_3)로서 선택한다.

<70> 본 발명의 일 실시예에 있어서, 상기 위장 발견노드(120)는 상기 위장 전송제어정보를 이웃 센서노드(122)로 전송하고 상기 이웃 센서노드(122)로 하여금 위장 이벤트(evnt')를 생성하도록 한다(S220).

<71> 구체적으로 설명하면, 상기 위장 발견노드(120; d'_1, d'_2 또는 d'_3)는 이웃 노드들에게 위장 이벤트($evnt_1$, $evnt_2$ 또는 $evnt_3$)를 생성하라는 메시지를 전송하며, 이때 상기 위장 전송제어정보($time_{evnt'}$, $dur_{evnt'}$, $per_{evnt'}$)를 함께 전송한다.

<72> 그 다음, 상기 위장 발견노드(120) 또는 상기 위장 발견노드(120)와 이웃 센서노드들은 상기 위장 전송제어정보에 따라 위장 이벤트(evnt')를 상기 위장 싱크노드로 전송한다(S230).

<73> 구체적으로 설명하면, 위장 발견노드(d'_1)는 이웃 센서노드들과 함께 임의의 위장 이벤트($evnt'_1$)를 생성하고 상기 위장 이벤트 전송 시작시간($time_{evnt'1}$)을 시작으로 상기 위장 발견노드의 전송 주기($per_{evnt'1}$)마다 상기 위장 이벤트 전송 지속시간($dur_{evnt'1}$)동안 상기 위장 이벤트($evnt'_1$)를 전송한다. 상기 위장 발견노드(d'_1)는 소정 시간($time_{evnt'1}+dur_{evnt'1}$)이 경과하면, 상기 위장 이벤트($evnt'_1$) 생성을 중지하고 위장 발견노드로서의 역할을 마친다. 다른 위장 발견노드들(d'_2, d'_3)도 동일한 과정을 수행한다.

<74> 본 발명의 일 실시예에 있어서, 상기 무선센서네트워크가 상기 주기 기반 무선센서네트워크인 경우, 위에서 설명한 바와 같이 상기 싱크노드(110)가 주기마다 새로운 위장 발견노드를 선택 및 설정하여 상기 과정들을 주기마다 반복하게 된다.

<75> 상기 위장 발견노드들(120)이 상기 위장 이벤트(evnt')를 상기 위장 싱크노드(130) 전송하는 동안, 상기 발견노드(100)는 상기 이벤트(evnt)를 상기 싱크노드(110)로 전송함으로써 네트워크 트래픽을 분산시키고 공격자(A)로 하여금 실제 데이터 전송 경로를 구별하지 못하도록 한다.

<76> 이상에서 설명한 바와 같이, 본 발명은 다양한 무선센서네트워크 환경에 유동성 있게 적용가능하다.

<77> 또한, 본 발명에 따른 무선센서네트워크에서의 위치 프라이버시 보호 방법은 무선센서네트워크를 제어하는 컴퓨터 시스템이 판독할 수 있는 기록매체에 상기 컴퓨터 시스템이 읽어들일 수 있는 프로그램 코드로서 구현하는 것이 가능하다. 즉, 본 발명은 센서노드(싱크노드)의 각각의 OS(Operating System)를 통해 소프트웨어적으로 구현될 수 있다. 본 발명이 소프트웨어를 통해 실행될 때, 본 발명의 구성 수단들은 필요한 작업을 실행하는 코드 세그먼트들이다. 프로그램 또는 코드 세그먼트들은 프로세서 판독 가능 매체에 저장되거나 전송 매체 또는 통신

망에서 반송파와 결합된 컴퓨터 데이터 신호에 의하여 전송될 수 있다.

<78> 컴퓨터 시스템이 판독할 수 있는 기록매체에는 컴퓨터 시스템이 읽어들일 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터 시스템이 판독할 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장장치 등이 있다. 또한, 컴퓨터 시스템이 판독할 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽어들일 수 있는 코드가 저장되고 실행될 수 있다.

<79> 이하, 시뮬레이션 결과 분석을 통해 본 발명의 현저한 효과를 검증한다.

<80> 본 발명의 효과를 검증하기 위한 시뮬레이션 환경은 4001×4001 공간 위에 1600(=40×40)개의 센서노드와 1개의 싱크노드로 구성하였다. 센서노드의 통신 반경을 r이라고 정의하였을 때, 각 센서노드 사이의 거리는 r'(r'=100 ≤r)로 일정하다.

<81> 시뮬레이션은 무선센서네트워크 유형 중 이벤트 감지 기반 무선센서네트워크 환경에서 이루어졌으며 이벤트는 한 곳에 고정되거나 계속하여 이동할 수 있다. 이벤트가 발생하는 최초 좌표는 [50, 50]이며 이벤트가 고정되어 있을 때 발견노드의 좌표는 [100, 100]이다. 그리고 네트워크 트래픽 분석을 용이하게 하기 위해 싱크노드를 구성된 무선센서네트워크의 중앙에 위치시켰다. 따라서, 싱크노드는 [2001, 2001]에 위치한다.

