(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0065640
(43) 공개일자 2009년06월23일

(51) Int. Cl.
H04L 12/28 (2006.01)
(21) 출원번호 10-2007-0133041
(22) 출원일자 2007년12월18일
심사청구일자 2007년12월18일

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 서천동 1 경희대학교 국제캠퍼스내
(72) 발명자
이승룡
경기 성남시 분당구 구미동 250 삼환빌라 102동 102호
이영구
경기 수원시 영통구 영통동 1024-14 경희유니빌 706호
샤키아리아즈 아메드
경기 용인시 기흥구 서천동 1번지 경희대학교 전자정보과
(74) 대리인
김삼수

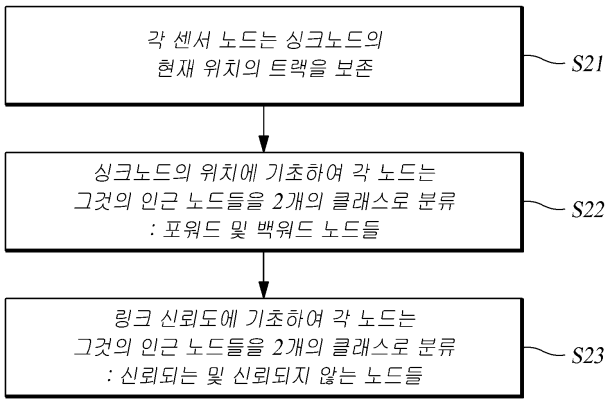
전체 청구항 수 : 총 9 항

(54) 무선 센서 네트워크내의 아이덴티티, 라우트 및 위치익명화 방법

(57) 요 약

본 발명은 무선 센서 네트워크내의 아이덴티티(identity), 라우트(route) 및 위치 익명화(anonymity) 방법에 관한 것이다. 각각의 센서 노드와 싱크 노드간의 패킷 전달은 포워드 방향(forward direction) 및 신뢰(trust)의 개념으로 이루어진다. 이를 위하여, 패킷이 센서 노드들로부터 싱크 노드로 전송될 때, 신뢰될 뿐만 아니라 포워드 방향에 있는 임의로 선택된 센서 노드들이 패킷전송에 관련된다. 본 발명은 도청자(eavesdropper)가 소스 노드의 고유성, 그것의 위치 및 패킷 전달 경로에 관한 완전한 정보에 대한 단서를 얻을 수 없음을 보증한다. 본 발명은 종래의 익명화(anonymity) 기법에 비교해서 무선 센서 네트워크 내에서 보다 적은 에너지 및 메모리를 요구하는 효과를 갖는다.

대 표 도 - 도2



특허청구의 범위

청구항 1

무선 센서 네트워크내의 아이덴티티, 라우트 및 위치 익명화 방법에서 각 센서 노드들에서 실행되는 공통 동작 방법에 있어서,

각 센서 노드들이 싱크 노드의 현 위치의 트랙을 보존하는 단계;

상기 싱크 노드의 현 위치에 기초하여 각 센서 노드의 인접 노드들을 방향에 따라 분류하는 단계;

링크 신뢰도에 기초하여 각 센서 노드의 인접 노드들을 신뢰에 따라 분류하는 단계

를 포함하는 무선 센서 네트워크내의 아이덴티티, 라우트 및 위치 익명화 방법.

청구항 2

제 1항에 있어서, 싱크 노드의 현 위치의 트랙은 GPS 또는 현 지리적인 위치에 대하여 싱크 노드가 보내는 주기적인 업데이트 수신을 통하는 무선 센서 네트워크내의 아이덴티티, 라우트 및 위치 익명화 방법.

청구항 3

무선 센서 네트워크내의 아이덴티티, 라우트 및 위치 익명화 방법에서 패킷이 소스 센서 노드에서 싱크 노드로 전송되는 방법에 있어서,

소스 노드가 싱크 노드로의 패킷 전송을 원하는 제1단계;

포워드 방향 내의 인접 노드들의 리스트 및 신뢰되는 인접 노드들의 리스트를 얻고, 상기 두 리스트의 공통 요소로 이루어진 새로운 리스트를 형성하는 제2단계;

형성된 새로운 리스트가 비어있는지 확인하는 제3단계;

새로운 리스트가 비어있는 경우 백워드 방향 내의 인접 노드들의 리스트를 얻는 제4단계;

백워드 방향 내의 인접 노드들의 리스트와 상기 신뢰되는 인접 노드들의 리스트의 공통 요소로 이루어진 새로운 리스트를 형성하는 제5단계;

상기 형성된 새로운 리스트가 비어있는지 확인하는 제6단계;

상기 새로운 리스트가 비어있는 경우 패킷을 드롭(drop)하는 제7단계;

상기 새로운 리스트가 비어있지 않은 경우 소스 노드가 넥스트-홉을 임의로 선택하고, 패킷을 형성한 후 선택된 넥스트-홉으로 패킷을 전송하는 제8단계

를 포함하는 무선 센서 네트워크내의 아이덴티티, 라우트 및 위치 익명화 방법.

