



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0035230
(43) 공개일자 2009년04월09일

(51) Int. Cl.

H04L 12/28 (2006.01)

(21) 출원번호 10-2007-0100376

(22) 출원일자 2007년10월05일

심사청구일자 2007년10월05일

(71) 출원인

이화여자대학교 산학협력단

서울 서대문구 대현동 11-1 이화여자대학교내

(72) 발명자

김미희

서울 종로구 무악동 현대아파트 106-303

이명진

서울 성북구 삼선동1가 214-1호 삼일빌라 나동 B01호

채기준

서울 성북구 돈암동 609-1 한신아파트 109-1801

(74) 대리인

김석현, 이희숙

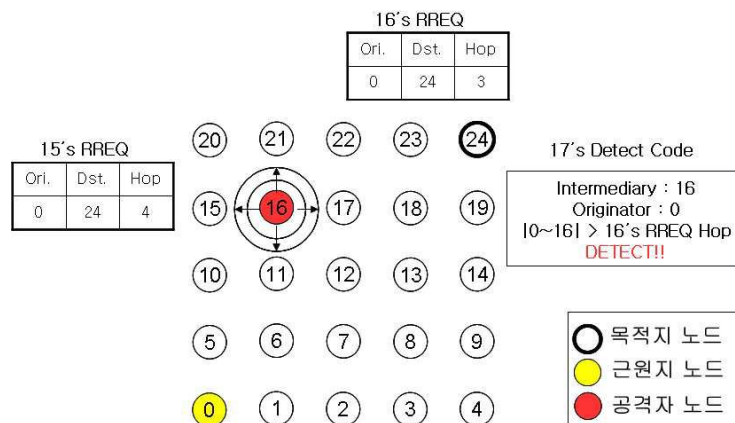
전체 청구항 수 : 총 14 항

(54) 센서 네트워크 시스템 및 그 공격 탐지 방법

(57) 요약

본 발명은 센서 네트워크 시스템 및 그 공격 탐지 방법에 관한 것이다. 본 센서 네트워크 시스템은, 임의로 배치된 복수의 노드를 포함하며, 노드 중 적어도 하나는, 라우팅 경로의 생성시 근원지 노드와 목적지 노드, 또는 근원지 노드와 중간 노드 간에 전달되는 메시지에 포함된 라우팅 정보 중 홉수의 변조를 탐지하는 탐지모드를 구비한다. 이에 의해, 라우팅 경로의 설정시 공격자 노드를 탐지할 수 있도록 함으로써, 공격자 노드를 통한 정보의 유출이나 오염을 차단하여 보안성을 향상시킬 수 있을 뿐만 아니라, 패킷 전송 지연 시간이 증가되는 것을 방지할 수 있다.

대표도 - 도6



특허청구의 범위

청구항 1

임의로 배치된 복수의 노드를 갖는 센서 네트워크 시스템에 있어서,

상기 노드 중 적어도 하나는,

라우팅 경로의 생성시 근원지 노드와 목적지 노드, 또는 근원지 노드와 중간 노드 간에 전달되는 메시지에 포함된 라우팅 정보 중 홉수의 변조를 탐지하는 탐지모드를 구비하는 것을 특징으로 하는 센서 네트워크 시스템.

청구항 2

제1항에 있어서,

상기 탐지모드를 구비하는 노드는,

RREQ 메시지를 생성한 근원지 노드와, 상기 탐지모드를 구비한 노드로 상기 RREQ 메시지를 전달한 노드와의 최단 라우팅 경로상의 최단 홉수를 산출하는 홉수 산출 모드를 구비하는 것을 특징으로 하는 센서 네트워크 시스템.

청구항 3

제1항에 있어서,

상기 탐지모드를 구비하는 노드는,

RREQ 메시지를 생성한 근원지 노드와, 상기 RREQ 메시지에 대한 RREP 메시지를 생성한 노드와의 최단 라우팅 경로상의 최단 홉수를 산출하는 홉수 산출 모드를 구비하는 것을 특징으로 하는 센서 네트워크 시스템.

청구항 4

제2항 또는 제3항에 있어서,

상기 홉수 산출 모드에서는, 상기 근원지 노드의 ID와, 상기 RREQ 메시지 또는 RREP 메시지를 상기 탐지모드를 구비하는 노드로 전달한 노드의 ID를 이용하여 상기 최단 홉수를 산출하는 것을 특징으로 하는 센서 네트워크 시스템.