<82> 시뮬레이션 시간은 20.0으로 설정하였다. 상기 설정된 시뮬레이션 시간은 Basic 방식(Basic), LPR 방식(LPR) 그리고 본 발명(prop)의 위치 프라이버시 안전성과 데이터 전송률을 비교하기 위한 충분한 시간이다. 상기 방식들 중 Basic 식(Basic)은 보안 알고리즘을 적용하지 않고 발견노드가 싱크노드까지 AODV(C. E. Perkins and E. M. Royer, "Ad hoc On-demand Distance Vector routing", Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999. 참조) 라우팅 알고리즘에 의해 설정된 최단 거리를 통하여 감지된 데이터를 전송하는 방식이다. LPR 방식(LPR)은 Y. Jian 외 다수의 논문 "Protecting Receiver-Location Privacy in Wireless Sensor Networks"(Proc. of 26th IEEE International Conference on Computer Communications (INFOCOM), 2007.)을 참조한다.

<83> **공격 모델 정의**

<84> 시뮬레이션을 위해 정의된 공격 모델은 LPR에서 정의된 공격 모델을 기반으로 더욱 강력한 공격 모델이다.

<85> 첫째, 공격자의 목적은 오직 발견노드와 싱크노드를 포획하는 것에 있다. 따라서 공격자는 각 센서노드 간 통신 또는 센서노드와 싱크노드 간 통신을 방해하거나 간섭하지 않는다. 둘째, 공격자는 구성된 무선센서네트워크 내의 모든 센서노드의 트래픽(Traffic)을 감시할 수 있는 장치를 지니고 있다. 공격자는 무선센서네트워크 전체를 포괄하는 범위의 레이더나 스펙트럼 분석기 같은 장치를 사용하여 트래픽이 집중되는 지역을 확인할 수 있다. LPR 방식에서는 센서노드가 감지할 수 있는 범위(r)와 공격자가 감시할 수 있는 범위(r')를 같게 정의하였으나, 상기 시뮬레이션에서는 더욱 강력한 공격 모델을 정의하였다. 전쟁이 발발했을 때 적군은 자원의 제한이 없는 최신 장비를 토대로 아군의 무선센서네트워크의 트래픽을 분석할 수 있으며 아군 전체의 트래픽을 감시할 수 있기 때문이다. 다만, LPR 방식에서와는 달리 공격자에게 패킷 추적 능력을 부여하지 않았다. 왜냐하면 LPR은 공격자의 감시 범위가 r로 한정되어 있기 때문에 패킷 추적으로 통하여 싱크노드를 발견해야 하나, 상기 시뮬레이션에서 공격자는 전체 네트워크 범위를 감시할 수 있는 능력을 지니고 있기 때문에 패킷 추적 능력은 커다란 효과를 발휘하지 못하기 때문이다.

<86> 세째, 공격자는 전송중인 패킷의 방향을 구분할 수 있다. 이러한 능력은 공격자가 발견노드와 싱크노드의 위치 정보를 구별하여 획득하기 위해 필요한 능력이다. 전송 패킷에 대한 트래픽이 집중되는 지역과 수신 패킷에 대한 트래픽이 집중되는 지역을 구분하여 분석하기 위해 공격자에게 패킷 방향 구분 능력을 부여하였다.

<87> 네째, 공격자는 무선센서네트워크에 사용되는 보안 라우팅 알고리즘을 알고 있다. 공격자는 발견노드와 싱크노드의 위치 프라이버시 보호를 위해 사용되는 알고리즘을 알고 있다는 가정으로 이것은 Kerckhoff의 원리에 따른 것이다. Kerckhoff의 원리란 암호 시스템의 안전성은 암호 알고리즘의 비밀에 의존해서는 안 된다는 것이다.

<88> 다섯째, 공격자는 항상 메모리를 지니고 있다. 공격자는 무선센서네트워크에서 발생하는 트래픽을 분석하여 각 지역별로 그리고 시간별로 메모리에 기록하여 이를 토대로 발견노드와 싱크노드에 대한 위치 정보를 분석할 수 있다.

<89> 여섯째, 공격자가 무선센서네트워크 내에서 발견노드 또는 싱크노드로 의심되는 센서노드를 찾아내었다면 한 번의 이동으로 의심되는 지역으로 이동할 수 있다. 공격자는 네트워크 트래픽 분석 결과 발견노드 또는 싱크노드로 간주되는 센서노드의 위치 정보를 획득하여 여러 번이 아닌 단 한 번의 이동으로 획득한 위치 정보가 발견노

드 또는 싱크노드가 배치된 지역의 위치 정보인지 아닌지를 확인할 수 있다. 확인 결과, 상기 의심되는 센서노드가 발견노드 또는 싱크노드라면 포획에 성공한 것이며, 그렇지 않으면 다음 예상 지역으로 이동한다.

<90> 일곱째, 공격자가 발견노드 또는 싱크노드로부터 근접한 위치에 있는 있으면 발견노드 또는 싱크노드를 포획할 수 있다. 공격자가 발견노드 또는 싱크노드로부터 근접한 거리r"(r"≤r)에 있다면 발견노드 또는 싱크노드 포획에 성공한 것으로 간주한다.

<91> 상기와 같이 정의된 공격 모델을 기반으로 다음과 같이 공격자 알고리즘을 정의한다.