청구항 4

제 3항에 있어서, 상기 제3단계 이후

형성된 새로운 리스트가 비어있지 않은 경우 소스 노드가 넥스트-홉을 임의로 선택하고, 패킷을 형성한 후 선택된 넥스트-홉으로 패킷을 전송하는 무선 센서 네트워크내의 아이덴티티, 라우트 및 위치 익명화 방법.

청구항 5

제 3항에 있어서, 상기 제8단계에서 형성된 패킷은

소스 자신의 라스트-홉의 아이덴티티, 선택된 넥스트-홉의 아이덴티티, 쿼리 id, 액츄얼 데이터, 타임 스탬프 등과 같은 데이터 전송 관련 정보 및 페이로드를 포함하는 무선 센서 네트워크내의 아이덴티티, 라우트 및 위치 익명화 방법.

청구항 6

무선 센서 네트워크내의 아이덴티티, 라우트 및 위치 익명화 방법에서 패킷이 en-route 노드로 수신되고 넥스트

-홉으로 포워드되는 방법에 있어서,

en-route 노드가 패킷을 수신하는 제1단계;

포워드 방향 내의 인접 노드들의 리스트 및 신뢰되는 인접 노드들의 리스트를 얻고, 상기 두 리스트의 공통 요소로 이루어진 새로운 리스트를 형성하는 제2단계;

형성된 새로운 리스트가 비어있는지 확인하는 제3단계;

새로운 리스트가 비어있는 경우 백워드 방향 내의 인접 노드들의 리스트를 얻는 제4단계;

백워드 방향 내의 인접 노드들의 리스트에서 패킷을 수신한 노드의 아이덴티티를 제거하는 제5단계;

패킷을 수신한 노드의 아이덴티티를 제거한 리스트와 신뢰되는 인접 노드들의 리스트의 공통 요소로 이루어진 새로운 리스트를 형성하는 제6단계;

상기 형성된 새로운 리스트가 비어있는지 확인하는 제7단계;

상기 새로운 리스트가 비어있는 경우 패킷을 드롭(drop)하는 제8단계;

상기 새로운 리스트가 비어있지 않은 경우 소스 노드가 넥스트-홉을 임의로 선택하고, 패킷을 넥스트-홉으로 포워드하는 제9단계

를 포함하는 무선 센서 네트워크내의 아이덴티티, 라우트 및 위치 익명화 방법.

청구항 7

제 6항에 있어서, 상기 제9단계에서

소스 노드가 넥스트-홉을 임의로 선택한 후, 패킷에 존재하는 라스트-홉 아이덴티티를 소스 노드 자신의 것으로 교체하고, 넥스트-홉 아이덴티티를 임의로 선택된 아이덴티티로 교체하는 단계를 더 포함하는 무선 센서 네트워크내의 아이덴티티, 라우트 및 위치 익명화 방법.

청구항 8

제 6항에 있어서, 상기 제3단계 이후,

새로운 리스트가 비어있지 않은 경우, 소스 토드가 넥스트-홉을 임의로 선택한 후, 패킷에 존재하는 라스트-홉 아이덴티티를 소스 노드 자신의 것으로 교체하고, 넥스트-홉 아이덴티티를 임의로 선택된 아이덴티티로 교체하여 패킷을 넥스트-홉으로 포워드하는 무선 센서 네트워크내의 아이덴티티, 라우트 및 위치 익명화 방법.

청구항 9

제 6항에 있어서, 상기 제9단계에서

패킷이 전송되는 넥스트-홉은 다른 en-route 노드 또는 싱크 노드가 될 수 있는 무선 센서 네트워크내의 아이덴티티, 라우트 및 위치 익명화 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 도청자(eavesdropper)가 소스 노드의 아이덴티티(identity), 그것의 위치 및 패킷이 전달된 경로에 관한 완전한 정보에 관한 어떤 단서도 얻을 수 없는 것과 같은 방식으로 패킷들이 소스 노드들과 싱크 노드들간에 전달되는 무선 센서 네트워크내에서 아이덴티티(identity), 위치, 라우트 익명을 획득하는 방법에 관한 것이다.