청구항 5

제2항 또는 제3항에 있어서,

상기 탐지모드에서는 상기 RREQ 메시지 또는 RREP 메시지에 포함된 홉수가 상기 홉수 산출 모드에서 산출된 최단 홉수보다 작은 경우, 상기 RREQ 메시지 또는 RREP 메시지를 상기 탐지모드를 구비하는 노드로 전달한 노드를 공격자 노드로 판단하는 것을 특징으로 하는 센서 네트워크 시스템.

청구항 6

제5항에 있어서,

상기 RREQ 메시지 또는 RREP 메시지를 상기 탐지모드를 구비하는 노드로 전달한 노드가 공격자 노드라는 탐지 메시지가 상기 탐지모드를 구비하는 노드로부터 제공되면, 상기 복수의 노드에 상기 공격자 노드에 대한 정보를 제공하여 상기 공격자 노드를 경유하는 라우팅 경로의 설정을 차단하는 관리 노드를 더 포함하는 것을 특징으로 하는 센서 네트워크 시스템.

청구항 7

제6항에 있어서,

상기 관리 노드는,

상기 공격자 노드로 판단된 노드가 새로운 노드이거나 고장난 노드가 교체된 경우에 해당하면, 상기 탐지모드를

구비하는 노드로부터의 탐지 메시지를 무시하는 것을 특징으로 하는 센서 네트워크 시스템.

청구항 8

임의로 배치된 복수의 노드를 갖는 센서 네트워크 시스템의 공격 탐지 방법에 있어서

라우팅 경로의 생성시 근원지 노드와 목적지 노드, 또는 근원지 노드와 중간 노드 간에 전달되는 메시지를 전달 받는 단계; 및,

상기 메시지에 포함된 라우팅 정보 중 홉수의 변조를 탐지하는 단계를 구비하는 것을 특징으로 하는 센서 네트워크 시스템의 공격 탐지 방법.

청구항 9

제8항에 있어서,

RREQ 메시지를 생성한 근원지 노드와, 홉수의 변조를 탐지하는 탐지모드를 구비하는 노드로 상기 RREQ 메시지를 전달한 노드와의 최단 라우팅 경로상의 최단 홉수를 산출하는 단계를 더 포함하는 것을 특징으로 하는 센서 네트워크 시스템의 공격 탐지 방법.

청구항 10

제8항에 있어서,

RREQ 메시지를 생성한 근원지 노드와, 상기 RREQ 메시지에 대한 RREP 메시지를 생성한 노드와의 최단 라우팅 경로상의 최단 홉수를 산출하는 단계를 더 포함하는 것을 특징으로 하는 센서 네트워크 시스템의 공격 탐지 방법.

청구항 11

제9항 또는 제10항에 있어서,

상기 최단 홉수를 산출하는 단계는, 상기 근원지 노드의 ID와, 상기 탐지모드를 구비하는 노드로 RREQ 메시지 또는 RREP 메시지를 전달한 노드의 ID를 이용하여 상기 최단 홉수를 산출하는 단계인 것을 특징으로 하는 센서 네트워크 시스템의 공격 탐지 방법.

청구항 12

제9항 또는 제10항에 있어서,

상기 홉수의 변조를 탐지하는 단계는,

상기 RREQ 메시지 또는 RREP 메시지에 포함된 홉수가 상기 최단 홉수보다 작은 경우, 상기 탐지모드를 구비하는 노드로 상기 RREQ 메시지 또는 RREP 메시지를 전달한 노드를 공격자 노드로 판단하는 단계인 것을 특징으로 하는 센서 네트워크 시스템의 공격 탐지 방법.

청구항 13

제12항에 있어서,

상기 탐지모드를 구비하는 노드로 상기 RREQ 메시지 또는 RREP 메시지를 전달한 노드가 공격자 노드임을 상기 복수의 노드에 전달하여 상기 공격자 노드를 경유하는 라우팅 경로의 설정을 차단하는 단계를 더 포함하는 것을 특징으로 하는 센서 네트워크 시스템의 공격 탐지 방법.

청구항 14

제11항에 있어서,

상기 공격자 노드로 판단된 노드가 새로운 노드이거나 고장난 노드가 교체된 경우에 해당하면, 상기 탐지모드를 구비하는 노드로부터의 탐지된 상기 공격자 노드에 대한 정보를 무시하는 단계를 더 포함하는 것을 특징으로 하는 센서 네트워크 시스템의 공격 탐지 방법.