Algorithm : Attacker A

```
Captured_ID = Source_node_id | Sink_node_id

STEP 1 (Attacker is Analyzing) :
while(IsTerminated()) {
if (Current_Time > Previous_Time) {
        for (i=1; i<=Number_Of_All_Nodes; i++) {
                Previous_Time += 0.01;
                Search_Max_ID();
                if(IsCaptured_ID(Current_ID)) {
                        Attack_Success();}}}}

STEP 2 (Attacker is Moving) :
if (STEP 1 IsNotSucceed()) {
for (i=1; i<=Number_Of_All_Nodes; i++) {
        Search_Next_Max_ID();
        if(IsCaptured_ID(Current_ID))
                Attack_Success();}}
```

<92>

<93> 즉, 공격자는 두 가지 상황을 고려하여 행동한다.

<94> 단계 1. 발견노드가 싱크노드로 계속 감지된 데이터를 전달할 때 : 공격자는 0.01초마다 송신 네트워크 트래픽과 수신 네트워크 트래픽을 분석하며 발견노드와 싱크노드의 위치를 탐색한다.

<95> 단계 2. 발견노드가 싱크노드로의 감지된 데이터 전송을 종료했을 때 : 단계 1 동안 공격자가 발견노드나 싱크노드를 포획하지 못했을 때 단계 2에서 탐색을 재시도한다. 공격자는 네트워크 트래픽이 가장 높은 지역부터 메모리의 기록에 근거하여 차례대로 이동하며 발견노드와 싱크노드를 탐색한다.

<96> 도 3a 내지 도 5b에는 각각의 위치 프라이버시 보호 방식에 따른 네트워크 트래픽 패턴이 도시되어 있다.

<97> 도 3a 내지 도 5b에 있어서, x축 및 y축은 각 센서노드가 배치된 좌표를 나타내며 z축은 시뮬레이션 시간 동안 각 센서노드가 송수신한 패킷의 수를 나타낸다.

<98> 도 3a 및 도 3b에는 각각 이벤트가 고정된 경우 및 이벤트가 이동하는 경우에 Basic 방식에 따른 네트워크 트래픽 패턴이 도시되어 있다. 도 3a 및 도 3b에 있어서, 고정된 이벤트는 좌표 [50, 50]에 고정되고, 이동하는 이벤트는 좌표 [50,50], [3950, 50], [3950, 3950], [50, 3950], 및 [50,50]으로 구성되는 무선센서네트워크의 가장 자리 경로를 통해 시뮬레이션 시간 동안 균일한 속력으로 이동한다.

<99> 도 3a 및 도 3b 참조하면, 이벤트가 고정된 경우보다 이벤트가 이동하는 경우 더 복잡한 네트워크 트래픽 패턴이 나타남을 확인할 수 있다. 즉, 이벤트가 고정된 경우 발견노드 및 싱크노드의 위치를 추적하는 것이 어렵지 않다. 좌표 [50,50]에 위치한 발견노드로부터 좌표 [2001, 2001]에 위치한 싱크노드까지의 네트워크 트래픽 패턴으로 인해 패킷의 경로가 그대로 드러나기 때문이다. 이벤트가 이동하는 경우에는 발견노드의 좌표를 추적하기는 쉽지 않지만, 이벤트가 고정된 경우와 마찬가지로 좌표 [2001, 2001] 지점에 트래픽이 집중되기 때문에 싱크노드의 위치를 쉽게 추적할 수 있다.

<100> 도 4a 및 도 4b에는 각각 LPR 방식에 의한 전송 트래픽 패턴 및 수신 트래픽 패턴이 도시되어 있다.

<101> 도 4a에 도시된 바와 같이, 전송 트래픽 패턴에 있어서 전송 트래픽이 발견노드(좌표 [50, 50])로 집중되어 있음을 알 수 있다. 따라서 공격자는 네트워크 트래픽 분석만으로 발견노드를 쉽게 추적할 수 있다.

<102> 또한 도 4b에 도시된 바와 같이, 수신 트래픽 패턴에 있어서 수신 트래픽이 중앙을 중심으로 집중되어 있음을 알 수 있다. 따라서 공격자는 네트워크 트래픽 분석에 의해 싱크노드의 위치를 어느 정도 예측할 수 있다.

<103> 도 5a 및 도 5b에는 각각 본 발명에 따른 전송 트래픽 패턴 및 수신 트래픽 패턴이 도시되어 있다.

<104> 도 5a에 도시된 바와 같이, 전송 트래픽 패턴에 있어서 전송 트래픽이 발견노드로 집중되지 않음을 확인할 수 있다. 오히려 여러 경로로 트래픽 패턴이 생성된다.

<105> 또한 도 5b에 도시된 바와 같이, 수신 트래픽 패턴에 있어서 수신 트래픽이 중앙에 집중되지 않고 여러 지역으로 분산됨을 확인할 수 있다.

<106> 상기 네트워크 트래픽 패턴 분석 결과를 통해, 본 발명에 의한 네트워크 트래픽 패턴이 기존 방식보다 무선센서네트워크상에 전체적으로 분산되어 있음을 확인할 수 있다.

<107> 도 6a 및 도 6b에는 상기 공격자 알고리즘을 이용하여 각각의 위치 프라이버시 보호 방식에 따른 발견노드 및 싱크노드의 위치 프라이버시 안정성을 분석한 결과가 그래프로 도시되어 있다. 도 6a 및 도 6b에 있어서, x축은 본 발명의 위장 싱크노드의 수를 나타내며, y축은 공격자의 평균 이동 횟수를 나타낸다. 또한, 상기 공격자 알고리즘의 단계 1에서 발견노드나 싱크노드가 포획당한 경우 공격자의 이동 횟수는 1로 설정하여 계산한 것이다.

