



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0002422
(43) 공개일자 2010년01월07일

(51) Int. Cl.

H04L 12/28 (2006.01)

(21) 출원번호 10-2008-0062317

(22) 출원일자 2008년06월30일

심사청구일자 2008년06월30일

(71) 출원인

경희대학교 산학협력단

경기도 용인시 기흥구 서천동 1 경희대학교 국제 캠퍼스내

(72) 발명자

홍충선

경기 용인시 수지구 상현동 성원3차상떼빌아파트 233-101

최병구

서울특별시 용산구 보광동 228-68

(뒷면에 계속)

(74) 대리인

서재승

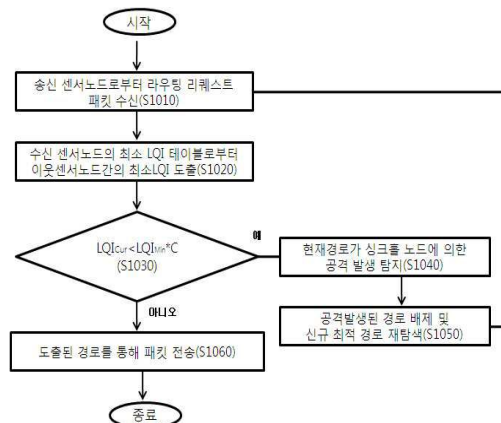
전체 청구항 수 : 총 10 항

(54) 공격 탐지 가능 무선 센서 네트워크 시스템 및 무선 센서네트워크에서 링크 품질 지표 기반 라우팅에 대한 공격탐지 방법

(57) 요약

본 발명은 공격 탐지 가능 무선 센서 네트워크 시스템 및 이를 이용한 무선 센서 네트워크에서 링크 품질 지표 기반 라우팅에 대한 공격 탐지 방법에 관한 것으로, 각 센서 노드별 및 각 탐지 노드별로 이웃 센서 노드들간의 최소 링크 품질 지표(LQI)값을 저장하는 단계와, 각 탐지 노드별로 주변 탐지 노드들간의 최적 경로에 대한 경로 비용을 저장하는 단계와, 임의의 수신 센서 노드가 임의의 송신 센서 노드로부터 라우팅 리퀘스트 패킷을 수신하는 단계와, 수신 센서 노드에 저장된 최소 링크 품질 지표값(LQI_{Min})과 송신 센서 노드로부터 수신된 라우팅 리퀘스트 패킷의 최소 링크 품질 지표값(LQI_{Cur})을 비교하는 단계 및 비교 결과에 따라 싱크홀 노드에 의한 공격 발생 여부를 탐지하는 단계를 포함하는 방법과 공격 탐지 가능 무선 센서 네트워크 시스템이 제공된다.

대표도 - 도10



(72) 발명자

김대선

서울 동대문구 휘경2동 65-4 동도빌라 나동 102호

김진호

경기도 고양시 일산동구 풍동 에이스아파트
101-510

특허청구의 범위

청구항 1

다수의 센서 노드와, 다수의 탐지 노드 및 베이스 스테이션을 포함하는 무선 센서 네트워크에서 링크 품질 지표 기반 라우팅에 대한 공격 탐지 방법으로서,

각 센서 노드별 및 각 탐지 노드별로 이웃 센서 노드들간의 최소 링크 품질 지표(LQI)값을 저장하는 단계; 및
각 탐지 노드별로 주변 탐지 노드들간의 최적 경로에 대한 경로 비용을 저장하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 2

제1항에 있어서, 상기 방법은

임의의 수신 센서 노드가 임의의 송신 센서 노드로부터 라우팅 리퀘스트 패킷을 수신하는 단계;

상기 수신 센서 노드에 저장된 최소 링크 품질 지표값(LQI_{Min})과 상기 송신 센서 노드로부터 수신된 라우팅 리퀘스트 패킷의 최소 링크 품질 지표값(LQI_{Cur})을 비교하는 단계; 및

상기 비교 결과에 따라 싱크홀 노드에 의한 공격 발생 여부를 탐지하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 3

제2항에 있어서,

상기 비교하는 단계는 이하의 식이 성립하는지 여부를 판단하며,

$$LQI_{Cur} < LQI_{Min} \times C \quad (C \text{는 허용 오차율}),$$

상기 탐지하는 단계는 상기 식이 성립하는 경우에, 상기 무선 센서 네트워크 내의 패킷 전송 경로에 싱크홀 노드에 의한 공격이 발생한 것으로 판단하는 것을 특징으로 하는 방법.

청구항 4

제1항에 있어서, 상기 방법은,

상기 탐지 노드들은 전파 범위 내의 상기 이웃 센서 노드들의 라우팅 리퀘스트 패킷을 수집하는 단계;

탐지 노드가 수집한 특정 센서 노드에서 전송한 라우팅 리퀘스트 패킷 내의 누적 링크 품질 지표값의 증가분을 도출하는 단계;

상기 특정 센서 노드간의 최적 경로 비용을 도출하는 단계;

상기 누적 링크 품질 지표값의 증가분과 상기 최적 경로 비용을 비교하는 단계; 및

상기 비교 결과에 따라 싱크홀 노드에 의한 공격 발생 여부를 탐지하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 5

제4항에 있어서,

상기 비교하는 단계는 이하의 식이 성립하는지 여부를 판단하며,

$$CLQI_B - CLQI_A < OLC_{CD} - (LQI_{AC} + LQI_{BD})$$

상기 탐지하는 단계는 상기 식이 성립하는 경우에, 상기 무선 센서 네트워크 내의 패킷 전송 경로에 싱크홀 노드에 의한 공격이 발생한 것으로 판단하며,

상기 CLQI는 탐지 노드가 수집한 특정 센서 노드에서 전송한 라우팅 리퀘스트 패킷 내의 누적 링크 품질 지표값

이며, 상기 OLC는 두 노드간의 최적 경로 비용이며, LQI는 두 이웃 노드간의 링크 품질 지표값이며, 상기 A 및 B는 특정 센서 노드이며, 상기 C 및 D는 탐지 노드인 것을 특징으로 하는 방법.