명세서

발명의 상세한 설명

기술 분야

- <1> 본 발명은 센서 네트워크 시스템 및 그 공격 탐지 방법에 관한 것으로서, 흡수의 변조를 관찰하여 공격자의 내부 공격을 탐지함으로써, 보안성을 향상시키고, 패킷 전송 지연 시간의 증가를 방지할 수 있도록 하는 센서 네트워크 시스템 및 그 공격 탐지 방법에 관한 것이다.

배경 기술

- <2> 센서 네트워크는 유비쿼터스 컴퓨팅 구현을 위한 기반 네트워크 중의 하나로서 그 중요성이 점차 부각되고 있으며, 네트워크 특성상 보안 기술 또한 기반 기술과 함께 중요하게 인식되고 있다.
- <3> 현재까지 진행된 센서 네트워크 보안 기술은 암호화에 의존하는 인증 구조나 키 관리 구조에 대한 연구가 주를 이루었다. 그러나 센서 노드는 쉽게 포획이 가능하고, 암호화 기술을 사용하는 환경에서도 키가 외부에 노출되기 쉽다. 공격자는 이를 이용하여 합법적인 노드로 가장하여 센서 네트워크 내부에서 공격할 수 있다. 이러한 내부 공격은 노드가 오염되어 공격자에 의해 악용될 수 있으며, 외부 공격에 비해 피해가 더욱 심각하다. 따라서 네트워크의 보안을 보장하기 위해서, 실행가능한 내부 공격 및 그 영향에 대해 분석하고, 이를 통해 내부 공격에 대비한 안전한 매커니즘이 개발되어야 한다.
- <4> 한편, AODV(Ad-hoc On-Demand Distance Vector) 프로토콜은 대표적인 라우팅 프로토콜이며, 라우팅 정보를 얻고자 할때 경로를 찾는 과정을 수행하는 "On-Demand Routing Protocol"이다.
- <5> AODV 프로토콜은, 근원지 노드가 목적지 노드로 데이터 패킷을 보내고자 할 때, 근원지 노드의 라우팅 테이블에 목적지 노드에 대한 라우팅 정보가 없으면, 이웃 노드에 RREQ(Route Request) 메시지를 브로드캐스트한다. 이웃 노드의 라우팅 테이블에도 목적지 노드에 대한 라우팅 정보가 없으면, 이웃 노드는 RREQ 메시지를 자신의 이웃 노드로 전달한다. RREQ 메시지가 목적지 노드에 도달하거나, 목적지 노드에 대한 라우팅 정보를 가진 노드에 도달하면, 해당 노드는 RREP(Route Reply) 메시지를 근원지 노드로 전달한다.
- <6> 이러한 AODV 프로토콜을 이용하는 센서 네트워크 상에서 내부 공격에 의해 받는 영향을 알아보기 위해, 노드 중 하나가 내부 공격에 의해 오염되어 생성된 공격자 노드가 존재하는 경우와, 공격자 노드가 존재하지 않는 경우 각각에 대해, 라우팅 경로 설정상태와, 각 노드를 경유하는 패킷의 수 변화, 각 노드의 패킷 전송 지연 시간의 변화를 살펴보기로 한다.
- <7> 도 1은 공격자 노드가 존재하지 않는 정상적인 환경에서 설정된 라우팅 경로가 표시된 센서 네트워크의 구성도이다.
- <8> 본 센서 네트워크는 NS-2를 기반으로 하여 카네기멜론 대학의 Monarch 그룹에서 개발한 AODV 모듈을 이용한 시뮬레이션으로 구성되었다. 본 센서 네트워크에서는 파라미터로 노드 수, 시뮬레이션 공간, 시뮬레이션 시간, 라디오 전송 범위, 라디오 전파 모델, 패킷 전송률, PHY계층 및 MAC계층이 사용되었고, 각 파라미터의 값으로는 노드 수 25개, 시뮬레이션 공간 70m*70m, 시뮬레이션 시간 100초, 라디오 전송 범위 15m, 라디오 전파 모델 Two-Ray, 패킷 전송률 5 pkt/sec, PHY계층 및 MAC계층으로는 삼성종합기술원과 뉴욕시립대학교에서 IEEE 802.15.4를 위해 개발한 WPAN 모듈이 사용되었다.
- <9> 본 센서 네트워크의 25개 노드는 0번부터 24번으로 명명되며, 각 노드는 행과 열을 따라 각각 5개씩 배치되도록 배열되어 있다. 여기서, 24번 노드가 싱크 노드이며, 0번 노드에서 23번 노드들은 5초마다 CBR 트래픽을 싱크 노드로 전송한다. 그리고 싱크 노드를 제외한 0번 노드에서 23번 노드 중 어떠한 노드라도 공격자 노드가 될 수 있다.
- <10> 도 1은 근원지 노드가 0번 노드이고, 목적지 노드가 24번 노드인 경우, 즉, 0번 노드에서 24번 노드로 가는 라우팅 경로가 설정된 상태를 표시하고 있다. 이는 AODV 매커니즘의 특성상 같은 목적지 노드로의 라우팅 경로는 처음 설정된 라우팅 경로의 영향을 많이 받게 되고, 공격자 노드가 존재할 경우 이러한 특성이 어떠한 영향을 미치는지 살펴보기 위해서 0번 노드가 첫번째 CBR 트래픽을 발생하도록 하였다.
- <11> AODV 프로토콜을 이용한 라우팅 경로의 설정 과정을 살펴보면, 먼저, 0번 노드는 자신의 ID, 목적지 ID, 흡수, 시리얼 넘버가 포함된 RREQ(Route Request) 메시지를 이웃 노드인 1번 노드와 5번 노드에게 전달한다. 1번 노드와 5번 노드는 RREQ 메시지에 포함된 목적지 ID가 자신의 것과 일치하는지 판단하고, 일치하지 아니하면 자신