<108> 도 6a에 도시된 바와 같이, Basic 방식(Basic)과 LPR 방식(LPR)에 대해 상기 공격자 알고리즘을 실행하였을 경우 발견노드가 항상 상기 단계 1에서 공격자에게 포획되었다. 그러나 본 발명(prop)은 발견노드가 상기 단계 1에서 공격자에게 포획당하지 않았으며 시뮬레이션 시간이 종료된 후, 상기 단계 2에서 공격자가 이동하며 탐색할 때 발견 노드가 포획 당했다. 구체적으로, 위장 싱크노드의 수가 7개일 때, 본 발명(prop)의 경우 시뮬레이션 시간이 종료된 후 공격자가 122회 이동을 한 후에야 발견노드를 포획하였다. 따라서, 본 발명은 기존 방식에 비해 발견노드의 위치 프라이버시 안전성을 크게 향상시킴을 확인할 수 있다.

<109> 또한, 도 6b에 도시된 바와 같이, Basic 방식(Basic)에 대해 상기 공격자 알고리즘을 실행하였을 경우 싱크노드가 항상 상기 단계 1에서 포획되었다. LPR 방식(LPR)의 경우 역시 싱크노드가 주로 상기 단계 1에서 포획되었지만 상기 단계 2에서 포획되는 경우도 존재했다. LPR 방식(LPR)의 공격자 평균 이동 횟수를 계산한 결과 약 2.12 정도의 값이 도출되었다. 그러나 본 발명의 경우 대부분 상기 단계 2에서 싱크노드가 공격자에게 포획되었으며, 상기 단계 1에서 싱크노드가 포획되는 경우는 극히 드물었다. 구체적으로, 위장된 싱크노드의 수가 7개일 때, 본 발명(prop)의 경우 공격자가 싱크노드를 포획하기까지 이동한 평균 횟수는 LPR 방식(LRP)에 비해 약 11.5배에 이른다. 따라서, 본 발명은 기존 방식에 비해 싱크노드의 위치 프라이버시 안전성을 크게 향상시킴을 확인할 수 있다.

<110> 결론적으로, 본 발명은 발견노드 및 싱크노드 양자의 위치 프라이버시 보호를 위해 현저히 향상된 안정성을 제공하는 이점이 있다.

<111> 도 7에는 각각의 위치 프라이버시 보호 방식에 따른 데이터 전송률 분석 결과가 그래프로 도시되어 있다.

<112> LPR 방식(LPR)에서는 발견노드가 근거리 리스트 또는 원거리 리스트를 확률 값 p_f에 의해 선택하게 되는데, 이때 발견노드가 원거리 리스트를 선택한다면 감지된 데이터는 싱크노드에게 전송되지 않는다. 상기 p_f값으로서 LPR 방식(LPR)에 관한 상기 논문에서 택한 0.35값을 설정했을 경우, 싱크노드로 감지된 데이터가 전송될 확률은 0.65($0.65=1-p_f$)가 된다. 그러나 본 발명은 확률 값에 무관하게 발견노드에서 감지된 데이터가 모두 싱크노드에게 전송된다. 즉, Basic 방식(Basic)과 마찬가지로 데이터 전송률은 1이며, 기존 방식보다 정밀한 데이터 분석을 필요로 하는 무선센서네트워크 환경에 더 적합하다.

<113> 결론적으로, 본 발명은 기존의 위치 프라이버시 보호 방식들처럼 데이터 전송률 감소를 초래하지 않는다는 이점을 제공한다.

<114> 한편, 본 발명에 있어서 위장 싱크노드의 수가 증가하면 위치 프라이버시 안전성과의 트레이트오프(trade-off) 관계상 통신 오버헤드가 다소 증가하지만, 이는 자원 제약적인 무선센서네트워크 환경에서도 문제되지 않는 수준이다.

<115> 상술한 바와 같이, 본 발명에 따른 무선센서네트워크에서의 위치 프라이버시 보호 방법과 이를 이용한 무선센서네트워크 시스템 및 기록매체는, 자원 제약적인 무선센서네트워크 환경에서 발견노드는 및 싱크노드의 위치 프라이버시 안정성을 동시에 제공하면서도 기존 기술에 비해 데이터 전송률을 현저히 향상시킨다는 이점을 제공한

다.

<116> 지금까지 본 발명에 대해 실시예들을 참고하여 설명하였다. 그러나 당업자라면 본 발명의 본질적인 기술적 사상으로부터 벗어나지 않는 범위에서 본 발명이 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 즉, 본 발명의 진정한 기술적 범위는 첨부된 특허청구범위에 나타나 있으며, 그와 균등범위 내에 있는 모든 차이점은 본 발명에 포함되는 것으로 해석되어야 할 것이다.

도면의 간단한 설명

<117> 도 1은 본 발명에 따른 위치 프라이버시를 보호하는 무선센서네트워크 시스템의 일례를 나타낸 도면.

<118> 도 2는 본 발명에 따른 무선센서네트워크에서의 위치 프라이버시 보호 방법의 일례를 나타낸 흐름도.