배 경 기 술

<2> 익명화(anonymity)는 프라이버시(privacy)가 얻어지는 방법 중 하나이다. 일반적으로 그것은 프라이버시 보호의 세 가지 타입(라우트 프라이버시, 아이덴티티 프라이버시, 위치 프라이버시)를 제공한다[Bo Zhu, Zhiguo Wan,

Mohan S. Kankanhalli, Feng Bao and Robert H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Network", In proc. of 29th IEEE International Conference on Local Computer Networks(LCN'04), Tampa, USA, 2004, pp. 102-108]. 라우트 프라이버시는 적(adversary)이 캡쳐된 패킷으로부터 소스 또는 목적지를 추적하기 위한 단서를 얻을 수 없는 것을 의미한다. 아이덴티티 프라이버시는 소스 또는 목적지를 제외하고는 누가 누구에게 패킷을 송신하는지에 관한 어떤 정보도 얻을 수 없는 것을 의미한다. 위치 프라이버시는 노드들이 그들 자신을 제외한 다른 노드들에 관한 위치(물리적 거리 또는 홉(hop)들의 수)에 관련된 어떤 정보도 갖지 않음을 의미한다.

<3> 전형적으로, 많은 다양한 익명 기법들은 Onion Routing[Michael G. Reed, Paul F. Syverson, and David M. Goldschlag, "Anonymous Connections and Onion Routing", IEEE Journal on Selected Areas in Communication, vol. 6(4), 1998, pp. 482-494], Hordes[Clay Shield and B. N. Levine, "A Protocol for Anonymous Communication Over the Internet", In proc. of the 7th ACM conference on Computer and communication security, Athens, Greece, Nov 2000, pp. 33-42], Herbivore[Sharad Goel, Mark Robson, Milo Polte, and Emin Gun Sirer, "Herbivore: A Scalable and Efficient Protocol for Anonymous Communication", Cornell University, Computing and information Science Technical Report TR2003-1890, Ithaca, New York, 2003], ARM[Stefaan Seys and Bart Preneel, "ARM:Anonymous Routing Protocol for Mobile Ad hoc Networks", In proc. of the 20th International Conference on Advanced Information Networking and Applications(AINA'06), Vienna Austria, Apr 2006, pp. 33-37] 및 많은 다른 사람들에 의해 제안되었다. 이들 기법에 사용된 가장 공통적인 접근은 커버 트래픽의 사용이다. 커버 트래픽은 다른 목적지들로 원래의 패킷들과 더불어 전송되는 더미 패킷들을 나타낸다. 커버 트래픽 이외에도 어떤 기법들은 가상의 아이덴티티들을 엔티티들로 할당하기 위해 가명들을 사용한다. 커버 트래픽 사용 목적은 공격자가 원래의 패킷 및 그것의 목적지에 관한 단서를 얻지 못하도록 하는 것이다. 이런 종류의 접근은 전형적인 네트워크에 적절하지 않고 많은 양의 트래픽 부하를 야기한다. 또한 이러한 기법은 높은 연산 비용(computational cost)을 요구한다. 이러한 공통 문제는 전형적인 익명 기법들이 높은 리소스 제약 환경 내에서 동작하는 무선 센서 네트워크에 부적절하게 만든다.

<4> 무선 센서 네트워크 도메인에서, 매우 적은 익명 기법들, 예를 들면 C. Ozturk et. al.에 의해 제안된 팬텀 라우팅 기법, ["Source-location privacy in energy-constrained sensor network routing", In proc. of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks, DC, USA, Oct 2004, pp. 88-93], P. Kamat et. al.에 의해 제안된 팬텀 단일 경로 라우팅 ["Enhancing source location privacy in wireless sensor networks", In proc. of 25th IEEE International conference on Distributed Computing Systems, Columbus, Ohio, USA, 2005, pp. 102-108], Satyajayant Misra and Guoliang Xue, SAS 및 CAS는 ["Efficient anonymity schemes for clustered wireless sensor networks", International Journal of Sensor Networks, vol. 1(1/2), 2006, pp. 50-63]들이 제안되었다.

<5> 그러나, 이러한 기법들은 다양한 제한들(예를 들어, 그들은 전혀 아이덴티티, 라우트 및 위치 프라이버시를 제공하지 못하고, 높은 메모리, 에너지 및/또는 연산 능력이 소모된다)로부터 영향받는다.