청구항 6

제1항에 있어서, 상기 방법은,

임의의 수신 센서 노드가 임의의 송신 센서 노드로부터 라우팅 리퀘스트 패킷을 수신하는 단계;

상기 수신 센서 노드에 저장된 최소 링크 품질 지표값(LQI_{min})과 상기 송신 센서 노드로부터 수신된 라우팅 리퀘스트 패킷의 최소 링크 품질 지표값(LQI_{cur})을 비교하는 단계;

상기 비교 결과에 따라 싱크홀 노드에 의한 공격 발생 여부를 탐지하는 단계;

상기 탐지 노드들은 전파 범위 내의 상기 이웃 센서 노드들의 라우팅 리퀘스트 패킷을 수집하는 단계;

탐지 노드가 수집한 특정 센서 노드에서 전송한 라우팅 리퀘스트 패킷 내의 누적 링크 품질 지표값의 증가분을 도출하는 단계;

상기 특정 센서 노드간의 최적 경로 비용을 도출하는 단계;

상기 누적 링크 품질 지표값의 증가분과 상기 최적 경로 비용을 비교하는 단계; 및

상기 비교 결과에 따라 싱크홀 노드에 의한 공격 발생 여부를 탐지하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 7

제2항 내지 제6항 중 어느 한 항에 있어서, 상기 방법은,

상기 공격 발생된 패킷 전송 경로를 배제한 후, 신규 최적 경로를 재탐색하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 8

제1항에 있어서,

상기 최소 링크 품질 지표(LQI)값을 저장하는 단계는,

각 센서 노드와 이웃 센서 노드 간의 링크 품질 지표값을 계산하고, 각 탐지 노드와 이웃 센서 노드 간의 링크 품질 지표값을 계산하는 단계;

상기 각 센서 노드와 상기 이웃 센서 노드 간의 최소 링크 품질 지표값을 도출하고, 상기 각 탐지 노드와 상기 이웃 센서 노드 간의 최소 링크 품질 지표값을 도출하는 단계; 및

상기 각 센서 노드별 및 각 탐지 노드별로 이웃 센서 노드들간의 최소 링크 품질 지표(LQI)값을 테이블로 구성하는 단계를 포함하며,

상기 최적 경로에 대한 경로 비용을 저장하는 단계는,

상기 각 탐지 노드가 주변 탐지 노드를 탐색하는 단계;

탐지 노드들 간의 최적 경로를 도출하고, 상기 최적 경로에 대한 경로 비용을 도출하는 단계; 및

상기 각 탐지 노드별로 주변 탐지노드 간의 경로 비용을 테이블로 구성하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 9

공격 탐지 가능 무선 센서 네트워크 시스템에 있어서,

다수의 센서 노드;

다수의 탐지 노드; 및

상기 다수의 센서 노드 및 다수의 탐지 노드를 제어하며, 상기 다수의 센서 노드가 센싱한 데이터를 수집하는 베이스 스테이션을 포함하며,

상기 각 센서 및 탐지 노드는 이웃 센서 노드들 간의 최소 링크 품질 지표값에 대한 데이터를 포함하며,

상기 각 탐지 노드는 주변 탐지 노드들간의 최적 경로에 대한 경로 비용에 대한 데이터를 포함하는 것을 특징으로 하는 공격 탐지 가능 무선 센서 네트워크 시스템.

청구항 10

제9항에 있어서,

상기 최소 링크 품질 지표값에 대한 데이터 및 상기 탐지 노드들간의 최적 경로에 대한 경로 비용 중 적어도 어느 하나를 이용하여 싱크홀 노드에 의한 공격 발생 여부를 탐지하는 것을 특징으로 하는 공격 탐지 가능 무선 센서 네트워크 시스템.

명세서

발명의 상세한 설명

기술 분야

- <1> 본 발명은 공격 탐지 가능 무선 센서 네트워크 시스템 및 이를 이용한 무선 센서 네트워크에서 링크 품질 지표 기반 라우팅에 대한 공격 탐지 방법에 관한 것으로, 보다 상세하게는 링크 품질 지표에 기반한 라우팅을 수행하는 무선 센서 네트워크에서 안전한 데이터 전송을 위해 싱크홀 공격을 탐지할 수 있는 공격 탐지 가능 무선 센서 네트워크 시스템 및 이를 이용한 무선 센서 네트워크에서 링크 품질 지표 기반 라우팅에 대한 공격 탐지 방법에 관한 것이다.

배경 기술

- <2> 무선 센서 네트워크는 미래의 유비쿼터스 환경에 기반이 될 중요한 기술 중의 하나이다. 무선 센서 네트워크는 저비용으로 데이터의 수집 및 측정에 폭넓게 이용될 수 있다. 그러나 무선 센서 네트워크는 무선 통신의 특성과 제한된 성능 및 자원으로 여러 가지 공격에 노출되어 있다. 특히 라우팅 프로토콜의 경우 공격에 노출되면 네트워크의 혼란이 발생되어 서비스 불능 상태가 될 수 있다. 하지만 유선 네트워크에서 사용되는 방어 기법들은 제한된 처리능력과 자원을 갖는 무선 센서 네트워크에서는 사용하기 어렵다.
- <3> 무선 센서 네트워크에서 라우팅 공격의 대표적인 형태중의 하나는 싱크홀 공격이다. 이 공격은 악의적인 노드가 자신을 베이스 스테이션(Base Station)이나 목적지 노드에 더 가까이 있다고 거짓 광고한다. 그 결과 많은 노드들이 전송 데이터를 악의적인 노드를 경유해서 보내게 된다. 따라서, 악의적인 노드는 자신을 거치는 네트워크의 트래픽들을 조절할 수 있게 된다. 그러므로, 싱크홀 공격의 탐지는 안전한 무선 센서 네트워크를 구성하기 위한 중요한 연구 분야이다.
- <4> 도 1에는 무선 센서 네트워크 내에서 싱크홀 공격이 발생한 상태가 도시된다. 이는 웜홀을 비롯한 다양한 형태의 공격으로 발전하기 쉽다.
- <5> 종래 기술에 따른 싱크홀 공격 탐지 방법은 홉카운트에 기반한 라우팅을 바탕으로 한다. 이러한 홉카운트 기반 라우팅에 대한 싱크홀 공격 탐지 방법은 모든 센서 노드들이 주기적으로 베이스 스테이션으로 데이터를 전송하는 환경을 가정한다.
- <6> 싱크홀 공격이 이루어질 경우, 싱크홀 노드가 취할 수 있는 대표적인 공격 방법은 선택적 포워딩(Selective Forwarding)이다. 이러한 선택적 포워딩은 악의적인 노드가 자신을 경유하는 패킷들의 일부를 전달하지 않으므로써 고의적으로 패킷을 손실시키는 공격이다. 이런 공격이 발생할 경우, 베이스 스테이션은 특정 주기에 데이터를 보고받지 못한 노드들의 목록을 작성할 수 있다. 이 노드들이 위치한 지역의 모든 노드들로부터 넥스트-홉(Next-hop) 정보를 모으고 이를 기반으로 네트워크 구조를 재구성한다.
- <7> 도 2는 종래 기술에 따른 홉카운트를 이용한 싱크홀 공격 탐지 방법을 도시한 도이다. 도 2를 참조하면, 트리 라우팅을 수행하는 네트워크에서 최상위에 위치한 노드가 싱크홀 공격 노드임을 추측할 수 있다.
- <8> 그러나, 이러한 공격 탐지 기법의 경우, 공격 노드가 싱크홀 공격 이외에 베이스 스테이션이 인지 가능한 공격

(예를 들면, 선택티브 포워딩 등)을 해야만 탐지과정을 수행한다는 단점이 있다. 즉, 싱크홀 공격과 동시에 이루어지는 공격에 대한 탐지 방법이 없다면 싱크홀 공격 여부를 판단할 기준이 모호해진다. 또한, 홉카운트에 기반을 둔 트리 라우팅 방식에 대해서만 적용하였으며 링크 품질 지표에 따른 메쉬 라우팅 방식에서는 적용할 수 없다. 더욱이, 공격이 발생하고 그것이 탐지되기 전까지는 센서 노드들은 공격에 그대로 노출되는 문제점이 있었다.