<119> 도 3a 및 도 3b는 이벤트가 고정된 경우 및 이벤트가 이동하는 경우에 Basic 방식에 따른 네트워크 트래픽 패턴을 나타낸 도면.

<120> 도 4a 및 도 4b는 LPR 방식에 의한 전송 트래픽 패턴 및 수신 트래픽 패턴을 나타낸 도면.

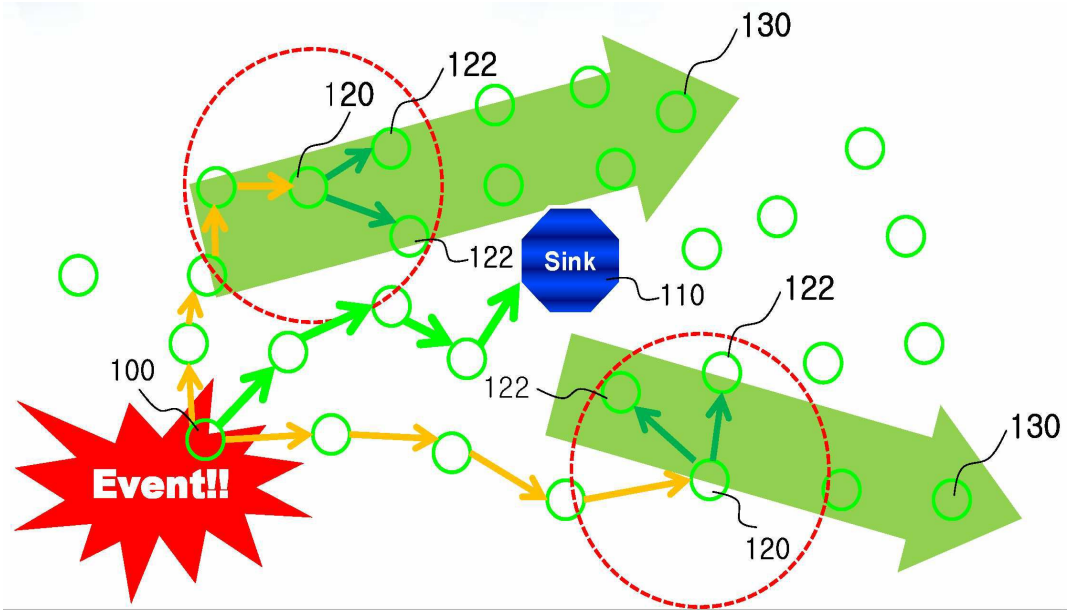
<121> 도 5a 및 도 5b는 본 발명에 따른 전송 트래픽 패턴 및 수신 트래픽 패턴을 나타낸 도면.

<122> 도 6a 및 도 6b는 위치 프라이버시 보호 방식에 따른 발견노드 및 싱크노드의 위치 프라이버시 안정성을 분석한 결과를 나타낸 그래프.

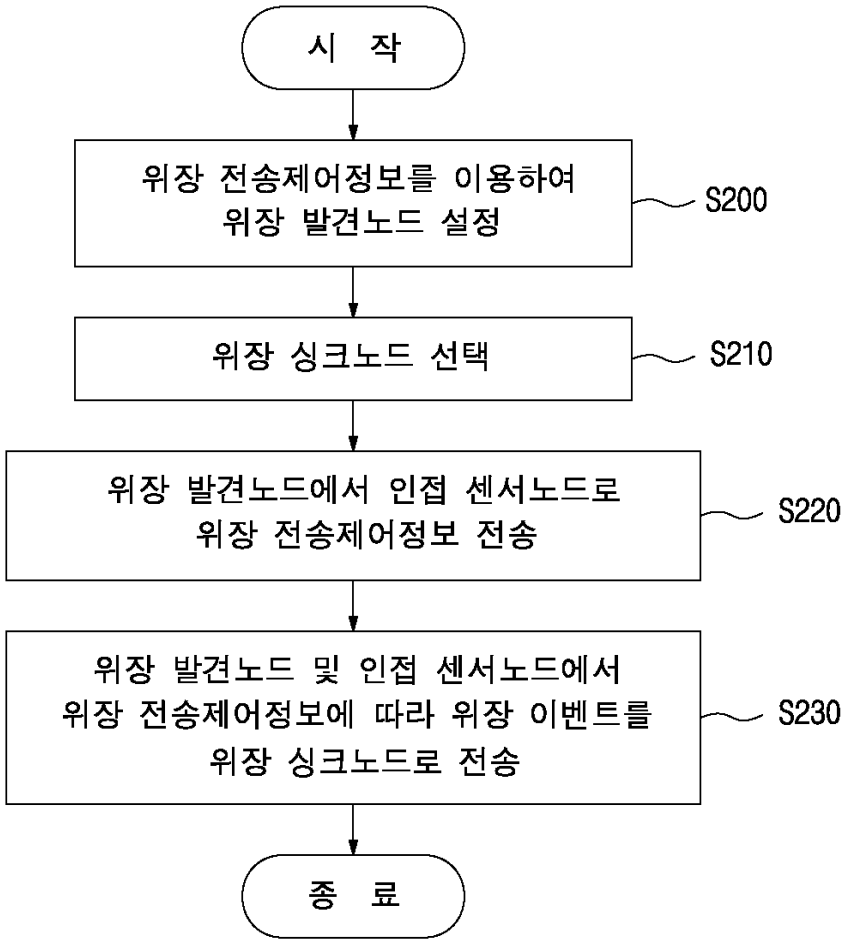
<123> 도 7은 위치 프라이버시 보호 방식에 따른 데이터 전송률 분석 결과를 나타낸 그래프.