의 라우팅 테이블의 시리얼 번호와 RREQ 메시지의 시리얼 번호를 비교하여 RREQ 메시지의 시리얼 번호가 자신의 시리얼 번호보다 큰 경우에만 홉수를 증가시켜 자신들의 이웃 노드에 RREQ 메시지를 전달하고, 시리얼 번호가 같은 경우에는 홉수가 작은 경우에만 이웃 노드에 RREQ 메시지를 전달한다. RREQ 메시지를 받은 이웃 노드들도 1번 노드와 5번 노드에서 수행한 것과 동일한 과정을 거쳐 RREQ 메시지를 자신의 이웃 노드들에 전달하고, 이러한 플러딩(flooding) 과정이 반복되어 RREQ 메시지가 24번 노드까지 전달된다. 여기서 0번 노드와 24번 노드 사이의 중간 노드들은, 0번 노드와 자신의 노드까지의 역 경로(reverse route)를 라우팅 테이블에 저장한다.

- <12> 24번 노드가 0번 노드의 RREQ 메시지를 수신하면, 24번 노드는 0번 노드와 24번 노드 사이의 역 경로를 라우팅 테이블에 저장하고, RREP(Route Reply) 메시지를 0번 노드로 전달한다. 이때, RREP 메시지는 유니캐스트 방식으로 전달된다. RREP 메시지를 받은 0번 노드는 RREP 메시지를 수신하였음을 알리는 RREP-ACK 메시지를 24번 노드로 전달한다.
- <13> 이러한 라우팅 경로 설정 과정에 의해, 도 1에 도시된 바와 같이, 0번 노드(근원지 노드) → 5번 노드 → 6번 노드 → 7번 노드 → 12번 노드 → 17번 노드 → 18번 노드 → 23번 노드 → 24번 노드(목적지 노드)에 이르는 0번 노드로부터 24번 노드에 이르는 라우팅 경로가 설정된다.
- <14> 마찬가지로 라우팅 설정 과정에 의해, 20번 노드에서 24번 노드까지의 라우팅 경로는, 20번 노드(근원지 노드) → 21번 노드 → 22번 노드 → 23번 노드 → 24번 노드(목적지 노드)로 설정된다.
- <15> 이렇게 라우팅 경로가 설정되면, 해당 라우팅 경로에 속한 노드들은 CBR 트래픽을 전송할 때, 미리 설정된 라우팅 경로를 사용하게 된다.
- <16> 도 2는 공격자 노드가 존재할 경우 설정된 라우팅 경로를 표시한 센서 네트워크의 구성도이다.
- <17> 일반적으로 센서 네트워크에 공격자 노드가 침입할 경우, 공격자 노드에 의해 라우팅 경로가 변경된다. 공격자 노드는 다양한 공격 유형으로 센서 네트워크를 공격할 수 있다. 공격 유형으로는 Bogus routing information, Selective forwarding, Wormholes, Shinkholes, HELLO Floods, Sybil Attack, DoS(Denial of Service) Attack 등을 들 수 있으며, 이러한 여러 공격 유형 중 라우팅 정보 변조 공격은 다른 공격의 기본이 된다. 라우팅 정보 변조 공격의 경우, 라우팅 정보를 변경하여 다른 노드들이 공격자 노드가 목적지 노드까지 최단의 라우팅 경로를 제공하는 것처럼 인지하도록 함으로써, 목적지 노드까지의 라우팅 경로상에 공격자 노드가 위치하도록 한다. 이렇게 공격자 노드를 라우팅 경로상에 배치시키면, 센서 네트워크상에서 공격자 노드의 영향을 받는 트래픽의 양을 증가시킬 수 있기 때문에, 다른 공격 유형들을 용이하게 적용할 수 있다.