발명의 내용

해결 하고자하는 과제

- <9> 본 발명은 상술한 종래의 문제점을 극복하기 위한 것으로서, 본 발명이 해결하고자 하는 과제는 보다 상세하게는 링크 품질 지표 기반 라우팅에도 적용할 수 있으며, 싱크홀 공격을 시도하는 과정 중에 싱크홀 공격을 탐지할 수 있는 공격 탐지 가능 무선 센서 네트워크 시스템 및 이를 이용한 무선 센서 네트워크에서 링크 품질 지표 기반 라우팅에 대한 공격 탐지 방법을 제공하기 위한 것이다.

과제 해결수단

- <10> 본 발명의 예시적인 실시예에 따르면, 다수의 센서 노드와, 다수의 탐지 노드 및 베이스 스테이션을 포함하는 무선 센서 네트워크에서 링크 품질 지표 기반 라우팅에 대한 공격 탐지 방법으로서, 각 센서 노드별 및 각 탐지 노드별로 이웃 센서 노드들간의 최소 링크 품질 지표(LQI)값을 저장하는 단계; 및 각 탐지 노드별로 주변 탐지 노드들간의 최적 경로에 대한 경로 비용을 저장하는 단계를 포함하는 방법이 제공된다.
- <11> 상기 방법은 임의의 수신 센서 노드가 임의의 송신 센서 노드로부터 라우팅 리퀘스트 패킷을 수신하는 단계; 상기 수신 센서 노드에 저장된 최소 링크 품질 지표값(LQI_{Min})과 상기 송신 센서 노드로부터 수신된 라우팅 리퀘스트 패킷의 최소 링크 품질 지표값(LQI_{Cur})을 비교하는 단계; 및 상기 비교 결과에 따라 싱크홀 노드에 의한 공격 발생 여부를 탐지하는 단계를 더 포함한다.
- <12> 상기 비교하는 단계는 이하의 식이 성립하는지 여부를 판단하며, $LQI_{Cur} < LQI_{Min} \times C$ (C는 허용 오차율), 상기 탐지하는 단계는 상기 식이 성립하는 경우에, 상기 무선 센서 네트워크 내의 패킷 전송 경로에 싱크홀 노드에 의한 공격이 발생한 것으로 판단하는 것을 특징으로 한다.
- <13> 상기 방법은 상기 탐지 노드들은 전파 범위 내의 상기 이웃 센서 노드들의 라우팅 리퀘스트 패킷을 수집하는 단계; 탐지 노드가 수집한 특정 센서 노드에서 전송한 라우팅 리퀘스트 패킷 내의 누적 링크 품질 지표값의 증가분을 도출하는 단계; 상기 특정 센서 노드간의 최적 경로 비용을 도출하는 단계; 상기 누적 링크 품질 지표값의 증가분과 상기 최적 경로 비용을 비교하는 단계; 및 상기 비교 결과에 따라 싱크홀 노드에 의한 공격 발생 여부를 탐지하는 단계를 더 포함한다.
- <14> 상기 비교하는 단계는 이하의 식이 성립하는지 여부를 판단하며,
- <15> $CLQI_B - CLQI_A < OLC_{CD} - (LQI_{AC} + LQI_{BD})$, 상기 탐지하는 단계는 상기 식이 성립하는 경우에, 상기 무선 센서 네트워크 내의 패킷 전송 경로에 싱크홀 노드에 의한 공격이 발생한 것으로 판단하며, 상기 CLQI는 탐지 노드가 수집한 특정 센서 노드에서 전송한 라우팅 리퀘스트 패킷 내의 누적 링크 품질 지표값이며, 상기 OLC는 두 노드간의 최적 경로 비용이며, LQI는 두 이웃 노드간의 링크 품질 지표값이며, 상기 A 및 B는 특정 센서 노드이며, 상기 C 및 D는 탐지 노드인 것을 특징으로 한다.
- <16> 상기 방법은 임의의 수신 센서 노드가 임의의 송신 센서 노드로부터 라우팅 리퀘스트 패킷을 수신하는 단계; 상기 수신 센서 노드에 저장된 최소 링크 품질 지표값(LQI_{Min})과 상기 송신 센서 노드로부터 수신된 라우팅 리퀘스트 패킷의 최소 링크 품질 지표값(LQI_{Cur})을 비교하는 단계; 상기 비교 결과에 따라 싱크홀 노드에 의한 공격 발생 여부를 탐지하는 단계; 상기 탐지 노드들은 전파 범위 내의 상기 이웃 센서 노드들의 라우팅 리퀘스트 패킷을 수집하는 단계; 탐지 노드가 수집한 특정 센서 노드에서 전송한 라우팅 리퀘스트 패킷 내의 누적 링크 품질 지표값의 증가분을 도출하는 단계; 상기 특정 센서 노드간의 최적 경로 비용을 도출하는 단계; 상기 누적 링크 품질 지표값의 증가분과 상기 최적 경로 비용을 비교하는 단계; 및 상기 비교 결과에 따라 싱크홀 노드에 의한 공격 발생 여부를 탐지하는 단계를 더 포함한다.
- <17> 상기 방법은 상기 공격 발생된 패킷 전송 경로를 배제한 후, 신규 최적 경로를 재탐색하는 단계를 더 포함한다.

- <18> 상기 최소 링크 품질 지표(LQI)값을 저장하는 단계는 각 센서 노드와 이웃 센서 노드 간의 링크 품질 지표값을 계산하고, 각 탐지 노드와 이웃 센서 노드 간의 링크 품질 지표값을 계산하는 단계; 상기 각 센서 노드와 상기 이웃 센서 노드 간의 최소 링크 품질 지표값을 도출하고, 상기 각 탐지 노드와 상기 이웃 센서 노드 간의 최소 링크 품질 지표값을 도출하는 단계; 및 상기 각 센서 노드별 및 각 탐지 노드별로 이웃 센서 노드들간의 최소 링크 품질 지표(LQI)값을 테이블로 구성하는 단계를 포함하며, 상기 최적 경로에 대한 경로 비용을 저장하는 단계는 상기 각 탐지 노드가 주변 탐지 노드를 탐색하는 단계; 탐지 노드들 간의 최적 경로를 도출하고, 상기 최적 경로에 대한 경로 비용을 도출하는 단계; 및 상기 각 탐지 노드별로 주변 탐지노드 간의 경로 비용을 테이블로 구성하는 단계를 포함한다.
- <19> 본 발명의 다른 실시예에 따르면, 다수의 센서 노드; 다수의 탐지 노드; 및 상기 다수의 센서 노드 및 다수의 탐지 노드를 제어하며, 상기 다수의 센서 노드가 센싱한 데이터를 수집하는 베이스 스테이션을 포함하며, 상기 각 센서 및 탐지 노드는 이웃 센서 노드들 간의 최소 링크 품질 지표값에 대한 데이터를 포함하며, 상기 각 탐지 노드는 주변 탐지 노드들간의 최적 경로에 대한 경로 비용에 대한 데이터를 포함하는 공격 탐지 가능 무선 센서 네트워크 시스템이 제공된다.
- <20> 상기 최소 링크 품질 지표값에 대한 데이터 및 상기 탐지 노드들간의 최적 경로에 대한 경로 비용 중 적어도 어느 하나를 이용하여 싱크홀 노드에 의한 공격 발생 여부를 탐지하는 것을 특징으로 한다.