<6> 팬텀 라우팅 기법에서, 각 메시지는 두 단계로 목적지에 도달한다.

<7> 1) 메시지가 첫 번째 h_{walk} 홉으로 랜덤 방식으로 유니캐스트되는 워킹(walking) 단계

<8> 2) 이후, 메시지는 베이스라인 플러딩(flooding) 기술을 사용하여 플러드된다.

<9> 이 기법은 메모리 효율적이지만, 플러딩(flooding) 단계는 이 기법이 큰 스케일의 센서 네트워크에서 특히 에너지 소비라는 관점에서 비효율적으로 만들 것이다.

<10> 무선 센서 네트워크에 대한 팬텀 단일 경로 라우팅 기법은 워킹(walking) 단계 후에 최단 경로 라우팅 메카니즘과 같은 단일 경로 라우팅 방법을 통해 패킷이 목적지로 포워드되는 것을 제외하고 원래의 팬텀 라우팅 기법과 같은 유사한 방식으로 동작한다. 이 기법은 원래의 팬텀 라우팅과 비교해서 보다 적은 에너지를 소모하고 약간 높은 메모리를 요구한다. 이 기법의 주요 한계는 오직 약한 적 모델(weaker adversary model)에 대해서만 보호를 제공한다는 것이다.

<11> 단일 익명 기법(Simple Anonymity Scheme : SAS) 및 암호화 익명 기법(Cryptographic Anonymity Scheme : CAS)은 오직 무선 센서 네트워크의 집단화(clustering) 환경에서 사용된다. SAS 기법은 통신 중에 진짜 신원(true identity) 대신 동적 가명들을 사용한다. 여기서, 각 센서 노드는 비-인접하는 주어진 가명들을 저장할 필요가 있다. 그러므로, SAS 기법은 메모리 효율적이지 않다. 이와 반면에, CAS 기법은 가명들을 생성하기 위해 암호화

된 해시(hash) 함수를 사용한다. 이 기법은 SAS 기법에 비교해서 메모리 효율적이지만 많은 연산 능력을 요구한다.

발명의 내용

해결 하고자하는 과제

<12> 따라서, 본 발명은 상기 언급된 문제들을 고려해서 만들어진 것으로, 소스 노드가 싱크 노드 또는 베이스 스테이션으로 패킷을 전송하기를 원할 때 소스 노드의 아이덴티티, 라우트 및 소스 노드의 위치 및 생성된 패킷을 지키기 위한 것이 본 발명의 목적이다.

효 과

<13> 본 발명에서의 신뢰와 방향 파라미터들의 결합은 신용, 에너지 효율 및 메모리 효율의 이익을 준다.

발명의 실시를 위한 구체적인 내용

<14> 첫 째로, 우리는 두 개의 key 개념 즉, 우리의 제안된 방법에서 사용되는 방향 및 신뢰를 정의한다.

<15> 우리의 방법에서 사용했던 첫 번째 개념은 방향이다.

<16> 싱크 노드의 물리적인 위치는 각 센서 노드에 대한 참조 포인트이다. 이 참조 포인트에 기초하여 각 노드는 그것의 인접 노드들을 두 개의 카테고리로 분류한다:

<17> 도 1에 도시된 바와 같이, 1) 포워드 인접 노드들 및 2) 백워드 인접 노드들.

<18> 노드 x는 라인 결합 노드 x와 베이스 스테이션 또는 싱크 노드를 고려하여 그것의 인접 노드들을 분류할 수 있다.

<19> 우리의 방법에서 사용했던 두 번째 개념은 신뢰(trust)이다.

<20> 여기서 우리는 인접 노드 움직임의 직접 관측에 기초하여 평가된 링크 신뢰도의 측정치를 신뢰(trust)라고 한다. 직접 관측은 성공적 및 비성공적 인터랙션의 수를 나타내고, 노드의 네트워크, 링크 또는 MAC 레이어와 같은 여러 레어어들에서 수신된 제어 패킷들에 기초하여 연산된다. 그것에 기초하여, 각 노드는 그들의 인접 노드들을 두 개의 카테고리로 분류한다:

<21> 1) 신뢰되는 노드, 2) 신뢰되지 않는 노드.

<22> 각 센서 노드들에서 실행되는 공통 동작은 도 2를 참조하여 설명될 것이다.