- <18> 본 실시예의 공격자 노드는 라우팅 정보 중 홉수를 감소시켜 다른 노드들에게 전달함으로써, 공격자 노드를 통한 라우팅 경로가 최단의 라우팅 경로인 것으로 다른 노드들이 인지하도록 한다. 즉, 공격자 노드는 이웃 노드로부터 RREQ 메시지를 수신하면, RREQ 메시지내에 포함된 홉수를 1이상 감소시켜 다음 노드로 전달한다.
- <19> 예를 들어, 공격자 노드가 16번 노드인 경우, 만약 공격자 노드가 이웃 노드 중 하나로부터 RREQ 메시지를 받게 되면, 16번 노드는 RREQ 메시지의 홉수를 1이상 감소시킨 후, 이웃 노드인 15번 노드, 17번 노드, 21번 노드, 11번 노드로 변조된 RREQ 메시지를 전달한다. 그러면, 이웃 노드들은 변조된 RREQ 메시지에서 홉수를 1 증가시켜 자신의 이웃 노드들로 전달한다. 이러한 과정을 통해 공격자 노드인 16번 노드를 포함하는 경로는 다른 경로보다 목적지 노드에 도달하기 위한 홉수가 적어질 수 있다.
- <20> 이에 따라, 도 2에 도시된 바와 같이, 공격자 노드가 존재하는 경우, 0번 노드에서 24번 노드로 CBR 트래픽을 전송하는 라우팅 경로는, 0번 노드(근원지 노드) → 5번 노드 → 10번 노드 → 15번 노드 → 16번 노드(공격자 노드) → 17번 노드 → 18번 노드 → 19번 노드 → 24번 노드(목적지 노드)로 설정된다.
- <21> 이렇게 설정된 라우팅 경로는 추후 다른 라우팅 경로의 설정에도 영향을 미치게 된다. 이에 따라, 6번 노드, 7번 노드, 20번 노드가 시작노드가 되어 24번 노드로 CBR 트래픽을 전송하는 경우, 공격자 노드를 포함하는 라우팅 경로가 설정된다. 이렇게 라우팅 경로가 설정되면, 공격자 노드를 경유하는 CBR 트래픽의 양이 증가하게 되며, 다른 노드들이 경유하는 라우팅 경로가 길어지게 된다.
- <22> 예를 들어, 20번 노드의 경우, 공격자 노드가 존재하지 않는 경우에는, 21번 노드, 22번 노드, 23번 노드를 거쳐 24번 노드로 CBR 트래픽을 전송하게 되므로, 4홉 만에 20번 노드부터의 CBR 트래픽이 24번 노드로 전달된다. 그러나 공격자 노드가 존재하는 경우, 15번 노드, 16번 노드, 17번 노드, 18번 노드, 19번 노드를 거쳐 24번 노드로 CBR 트래픽을 전송하게 되므로, 2홉이 늘어나게 된다. 이러한 라우팅 경로의 변경은 공격자 노드가 센서 네트워크를 보다 다양하게 공격할 수 있도록 할 뿐만 아니라, 각 노드들의 CBR 트래픽 전송시간을 증가시

킨다.