효 과

- <21> 본 발명에서와 같이, 싱크홀이 발생한 후 탐지를 하는 기존의 탐지 기법과는 다르게 싱크홀 공격을 시도하는 과정에서 공격을 탐지할 수 있는 효과를 얻을 수 있다.
- <22> 또한, 종래 기술에 따른 탐지 방법과는 달리 싱크홀 공격만 발생하는 경우에도 싱크홀 공격을 탐지할 수 있게 된다.

발명의 실시를 위한 구체적인 내용

- <23> 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 대해 상세히 설명한다.
- <24> 도 3은 본 발명에 따른 방법 중 네트워크 초기 설정 과정에서 임의의 센서 노드와 이웃 센서 노드들간의 최소 링크 품질 지표값 테이블의 구성예이다.
- <25> 도 3에 도시된 바와 같이, 네트워크 초기 설정 과정에서는 각 센서 노드들은 이웃 센서 노드들과의 링크 품질 지표(LQI: Link Quality Indicator) 값을 계산한다.
- <26> 각 센서 노드들은 발신 가능한 범위 내에서 최대 신호를 이웃 센서 노드에게 보내고, 이러한 신호를 수신한 수신 센서 노드는 송신 센서 노드와의 링크 품질 지표를 계산하여 기록한다. 이 과정을 반복하면 각 센서 노드들은 주변 센서 노드들로부터의 최소 링크 품질 지표값을 도출할 수 있다.
- <27> 도출된 최소 LQI값에 따라 이웃 센서들 간의 최소 링크 품질 지표값 테이블을 구성한다. 도 3에는 A 센서 노드와 이웃 센서들간의 최소 링크 품질 지표값 테이블이 도시되어 있다. 센서 노드 AB간 최소 링크 품질 지표값은 34, 센서 노드 AC간 최소 링크 품질 지표값은 78, 센서 노드 AD간 최소 링크 품질 지표값은 33, 센서 노드 AE간 최소 링크 품질 지표값은 75이며, 센서 노드AF간 최소 링크 품질 지표값은 50이다.
- <28> 이러한 이웃 센서들 간의 최소 링크 품질 지표값 테이블은 상대노드가 인위적으로 매우 강한 신호를 보냄으로써, 링크 품질 지표값을 낮추어 라우팅 경로를 변경하려는 공격을 탐지하는데 사용된다.
- <29> 도 4는 본 발명에 따른 방법 중 네트워크 초기 설정 과정에서 탐지 노드들간의 최적 경로 및 최적 경로에 대한 경로 비용 테이블의 구성예이다.
- <30> 탐지 노드의 경우에는 도 3에 도시된 과정 즉, 탐지 노드와 이웃 센서 노드간의 최소 링크 품질 지표값 테이블을 구성하는 과정 이외에, 다음의 과정이 추가된다.
- <31> 탐지 노드는 주변의 탐지 노드들을 탐색하고, 탐지 노드들간의 최적 경로와 이러한 최적 경로에 대한 경로 비용(즉, 누적 LQI)을 기록한다. 도 4에는 탐지 노드들간의 최소 경로 비용 테이블이 도시되어 있다. 탐지노드 D_A와 D_B간 경로 비용은 102, 탐지노드 D_A와 D_C간 경로 비용은 70이며, 탐지노드 D_B와 D_A간 경로 비용은 102, 탐지노드 D_B와 D_C간 경로 비용은 80이며, 탐지노드 D_C와 D_A간 경로 비용은 70, 탐지노드 D_C와 D_B간 경로 비용은 80이다.

- <32> 도 5는 각 센서 노드와 이웃 센서 노드들간의 최소 링크 품질 지표(LQI)값 테이블을 구성하는 과정을 도시한 흐름도이며, 도 6은 각 탐지 노드별로 주변 탐지 노드들간의 최적 경로에 대한 경로 비용 테이블을 구성하는 과정을 도시한 흐름도이다.
- <33> 도 5를 참조하여, 각 센서 노드별 및 각 탐지 노드별로 이웃 센서 노드들간의 최소 링크 품질 지표(LQI)값을 저장하는 과정을 살펴본다.
- <34> 우선, 각 센서 노드와 이웃 센서 노드 간의 링크 품질 지표값을 계산하는 과정을 수행한다(S510). 그 다음에, S510과정을 반복하면서, 각 센서 노드와 이웃 센서 노드 간의 최소 링크 품질 지표값을 도출하는 과정을 수행한다(S520).
- <35> 그리고 나서, 각 센서 노드별로 이웃 센서 노드들간의 최소 링크 품질 지표(LQI)값을 테이블로 구성하는 과정을 수행한다(S530).
- <36> 도 6을 참조하여, 각 탐지 노드별로 주변 탐지 노드들간의 최적 경로에 대한 경로 비용을 저장하는 과정을 살펴본다.
- <37> 우선, 각 탐지 노드와 이웃 센서 노드 간의 링크 품질 지표값을 계산하는 과정을 수행한다(S610). 그 다음에, S610과정을 반복하면서, 각 탐지 노드와 이웃 센서 노드 간의 최소 링크 품질 지표값을 도출하는 과정을 수행한다(S620). 각 탐지 노드별로 이웃 센서 노드들간의 최소 링크 품질 지표(LQI)값을 테이블로 구성하는 과정을 수행한다(S630).
- <38> 그리고 나서, 각 탐지 노드는 주변 탐지 노드를 탐색하는 과정을 수행한다(S640). 탐지 노드들 간의 최적 경로를 도출하고, 최적 경로에 대한 경로 비용을 도출하는 과정을 수행한다(S650). 그 다음에, 각 탐지 노드별로 주변 탐지노드 간의 경로 비용을 테이블로 구성하는 과정을 수행한다(S660).
- <39> 도 7은 무선 센서 네트워크에서 최적 경로 비용과 싱크홀 노드를 거치는 경우의 경로 비용을 비교한 도이다.
- <40> 링크 품질 지표 기반 라우팅에서는 각 라우팅 경로에서의 링크 품질 지표를 누적하여 최소의 값을 가지는 경로를 최적의 경로로 선택한다. 도 7에는 이러한 환경에서 송신 노드(Src. Node)와 수신 노드(Dest. Node)사이의 일반적인 경로 비용과 싱크홀 노드(SH Node)를 거치는 경우의 경로비용이 도시된다. 일반적인 경로 탐색의 경우 최소 경로 비용이 $204(26+24+20+29+30+35+40)$ 가 되고, 싱크홀 노드를 거치는 경우에는 경로 비용이 $249(26+23+25+27+30+26+22+30+40)$ 가 되므로 경로 비용이 204가 되는 최적의 경로에 따라 패킷이 전송된다.
- <41> 위와 같은 환경에서 싱크홀 노드가 라우팅 경로 상에 자신이 포함되도록 하기 위해 취할 수 있는 방법 즉, 싱크홀 공격 방법에는 다음과 같은 방법들이 있다.
- <42> 1. 라우팅 리퀘스트(Routing Request) 패킷을 정상적인 출력보다 더 강한 신호로 보내어 더 멀리 보내거나 또는 수신 노드들이 더 좋은 품질의 신호로 인지하도록 하는 공격 방법.
- <43> 2. 경로 탐색 시 전달되는 라우팅 리퀘스트(Routing Request) 패킷 내의 누적 LQI값을 더 작게 수정하는 공격 방법.
- <44> 이러한 방법을 사용할 경우 싱크홀 노드를 거치는 경로가 최적 경로인 것으로 판단되어 공격이 성공할 수 있다.
- <45> 이러한 예가 도 8에 도시되며, 도 8에서는 상기 2가지 공격 방법이 모두 적용되고 있다. 즉, 싱크홀 노드가 라우팅 리퀘스트 패킷 내의 누적된 LQI값을 131에서 100으로 위조하면서, 정상적인 출력보다 더 강한 신호(LQI값 20)로 메시지를 전달한 경우 경로 비용은 원래의 249가 아닌 190이 되어, 싱크홀 노드를 경유하는 경로를 최적 경로로 선택될 수 있다.
- <46> 도 9는 본 발명에 따른 무선 센서 네트워크에서 링크 품질 지표 기반 라우팅에 대한 싱크홀 공격 탐지의 예를 도시한 도이며, 도 10은 본 발명의 예시적인 일 실시예에 따른 싱크홀 공격 탐지 방법을 도시한 흐름도이다.
- <47> 도 9 및 10을 참조하여, 라우팅 리퀘스트(Routing Request) 패킷을 정상적인 출력보다 더 강한 신호로 보내어 링크 품질을 향상시키는 공격이 발생한 경우의 공격 탐지 방법을 살펴본다.
- <48> 우선, 임의의 수신 센서 노드가 임의의 송신 센서 노드로부터 라우팅 리퀘스트 패킷을 수신한다(S1010).
- <49> 그리고 나서, 수신 센서 노드의 최소 링크 품질 지표값 테이블로부터 이웃 센서 노드간의 최소 링크 품질 지표값을 추출한다(S1020).