도면

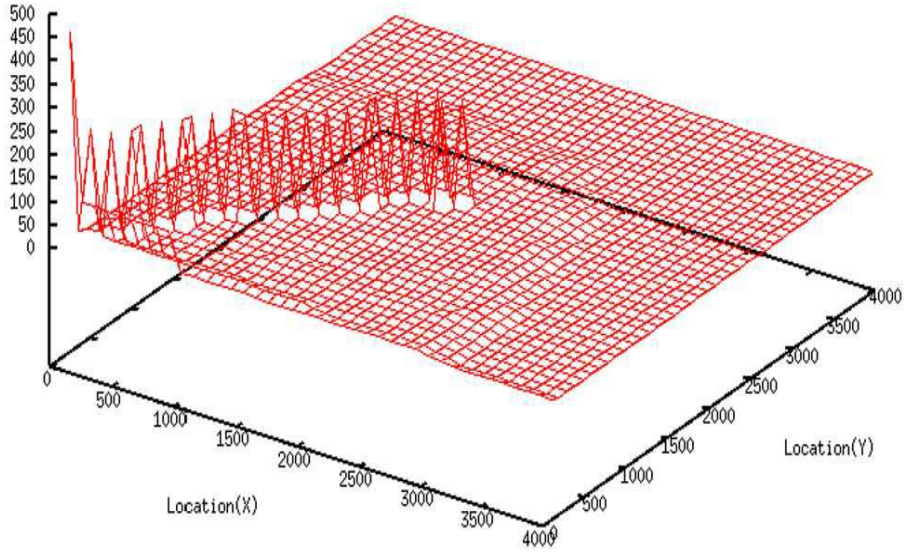
도면1



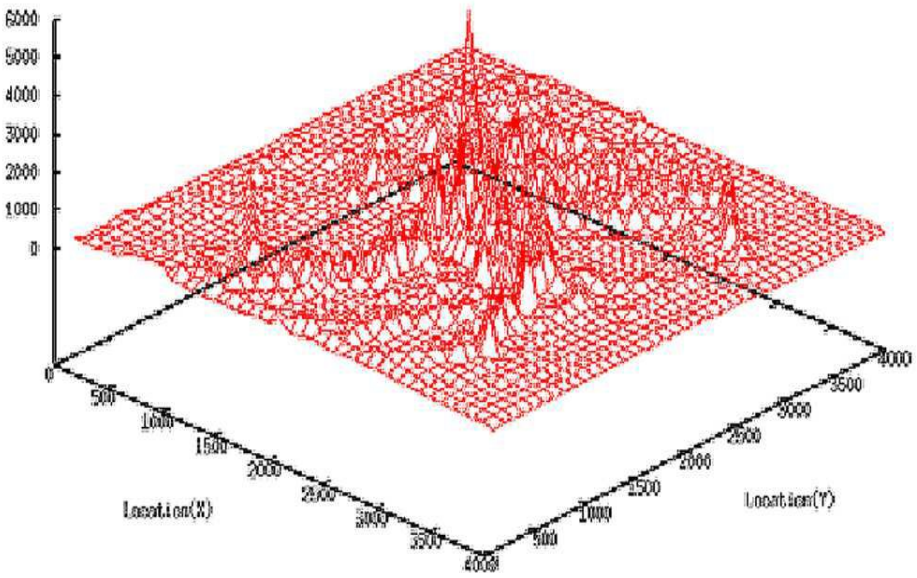
도면2


시 작
위장 전송제어정보를 이용하여
위장 발견노드 설정
S200
위장 싱크노드 선택
S210
위장 발견노드에서 인접 센서노드로
위장 전송제어정보 전송
S220
위장 발견노드 및 인접 센서노드에서
위장 전송제어정보에 따라 위장 이벤트를
위장 싱크노드로 전송
S230
종 료

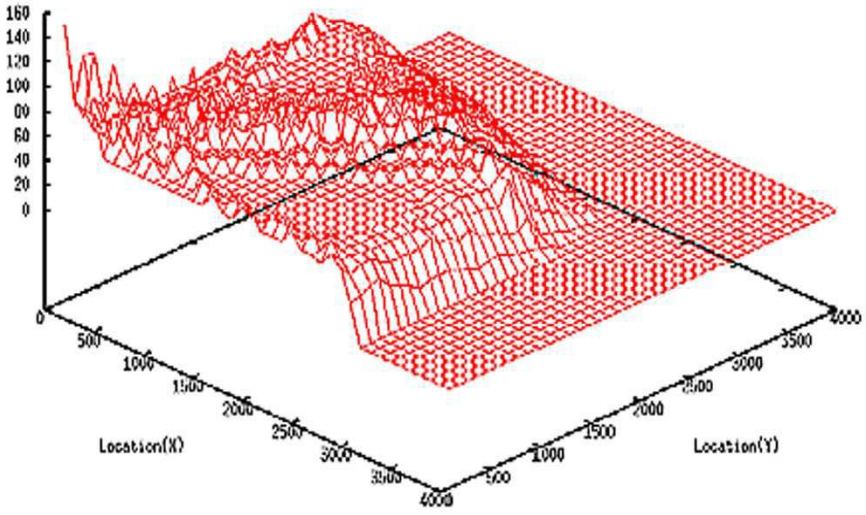
도면3a


500
450
400
350
300
250
200
150
100
50
0
0
500
1000
1500
2000
2500
3000
3500
4000
Location(X)
0
500
1000
1500
2000
2500
3000
3500
4000
Location(Y)