- <23> 도 3은 각 노드들이 정상노드인 경우와 공격자 노드인 경우에 각 노드를 경유하는 패킷의 수를 나타낸 그래프이다.
- <24> 도 3에는 0번 노드에서 23번 노드가 정상인 경우, 각 노드를 경유하는 패킷의 수와, 0번 노드에서 23번 노드가 각각 공격자 노드인 경우, 각 노드를 경유하는 패킷의 수가 비교되어 있다. 도시된 바와 같이, 각 노드는 정상인 경우와 공격자 노드인 경우 경유하는 패킷의 수가 현저히 차이가 남을 알 수 있다.
- <25> 다만, 동그라미 표시가 되어 있는 4번 노드, 9번 노드, 19번 노드, 20번 노드, 21번 노드, 23번 노드의 경우에는 정상 상태에서와 공격자 노드인 경우에서 경유하는 패킷의 수가 동일하다.
- <26> 여기서 19번 노드와 23번 노드의 경우, 목적지 노드인 24번 노드와 1홉 거리에 있기 때문에, 목적지 노드로 패킷을 전달하기 위해서 19번 노드와 23번 노드 중 하나를 필수적으로 거쳐야 한다. 따라서 공격자인지 아닌지 여부에 무관하게 경유하는 패킷의 수가 동일하게 된다.
- <27> 나머지 노드의 경우, 4번 노드 및 9번 노드는 센서 네트워크의 오른쪽 아래에 위치하고, 20번 노드와 21번 노드는 센서 네트워크의 왼쪽 위에 위치함으로써, 0번 노드와 24번 노드를 잇는 대각선으로부터 멀리 이격되어 있다. 일반적으로 AODV 매커니즘에 따르면 RREQ 메시지를 받은 노드들은, 자신이 목적지 노드가 아니더라도 목적지 노드로의 라우팅 경로를 알고 있으면 RREP 메시지를 전송하게 된다. 따라서 같은 목적지 노드로 여러 노드가 패킷을 전송하는 네트워크의 경우에는 처음 결정된 라우팅 경로에 영향을 많이 받게 된다. 즉, 0번 노드로부터 24번 노드로 CBR 트래픽을 전송하기 때문에 0번 노드와 24번 노드를 잇는 대각선으로부터 멀리 이격된 4번 노드, 9번 노드, 20번 노드, 21번 노드의 경우에는 정상 상태에서도 경유하는 패킷의 수가 적을 뿐만 아니라, 이웃 노드의 수가 적기 때문에, 공격자 노드가 되더라도 큰 영향을 미칠 수 없다.
- <28> 도 4는 도 3의 각 노드들이 정상노드인 경우와 공격자 노드인 경우에 각 노드를 경유하는 패킷의 수를 비율로 나타낸 그래프이다.
- <29> 각 노드들이 공격자 노드로 변경되었을 경우, 각 노드들을 경유하는 패킷의 수와 패킷 전송시간이 증가하게 된다. 예를 들어, 11번 노드의 경우, 정상노드인 경우 40개의 패킷이 11번 노드를 경유하게 되지만, 공격자 노드로 변경되었을 경우에는 경유하는 패킷의 수가 120으로 증가한다. 즉, 3배나 더 많은 패킷이 11번 노드를 경유하게 되는 것이다.
- <30> 결과적으로, 각 노드들을 경유하는 패킷의 수는 최대 142 패킷, 평균 55 패킷이 증가하였으며, 이에 따라, 패킷의 증가율은 최대 8.1배, 평균 2.56배가 된다. 그리고 패킷 전송 지연 시간은 최대 0.017초이고 평균 0.0089초가 된다.
- <31> 한편, 3배 이상의 증가율을 보이는 노드는, 1번 노드, 8번 노드, 10번 노드, 11번 노드, 15번 노드, 16번 노드, 22번 노드이다. 이들 노드들은 모두 정상노드인 경우 0번 노드에서 24번 노드 사이에 설정된 라우팅 경로의 주변에 위치한 노드들이다.
- <32> 이를 통해, 정상노드인 경우 설정된 라우팅 경로에 인접한 노드들이 공격자 노드가 될 경우, 공격자 노드가 아닐 때에 비해 경유하는 패킷의 수가 급격히 증가하여 트래픽의 양이 증가함을 알 수 있다. 이는 공격자 노드가 정상노드였을 때 형성된 라우팅 경로와 인접하게 위치하는 경우, 센서 네트워크에 더 치명적인 공격이 가해질 수 있다는 것을 의미한다.
- <33> 도 5는 11번 노드가 공격자 노드인 경우, 주변 노드들의 패킷 전송 지연 시간을 나타낸 그래프이다.
- <34> 11번 노드가 공격자 노드가 되면, 0번 노드에서 24번 노드 사이의 라우팅 경로는, 11번 노드를 포함하는 0번 노드 → 5번 노드 → 10번 노드 → 11번 노드 → 16번 노드 → 17번 노드 → 18번 노드 → 19번 노드 → 24번 노드가 된다.
- <35> 도 5에는 11번 노드의 주변 노드 중, 0번 노드와, 라우팅 경로에 포함되지 아니하는 6번 노드, 7번 노드, 12번 노드, 15번 노드에 대한 패킷 전송 지연시간을, 11번 노드가 정상노드일 때와 11번 노드가 공격자 노드일 때로 나누어 표시하고 있다.
- <36> 대부분의 주변 노드들이 11번 노드가 정상노드일 때보다 11번 노드가 공격자 노드가 되었을 때 패킷 전송 지연 시간이 증가된 것을 볼 수 있다. 특히 7번 노드와 12번 노드의 경우, 정상노드일 때보다 11번 노드가 공격자 노드인 경우 패킷 전송 지연 시간이 다른 노드들보다 길어져 있다. 이는 7번 노드와 12번 노드의 경우 11번 노