- <50> 그 다음에, 추출된 최소 링크 품질 지표값 (LQI_{Min})과 송신 센서 노드로부터 수신된 라우팅 리퀘스트 패킷의 최소 링크 품질 지표값(LQI_{Cur})을 비교한다(S1030). 이때, 이하의 [식 1]이 성립하는지 여부를 판단한다.
- <51> [식 1]
- <52> $LQI_{Cur} < LQI_{Min} \times C$ (C는 허용 오차율),
- <53> 상기 식 1이 성립하는 경우에는 해당 메시지가 최적의 링크 품질보다 좋게 전송된 것이므로, 무선 센서 네트워크 내의 패킷 전송 경로에 싱크홀 노드에 의한 공격이 발생한 것으로 판단(S1040)하고, 공격 발생된 패킷 전송 경로를 배제한 후, 신규 최적 경로를 재탐색하는 과정을 수행한다(S1050).
- <54> 만약, 상기 식 1이 성립하지 않는 경우에는 싱크홀 노드에 의한 공격이 발생하지 않은 것이므로, 설정된 경로를 통하여 패킷을 전송한다(S1060).
- <55> 도 11은 본 발명의 예시적인 다른 실시예에 따른 싱크홀 공격 탐지 방법을 도시한 흐름도이다.
- <56> 도 9 및 도 11을 참조하여, 경로 탐색 시 전달되는 라우팅 리퀘스트(Routing Request) 패킷 내의 누적 LQI값을 더 작게 수정하는 공격이 발생한 경우의 공격 탐지 방법을 살펴본다. 이와 같은 공격은 상기 도 10에서 살펴본 탐지 방법으로는 탐지가 불가능하므로 이하의 공격 탐지 방법을 통하여 공격을 탐지한다.
- <57> 우선, 탐지 노드들은 전파 범위 내의 이웃 센서 노드들의 라우팅 리퀘스트 패킷을 수집하는 과정을 수행한다(S1110).
- <58> 탐지 노드로부터 특정 센서 노드간의 라우팅 리퀘스트 패킷 내의 누적 링크 품질 지표값의 증가분을 도출하는 과정을 수행한다(S1120). 그리고 나서, 탐지 노드를 이용하여 특정 센서 노드간의 최적 경로 비용을 도출하는 과정을 수행한다(S1130).
- <59> 그리고 나서, 누적 링크 품질 지표값의 증가분과 최적 경로 비용을 비교하는 과정을 수행한다(S1140). 상기 비교하는 단계는 이하의 [식 2]가 성립하는지 여부를 판단한다.
- <60> [식 2]
- <61> $CLQI_B - CLQI_A < OLC_{CD} - (LQI_{AC} + LQI_{BD})$
- <62> 이때, $CLQI$ 는 탐지 노드가 수집한 특정 센서 노드에서 전송한 라우팅 리퀘스트 패킷 내의 누적 링크 품질 지표값이며, OLC 는 두 노드간의 최적 경로 비용이며, LQI 는 두 이웃 노드간의 링크 품질 지표값이며, A 및 B는 특정 센서 노드이며, C 및 D는 탐지 노드이다.
- <63> 상기 [식 2]가 성립하는 경우에는 최적의 경로보다 더 좋은 경로로 전송되었다는 모순이 나타나므로, 두 탐지 노드 사이에 싱크홀 공격이 발생한 것으로 판단(S1150)하고, 공격 발생된 패킷 전송 경로를 배제한 후, 신규 최적 경로를 재탐색하는 과정을 수행한다(S1160).
- <64> 도 9를 참조하여 살펴보면, 두 탐지 노드 사이의 최적 경로 비용은 102가 되나, 라우팅 리퀘스트 패킷이 수집된 노드와 탐지 노드간의 비용을 제외해야 하므로 결과적으로 67이라는 값을 얻게 된다. 이 값과 라우팅 리퀘스트 패킷 내의 누적 LQI 값의 증가분인 50을 비교하면, 라우팅 리퀘스트 패킷이 최적의 경로 보다 더 좋은 경로를 통해 전달되었다는 모순이 나타난다. 이런 경우 두 탐지 노드 사이에서 싱크홀 공격이 일어나고 있음을 판단할 수 있다.
- <65> 만약, 상기 [식 2]가 성립하지 않는 경우에는 설정된 경로가 최적 경로이므로, 이러한 경로를 통하여 패킷을 전송한다(S1170).
- <66> 도 12은 본 발명의 예시적인 또 다른 실시예에 따른 싱크홀 공격 탐지 방법을 도시한 흐름도이다. 도 12는 도 10과 도 11에 도시된 공격 탐지 방법을 조합한 방법이다.
- <67> 도 12를 참조하면, 우선, 임의의 수신 센서 노드가 임의의 송신 센서 노드로부터 라우팅 리퀘스트 패킷을 수신한다(S1210).
- <68> 그리고 나서, 수신 센서 노드의 최소 링크 품질 지표값 테이블로부터 이웃 센서 노드간의 최소 링크 품질 지표값을 추출한다(S1220).