<23> 제안된 방법에서, 본 발명에 따르면 각 센서 노드들은 싱크 노드의 현 위치의 트랙을 보존한다(S21). 트랙킹 메카니즘은 GPS 또는 현 지리적인 위치에 대하여 싱크 노드가 보내는 주기적인 업데이트 수신을 통하는 것과 같은 어떤 것도 될 수 있다. 싱크 노드의 현 위치에 기초하여, 각 센서 노드는 그것의 인접 노드들을 두 개의 카테고리로 분류한다:

<24> 1) 포워드 인접 노드들, 2) 백워드 인접 노드들(S22).

<25> 이러한 분류 후에, 링크 신뢰도에 기초하여 각 노드는 그것의 인접 노드들을 두 개의 카테고리로 분류한다:

<26> 1) 신뢰되는, 2) 신뢰되지 않는(S23).

<27> 패킷이 소스 센서 노드에서 싱크 노드로 전송되는 본 발명의 일 실시 예는 도 3을 참조하여 설명될 것이다.

<28> 소스 노드가 싱크 노드로 패킷을 보내는 것을 원할 때(S41), 첫 번째로 포워드 방향내에 있는 그것의 인접 노드들의 리스트를 얻고 나서(S42), 신뢰되는 인접 노드들의 리스트를 얻는다(S43). 그리고, 소스 노드는 S42 및 S44의 공통 요소로 이루어진 새로운 리스트를 형성할 것이다(S44). 만일 이 리스트가 비어있다면(S45), 그것의 백워드 방향 내에 있는 인접 노드들의 또 다른 리스트를 얻을 것이다(S46). 후에 그것은 S46 및 S43의 공통 노드로 이루어진 새로운 리스트를 형성할 것이다. 만일 이 리스트 또한 비어있다면(S48), 노드는 패킷을 드롭(drop)할 것이다(S49). 만일 S45 또는 S48의 리스트가 비어있지 않다면 소스 노드는 넥스트-홉으로 임의로 한 노드를 선택할 것이다(S410). 후에 노드는 라스트-홉(이런 경우 소스 자신)의 아이덴티티, S410에서 선택된 넥스트-홉의 아이덴티티, 쿼리 id, 액츄얼 데이터, 타임 스탬프 등과 같은 데이터 전송에 관련된 정보를 포함하고

페이로드를 포함하는 패킷을 형성할 것이다. 한번 패킷이 형성되면 그것은 넥스트-홉으로 포워드될 것이다(S411).

<29> 패킷이 en-route 노드로 수신되고 다른 en-route 노드 또는 싱크 노드가 될 수 있는 넥스트-홉으로 포워드되는 본 발명의 실시 예는 도 4를 참조하여 설명될 것이다.

<30> en-route 노드가 소스 노드 및 다른 en-route 노드일 수 있는 노드로부터 패킷을 수신하면(S51), 첫 번째로 포워드 방향 내에 있는 그것의 인접 노드들의 목록을 얻고 나서(S52) 신뢰되는 인접 노드들의 리스트를 얻는다(S53). 그런 후에, en-route 노드는 S52 및 S54의 공통 노드로 이루어진 새로운 리스트를 형성한다(S54). 만일 이 리스트가 비어있다면(S55), 그것의 백워드 방향 내에 있는 인접 노드들의 또 다른 목록을 얻을 것이다(S56). 그런 후에, 리스트 S56에서 패킷을 수신한 노드의 아이덴티티를 제거한다(S57).

<31> 그리고나서, en-route 노드는 S57 및 S53의 공통 노드들로 이루어진 새로운 목록을 형성할 것이다(S58). 만일 이 리스트 또한 비어있다면(S59), 노드는 그 패킷을 드롭(drop)할 것이다(S510). 만일 S55 또는 S58에서 리스트가 비어있지 않다면 소스 노드는 넥스트-홉으로 하나의 노드를 임의로 선택할 것이다(S511). 그런 후에, 노드는 라스트-홉 아이덴티티(패킷에 존재하는)를 자신의 것으로 교체하고, 넥스트-홉 아이덴티티를 S511에서 선택된 아이덴티티로 교체하고, 패킷을 넥스트-홉으로 포워드시킬 것이다(S512). 이 프로세스는 패킷이 싱크 노드에 도달할 때까지 계속될 것이다.

<32> 이 알고리즘 내에서 제1의 우선순위는 포워드 방향 내에 있는 신뢰되는 노드들에게 주어진다. 패킷은 오직 포워드 방향 내에 신뢰되는 노드가 없을 때 백워드 방향으로 전환할 것이다.