드를 통해 24번 노드로 가는 라우팅 경로가 최단 라우팅 경로가 아니기 때문이다.

- <37> 반면, 11번 노드를 통해 24번 노드로 가는 라우팅 경로가 최단의 라우팅 경로인 노드, 예를 들어, 6번 노드의 경우에도 패킷 전송 지연 시간이 증가된 것을 볼 수 있다. 이는 11번 노드의 트래픽 양이 증가함에 따라 11번 노드를 경유하는 노드들의 패킷 전송 지연 시간도 증가되기 때문인 것으로 판단된다.
- <38> 상술한 센서 네트워크의 경우, 노드의 수가 25개로 센서 네트워크의 규모가 작고 트래픽의 양이 많지 않기 때문에 정상노드일 때와 공격자가 존재하는 상태에서의 패킷 전송 지연 시간의 차이가 크지 않지만, 실제적인 센서 네트워크에서는 공격자가 존재할 경우 패킷 전송 지연 시간의 차이가 클 것으로 예상된다.
- <39> 이와 같이, 센서 네트워크의 내부에 공격자 노드가 존재할 경우, 공격자 노드는 센서 네트워크내의 라우팅 경로 중 상당 부분이 공격자 노드를 경유하도록 라우팅 정보를 변조한다. 이에 따라, 공격자 노드를 통한 정보의 유출이 용이하게 이루어지므로 보안이 치명적으로 손상된다. 또한, 공격자 노드를 경유하는 패킷의 수가 증가함에 따라, 공격자 노드의 패킷 전송 지연 시간이 증가할 뿐만 아니라, 공격자 노드에 인접하게 배치된 주변 노드들의 패킷 전송 지연 시간도 증가한다.
- <40> 이에 따라, 공격자 노드를 탐지하여 공격자 노드를 경유하는 라우팅 경로가 생성되지 않도록 하는 방법을 모색할 필요가 있다.

발명의 내용

해결 하고자하는 과제

- <41> 본 발명의 목적은, 공격자 노드를 탐지하여 공격자 노드를 경유하는 라우팅 경로가 생성되지 않도록 함으로써, 정보의 보안성을 향상시키고 센서 네트워크의 패킷 전송 지연 시간이 증가하는 것을 방지할 수 있도록 하는 센서 네트워크 시스템 및 그 공격 탐지 방법을 제공하는 것이다.