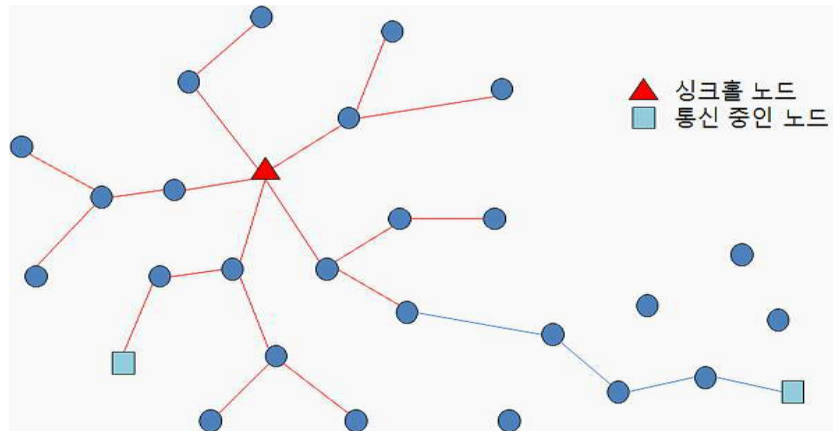
- <69> 그 다음에, 추출된 최소 링크 품질 지표값 (LQI_{Min})과 송신 센서 노드로부터 수신된 라우팅 리퀘스트 패킷의 최소 링크 품질 지표값(LQI_{Cur})을 비교한다(S1230).
- <70> $LQI_{Cur} < LQI_{Min} \times C$ (C는 허용 오차율),
- <71> 상기 식이 성립하는 경우에는 해당 메시지가 최적의 링크 품질보다 좋게 전송된 것이므로, 무선 센서 네트워크 내의 패킷 전송 경로에 싱크홀 노드에 의한 공격이 발생한 것으로 판단(S1240)하고, 공격 발생된 패킷 전송 경로를 배제한 후, 신규 최적 경로를 재탐색하는 과정을 수행한다(S1250).
- <72> 만약, 상기 식이 성립하지 않는 경우에는, 탐지 노드들은 전파 범위 내의 이웃 센서 노드들의 라우팅 리퀘스트 패킷을 수집하는 과정을 수행한다(S1260).
- <73> 탐지 노드로부터 특정 센서 노드간의 라우팅 리퀘스트 패킷 내의 누적 링크 품질 지표값의 증가분을 도출하는 과정을 수행한다(S1270). 그리고 나서, 탐지 노드를 이용하여 특정 센서 노드간의 최적 경로 비용을 도출하는 과정을 수행한다(S1280).
- <74> 그리고 나서, 누적 링크 품질 지표값의 증가분과 최적 경로 비용을 비교하는 과정을 수행한다(S1290). 비교한 결과, 누적 링크 품질 지표값의 증가분이 최적 경로 비용 보다 작다면, 최적의 경로보다 더 좋은 경로로 전송되었다는 모순이 나타나므로, 두 탐지 노드 사이에 싱크홀 공격이 발생한 것으로 판단(S1240)하고, 공격 발생된 패킷 전송 경로를 배제한 후, 신규 최적 경로를 재탐색하는 과정을 수행한다(S1250).
- <75> 만약, 누적 링크 품질 지표값의 증가분이 최적 경로 비용 보다 크다면, 설정된 경로가 최적 경로이므로, 이러한 경로를 통하여 패킷을 전송한다(S1300).
- <76> 이상에서 설명한 것은 본 발명에 따른 공격 탐지 가능 무선 센서 네트워크 시스템 및 이를 이용한 무선 센서 네트워크에서 링크 품질 지표 기반 라우팅에 대한 공격 탐지 방법의 예시적인 실시예에 불과한 것으로서, 본 발명은 상기한 실시예에 한정되지 않고, 이하의 특허청구범위에서 청구하는 바와 같이, 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변경 실시가 가능한 범위까지 본 발명의 기술적 정신이 있다고 할 것이다.

도면의 간단한 설명

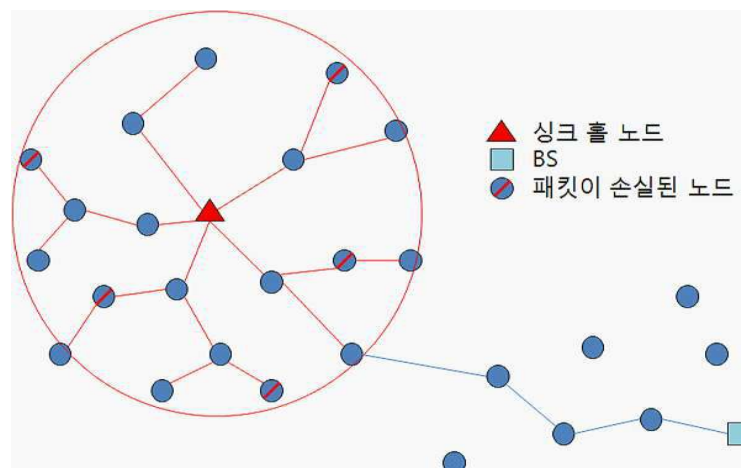
- <77> 도 1은 무선 센서 네트워크 내에서 싱크홀 공격이 발생한 상태를 도시한 개략도이다.
- <78> 도 2는 종래 기술에 따른 홉카운트를 이용한 싱크홀 공격 탐지 방법을 도시한 도이다.
- <79> 도 3은 본 발명에 따른 방법 중 네트워크 초기 설정 과정에서 임의의 센서 노드와 이웃 센서 노드들간의 최소 링크 품질 지표값 테이블의 구성예이다.
- <80> 도 4는 본 발명에 따른 방법 중 네트워크 초기 설정 과정에서 탐지 노드들간의 최적 경로 및 최적 경로에 대한 경로 비용 테이블의 구성예이다.
- <81> 도 5는 각 센서 노드와 이웃 센서 노드들간의 최소 링크 품질 지표(LQI)값 테이블을 구성하는 과정을 도시한 흐름도이다.
- <82> 도 6은 각 탐지 노드별로 주변 탐지 노드들간의 최적 경로에 대한 경로 비용 테이블을 구성하는 과정을 도시한 흐름도이다.
- <83> 도 7은 무선 센서 네트워크에서 최적 경로 비용과 싱크홀 노드를 거치는 경우의 경로 비용을 비교한 도이다.
- <84> 도 8은 싱크홀 공격 발생시의 경로 비용을 도시한 도이다.
- <85> 도 9는 본 발명에 따른 무선 센서 네트워크에서 링크 품질 지표 기반 라우팅에 대한 싱크홀 공격 탐지의 예를 도시한 도이다.
- <86> 도 10은 본 발명의 예시적인 일 실시예에 따른 싱크홀 공격 탐지 방법을 도시한 흐름도이다.
- <87> 도 11은 본 발명의 예시적인 다른 실시예에 따른 싱크홀 공격 탐지 방법을 도시한 흐름도이다.
- <88> 도 12은 본 발명의 예시적인 또 다른 실시예에 따른 싱크홀 공격 탐지 방법을 도시한 흐름도이다.