<33> 노드에 대한 완벽한 위치 프라이버시를 얻는 것은 매우 어렵다. 적어도 그것의 라디오레인지(radio range)내에 있는 인접 노드들은 수신되는 신호 강도(signal strength)와 도래각(angle of arrival)을 측정함으로써 각각의 위치에 쉽게 접근할 수 있다. 만일 적(adversary)이 소스 노드의 영역 내에 있다면, 그는 소스의 위치를 쉽게 추정할 수 있다. 한번 패킷이 원 소스 노드의 라디오레인지를 크로스(cross)했으면, 공격자는 물리적인 거리에 대해서나 원 소스 노드의 홉의 수에 대해서 위치를 추정하는 것은 매우 어렵다.

<34> 이 제안된 방법은, 지리적 라우팅(GR) 기법[B. Karp, H. T. Kung, "GPSR:Greedy perrimeter stateless routing for wireless networks", proceedings of the 6th International conference on Mobile Computing and Networking, NY, USA, 2000, pp.243-254][K. Liu, N. Abu-Ghazaleh, K.D. Kang, "Location verification and trust management for resilient geographic routing", Journal of Parallel and Distributed Computing, vol. 67, 2007, pp. 215-228]뿐 아니라 랜덤 라우팅(RR) 기법[C. Karlof, Y. Li, J. Polastre, "ARRIVE: Algorithm for robust routing in volatile environment", Technical Report UCB//CSD-02-1233, Computer Science Division, University of California, 2003][J. Deng, R. Han, S. Nishra, "Countermeasures against traffic analysis attacks in wireless sensor networks", Technical Report CU-CS-987-04, Comp. Sci. Dept, university of Colorado, Boulder, 2004]의 패밀리에도 속한다.

<35> 일반적으로, RR 기법은 라우트 익명을 제공하지만 딜레이를 초래하고, 이에 반하여 GR 기법은 적시성(timeliness)을 제공하지만 라우트 익명을 보호하지 못한다. 그래서 우리의 제안된 방법 내에서 방향과 같은 특성들과 무작위성(randomness)의 결합은 적시성뿐 아니라 라우트 익명의 이득을 준다.

도면의 간단한 설명

<36> 도 1은 포워드 인접 노드들 및 백워드 인접 노드들의 개념을 나타내는 도면이다.

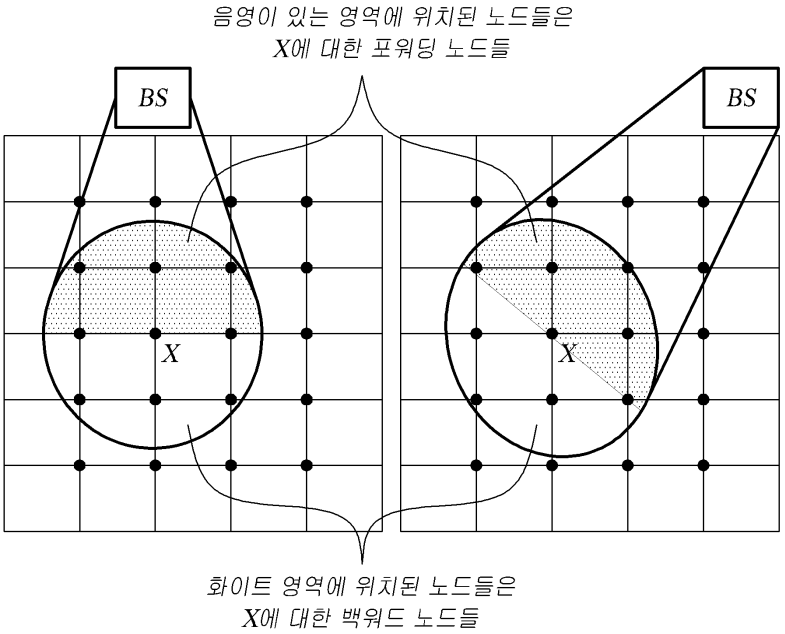
<37> 도 2는 본 발명의 제1실시 예에 따른 각 센서 노드에 실행되는 공통 동작들을 나타내는 도면이다.

<38> 도 3은 본 발명의 제2실시 예에 따른 소스 센서 노드에서의 동작을 나타내는 순서도이다.