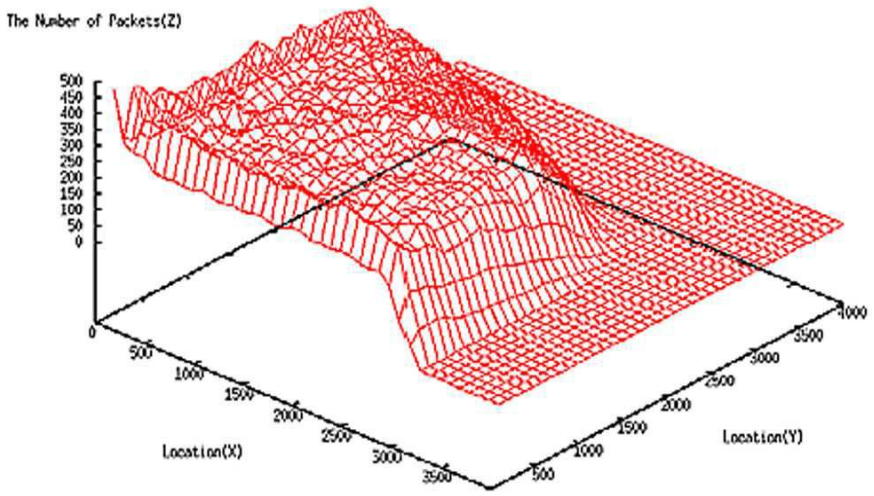
도면3b


6000
5000
4000
3000
2000
1000
0
0
500
1000
1500
2000
2500
3000
3500
4000
Location(X)
Location(Y)

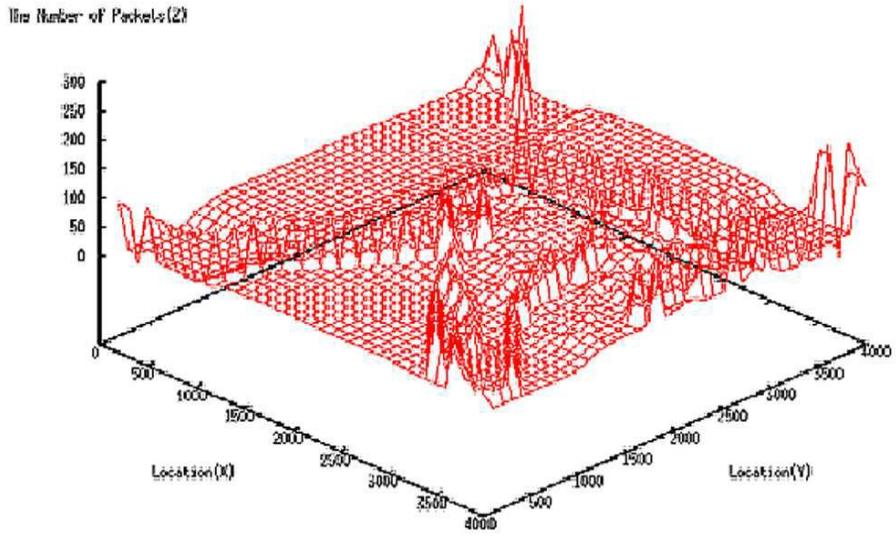
도면4a


160
140
120
100
80
60
40
20
0
0
500
1000
1500
2000
2500
3000
3500
4000
Location(X)
Location(Y)

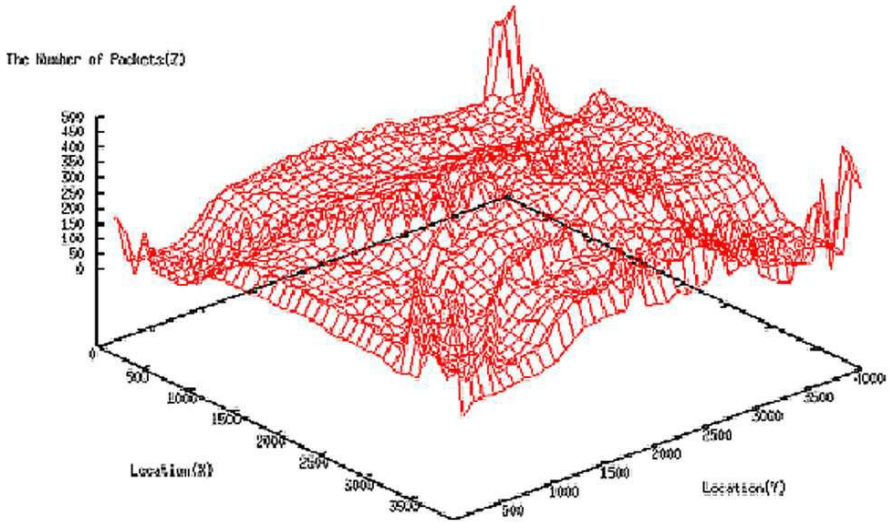
도면4b


The Number of Packets(Z)
500
450
400
350
300
250
200
150
100
50
0
0
500
1000
1500
2000
2500
3000
3500
Location(X)
500
1000
1500
2000
2500
3000
3500
4000
Location(Y)