도면

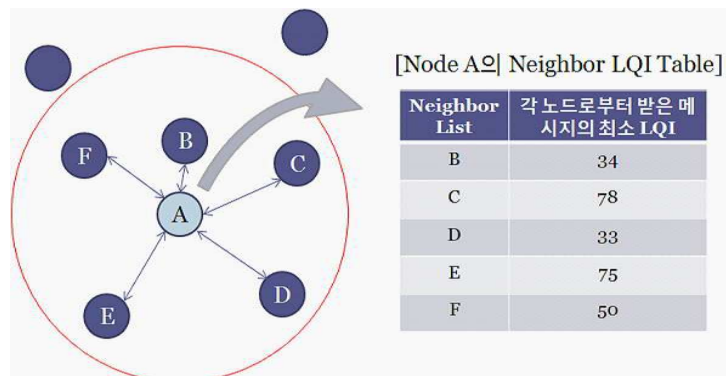
도면1



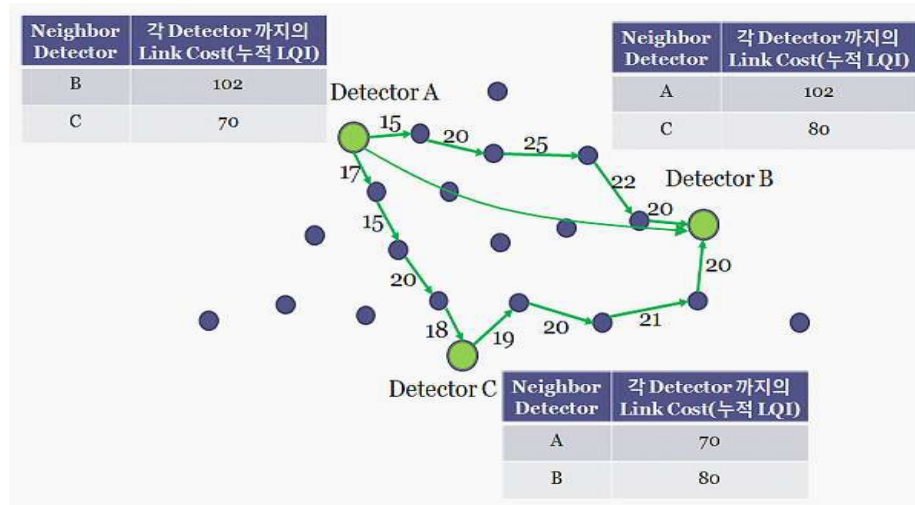
도면2



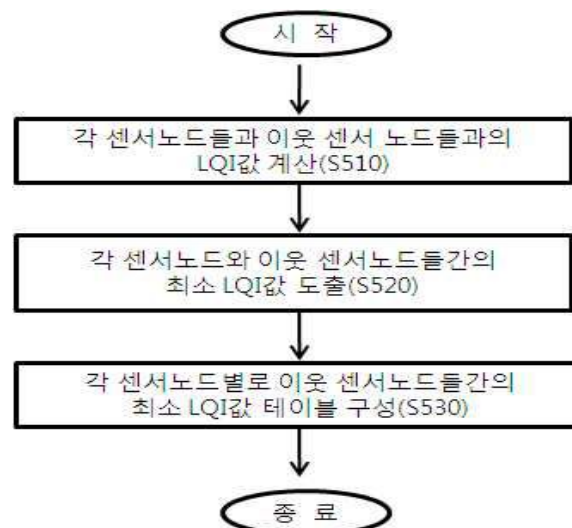
도면3



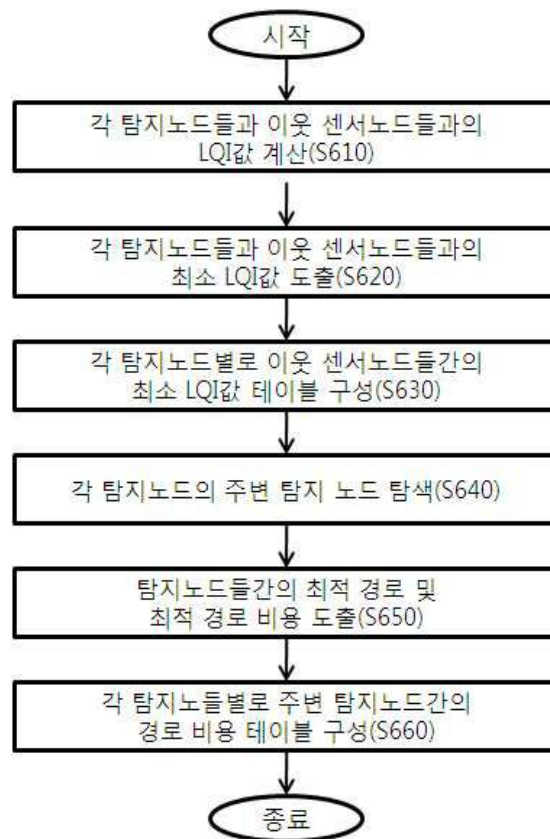
도면4



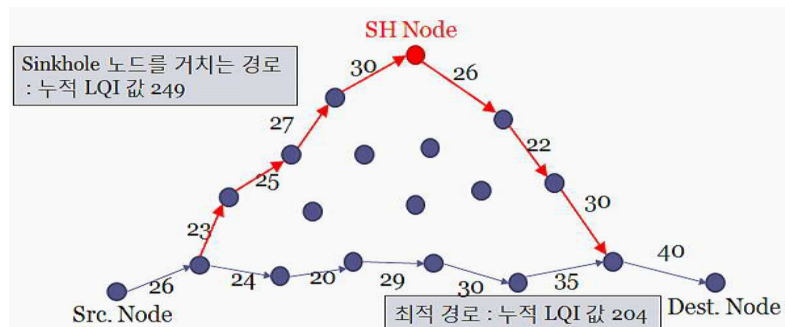