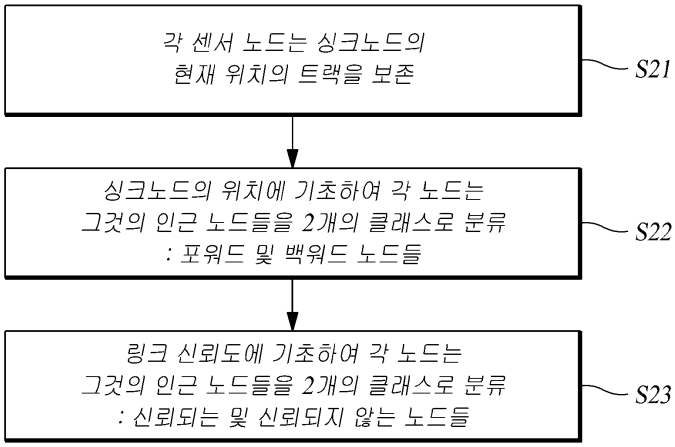
<39> 도 4는 본 발명의 제3실시 예에 따른 en-route 센서 노드에서의 동작을 나타내는 순서도이다.

도면

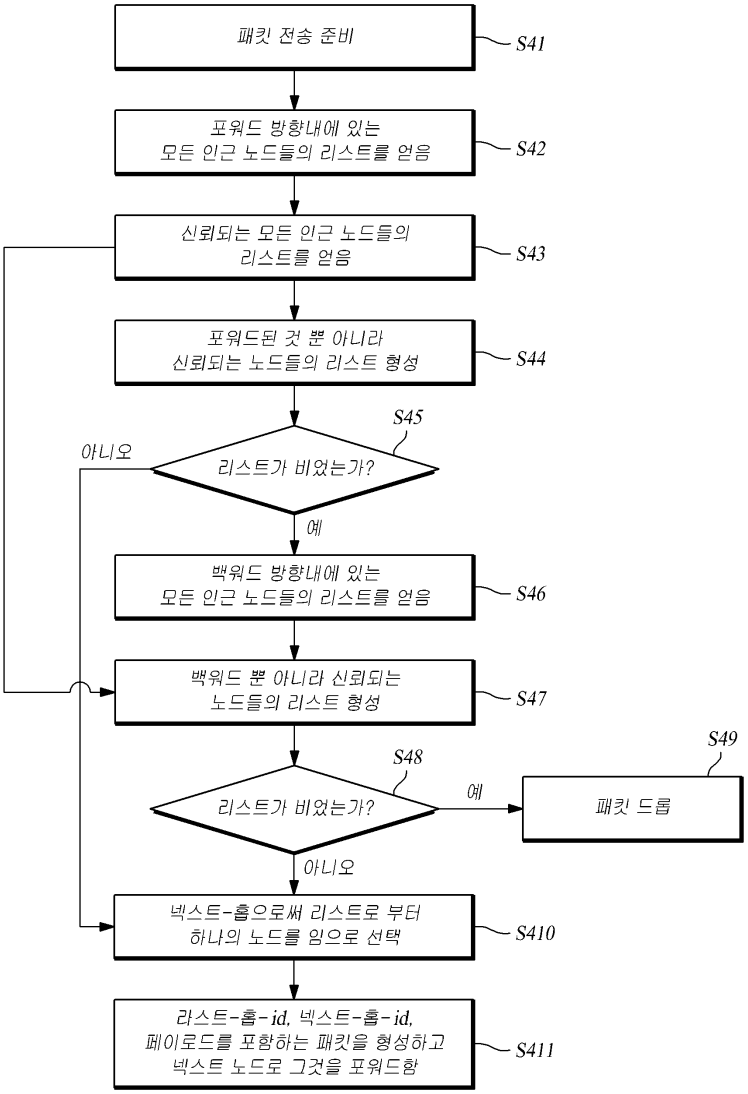
도면1


음영이 있는 영역에 위치된 노드들은
X에 대한 포워딩 노드들
BS
BS
X
X
화이트 영역에 위치된 노드들은
X에 대한 백워드 노드들

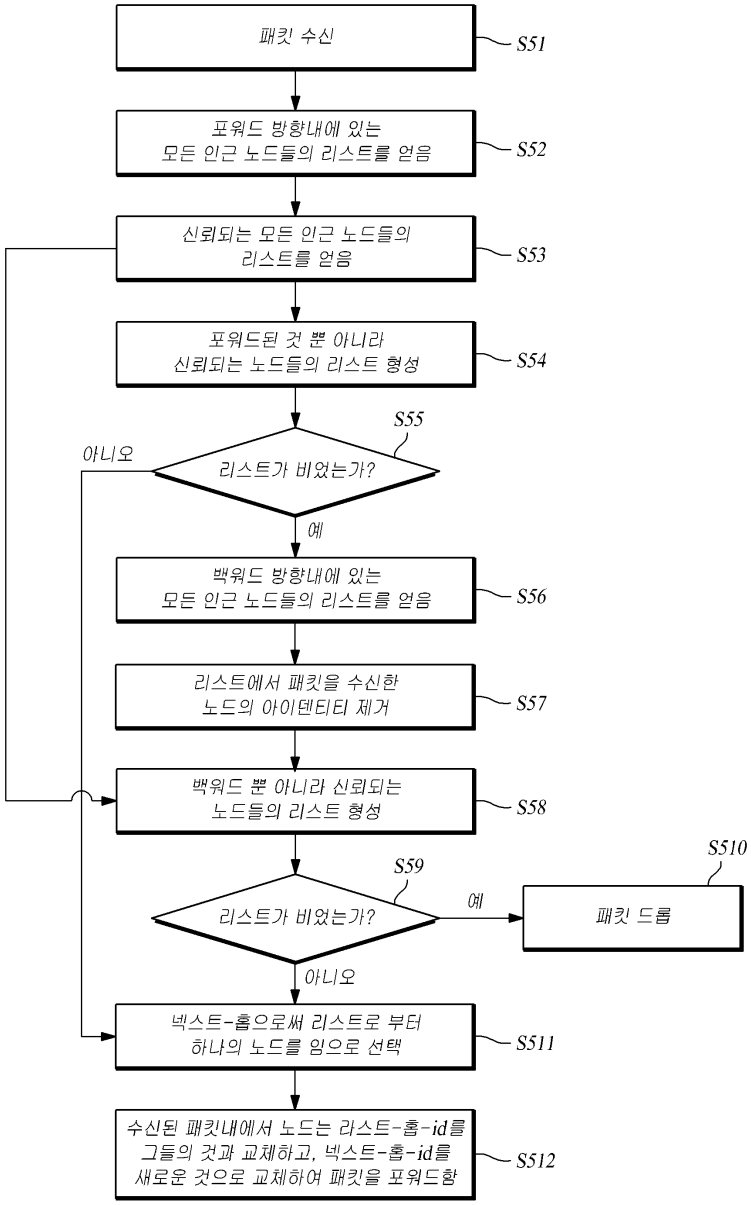
도면2


각 센서 노드는 싱크노드의
현재 위치의 트랙을 보존
S21
싱크노드의 위치에 기초하여 각 노드는
그것의 인근 노드들을 2개의 클래스로 분류
: 포워드 및 백워드 노드들
S22
링크 신뢰도에 기초하여 각 노드는
그것의 인근 노드들을 2개의 클래스로 분류
: 신뢰되는 및 신뢰되지 않는 노드들
S23

도면3


패킷 전송 준비
S41
포워드 방향내에 있는
모든 인근 노드들의 리스트를 얻음
S42
신뢰되는 모든 인근 노드들의
리스트를 얻음
S43
포워드된 것 뿐 아니라
신뢰되는 노드들의 리스트 형성
S44
S45
리스트가 비었는가?