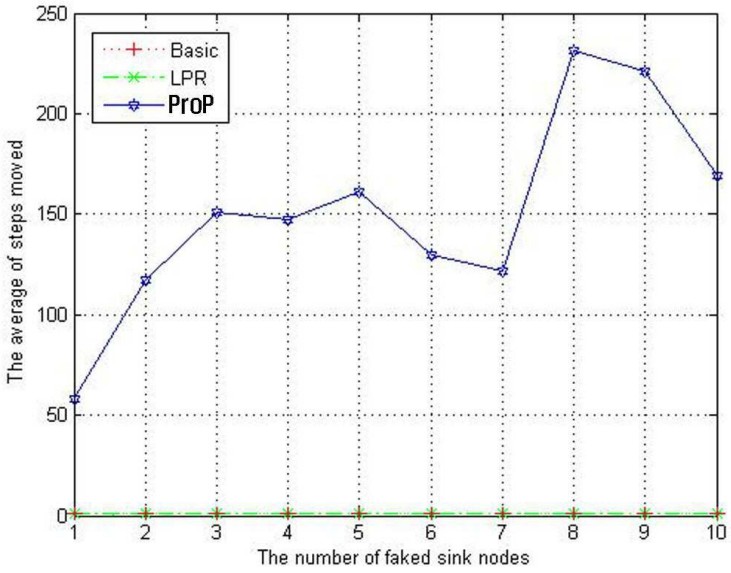
도면5a


The Number of Packets(Z)
300
250
200
150
100
50
0
0
500
1000
1500
2000
2500
3000
3500
4000
Location(X)
500
1000
1500
2000
2500
3000
3500
4000
Location(Y)

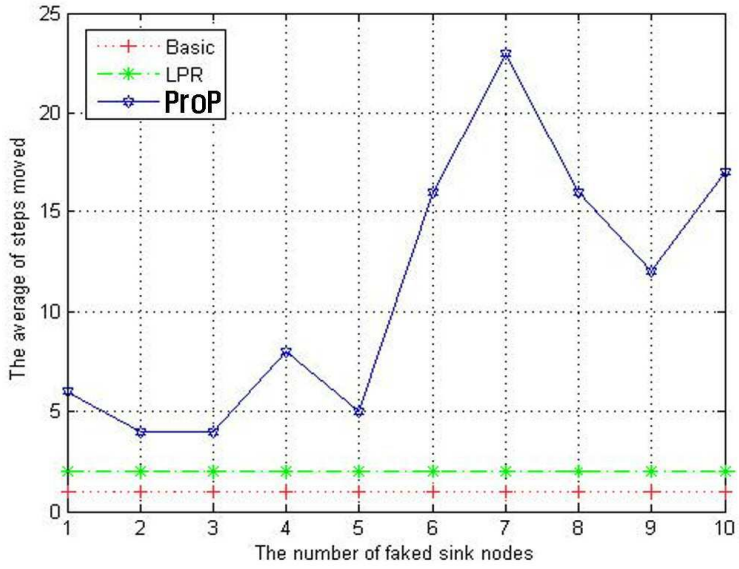
도면5b


The Number of Packets(Z)
Location(X)
Location(Y)

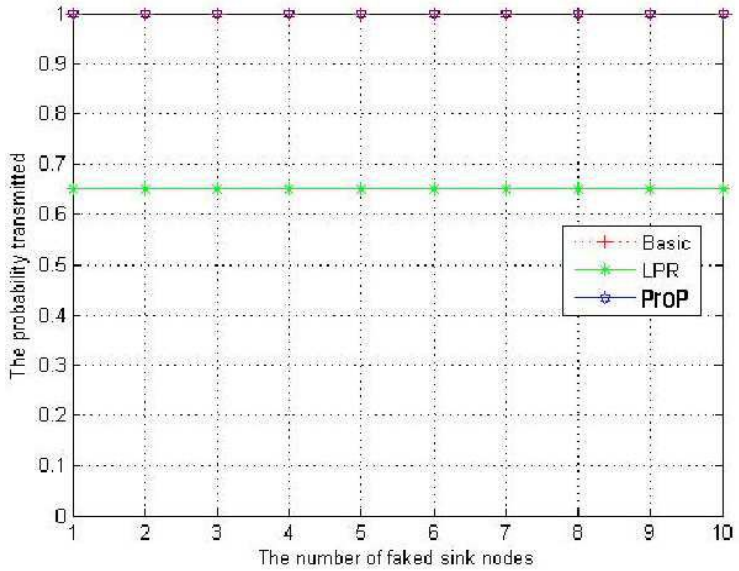
도면6a


Basic
LPR
ProP
The average of steps moved
The number of faked sink nodes
0
50
100
150
200
250
1
2
3
4
5
6
7
8
9
10

도면6b


Basic
LPR
ProP
The average of steps moved
The number of faked sink nodes
0
5
10
15
20
25
1
2
3
4
5
6
7
8
9
10

도면7


Basic
LPR
ProP
The probability transmitted
The number of faked sink nodes
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
1
2
3
4
5
6
7
8
9
10