도면5



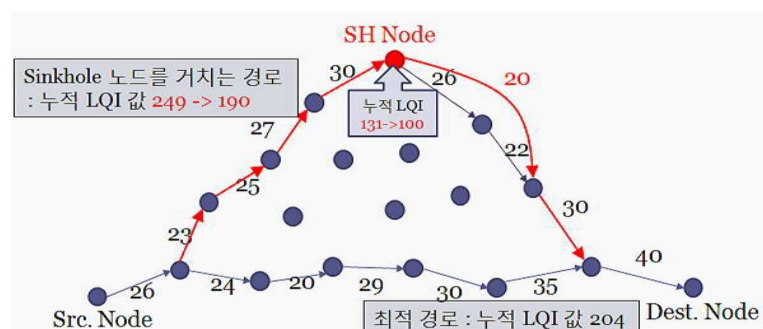
도면6



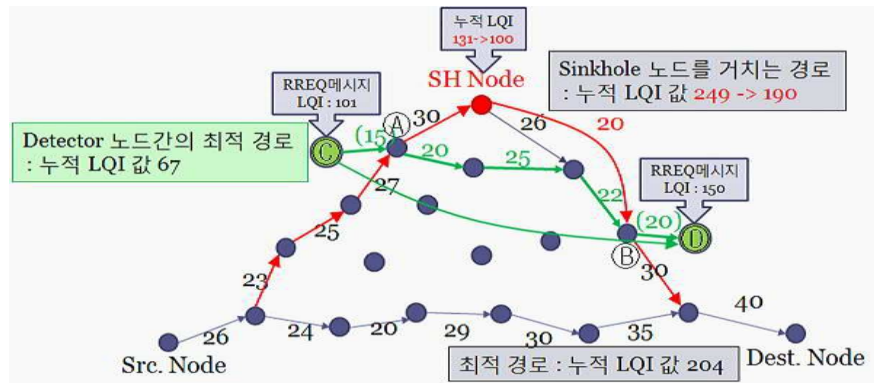
도면7



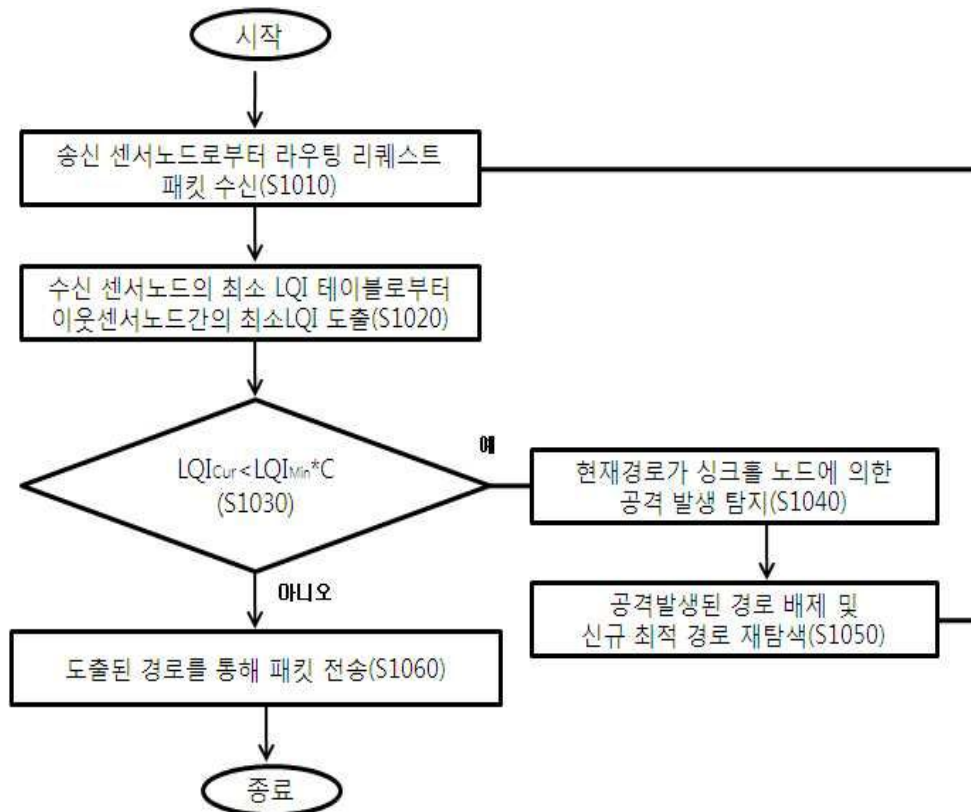
도면8



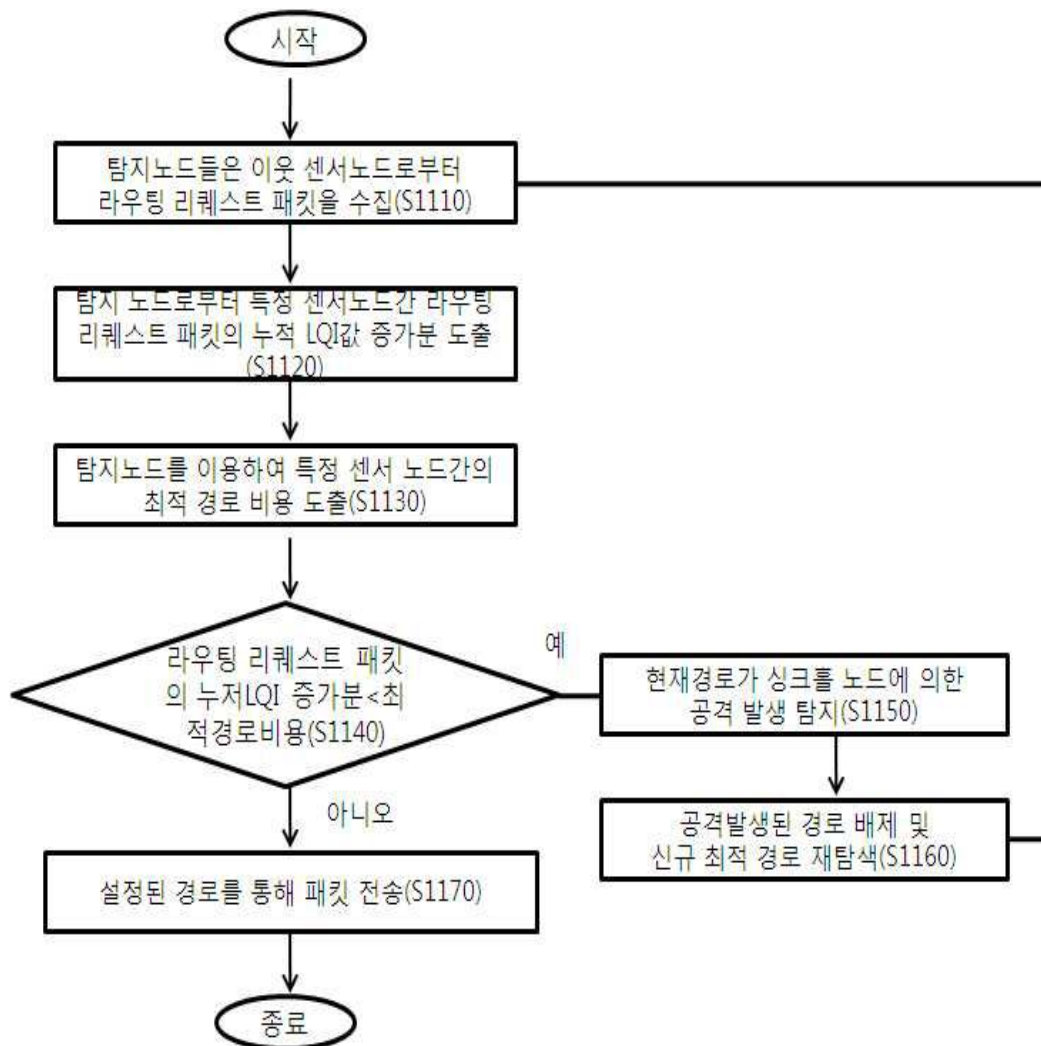
도면9



도면10



도면11



도면12