아니오
예
백워드 방향내에 있는
모든 인근 노드들의 리스트를 얻음
S46
백워드 뿐 아니라 신뢰되는
노드들의 리스트 형성
S47
S48
리스트가 비었는가?
예
S49
패킷 드롭
아니오
넥스트-홉으로써 리스트로 부터
하나의 노드를 임으로 선택
S410
라스트-홉-id, 넥스트-홉-id,
페이로드를 포함하는 패킷을 형성하고
넥스트 노드로 그것을 포워드함
S411

도면4


패킷 수신
S51
포워드 방향내에 있는
모든 인근 노드들의 리스트를 얻음
S52
신뢰되는 모든 인근 노드들의
리스트를 얻음
S53
포워드된 것 뿐 아니라
신뢰되는 노드들의 리스트 형성
S54
S55
리스트가 비었는가?
아니오
예
백워드 방향내에 있는
모든 인근 노드들의 리스트를 얻음
S56
리스트에서 패킷을 수신한
노드의 아이덴티티 제거
S57
백워드 뿐 아니라 신뢰되는
노드들의 리스트 형성
S58
S59
리스트가 비었는가?
예
S510
패킷 드롭
아니오
넥스트-홉으로써 리스트로 부터
하나의 노드를 임으로 선택
S511
수신된 패킷내에서 노드는 라스트-홉-id를
그들의 것과 교체하고, 넥스트-홉-id를
새로운 것으로 교체하여 패킷을 포워드함
S512