과제 해결수단

- <42> 상기 목적은, 임의로 배치된 복수의 노드를 갖는 센서 네트워크 시스템에 있어서, 상기 노드 중 적어도 하나는, 라우팅 경로의 생성시 근원지 노드와 목적지 노드, 또는 근원지 노드와 중간 노드 간에 전달되는 메시지에 포함된 라우팅 정보 중 홉수의 변조를 탐지하는 탐지모드를 구비하는 것을 특징으로 하는 센서 네트워크 시스템에 의해 달성될 수 있다.
- <43> 상기 탐지모드를 구비하는 노드는, RREQ 메시지를 생성한 근원지 노드와, 상기 탐지모드를 구비한 노드로 상기 RREQ 메시지를 전달한 노드와의 최단 라우팅 경로상의 최단 홉수를 산출하는 홉수 산출 모드를 구비하는 것이 바람직하다.
- <44> 상기 탐지모드를 구비하는 노드는, RREQ 메시지를 생성한 근원지 노드와, 상기 RREQ 메시지에 대한 RREP 메시지를 생성한 노드와의 최단 라우팅 경로상의 최단 홉수를 산출하는 홉수 산출 모드를 구비하는 것이 바람직하다.
- <45> 상기 홉수 산출 모드에서는, 상기 근원지 노드의 ID와, 상기 RREQ 메시지 또는 RREP 메시지를 상기 탐지모드를 구비하는 노드로 전달한 노드의 ID를 이용하여 상기 최단 홉수를 산출할 수 있다.
- <46> 상기 탐지모드에서는 상기 RREQ 메시지 또는 RREP 메시지에 포함된 홉수가 상기 홉수 산출 모드에서 산출된 최단 홉수보다 작은 경우, 상기 RREQ 메시지 또는 RREP 메시지를 상기 탐지모드를 구비하는 노드로 전달한 노드를 공격자 노드로 판단할 수 있다.
- <47> 상기 RREQ 메시지 또는 RREP 메시지를 상기 탐지모드를 구비하는 노드로 전달한 노드가 공격자 노드라는 탐지 메시지가 상기 탐지모드를 구비하는 노드로부터 제공되면, 상기 복수의 노드에 상기 공격자 노드에 대한 정보를 제공하여 상기 공격자 노드를 경유하는 라우팅 경로의 설정을 차단하는 관리 노드를 더 포함할 수 있다.
- <48> 상기 관리 노드는, 상기 공격자 노드로 판단된 노드가 새로운 노드이거나 고장난 노드가 교체된 경우에 해당하면, 상기 탐지모드를 구비하는 노드로부터의 탐지 메시지를 무시할 수 있다.
- <49> 한편, 상기 목적은, 임의로 배치된 복수의 노드를 갖는 센서 네트워크 시스템의 공격 탐지 방법에 있어서, 라우팅 경로의 생성시 근원지 노드와 목적지 노드, 또는 근원지 노드와 중간 노드 간에 전달되는 메시지를 전달받는 단계; 및, 상기 메시지에 포함된 라우팅 정보 중 홉수의 변조를 탐지하는 단계를 구비하는 것을 특징으로 하는 센서 네트워크 시스템의 공격 탐지 방법에 의해서도 달성될 수 있다.

- <50> RREQ 메시지를 생성한 근원지 노드와, 홉수의 변조를 탐지하는 탐지모드를 구비하는 노드로 상기 RREQ 메시지를 전달한 노드와의 최단 라우팅 경로상의 최단 홉수를 산출하는 단계를 더 포함하는 것이 바람직하다.
- <51> RREQ 메시지를 생성한 근원지 노드와, 상기 RREQ 메시지에 대한 RREP 메시지를 생성한 노드와의 최단 라우팅 경로상의 최단 홉수를 산출하는 단계를 더 포함하는 것이 바람직하다.
- <52> 상기 최단 홉수를 산출하는 단계는, 상기 근원지 노드의 ID와, 상기 탐지모드를 구비하는 노드로 RREQ 메시지 또는 RREP 메시지를 전달한 노드의 ID를 이용하여 상기 최단 홉수를 산출하는 단계일 수 있다.
- <53> 상기 홉수의 변조를 탐지하는 단계는, 상기 RREQ 메시지 또는 RREP 메시지에 포함된 홉수가 상기 최단 홉수보다 작은 경우, 상기 탐지모드를 구비하는 노드로 상기 RREQ 메시지 또는 RREP 메시지를 전달한 노드를 공격자 노드로 판단하는 단계일 수 있다.
- <54> 상기 탐지모드를 구비하는 노드로 상기 RREQ 메시지 또는 RREP 메시지를 전달한 노드가 상기 공격자 노드임을 상기 복수의 노드에 전달하여 상기 공격자 노드를 경유하는 라우팅 경로의 설정을 차단하는 단계를 더 포함할 수 있다.
- <55> 상기 공격자 노드로 판단된 노드가 새로운 노드이거나 고장난 노드가 교체된 경우에 해당하면, 상기 탐지모드를 구비하는 노드로부터의 탐지된 상기 공격자 노드에 대한 정보를 무시하는 단계를 더 포함할 수 있다.

효 과

- <56> 본 발명의 센서 네트워크 시스템 및 그 공격 탐지 방법에 따르면, 라우팅 경로의 설정시 공격자 노드를 탐지할 수 있도록 함으로써, 공격자 노드를 통한 정보의 유출이나 오염을 차단하여 보안성을 향상시킬 수 있을 뿐만 아니라, 패킷 전송 지연 시간이 증가되는 것을 방지할 수 있다.

발명의 실시를 위한 구체적인 내용

- <57> 본 발명에 따른 센서 네트워크 시스템 및 그 공격 탐지 방법은, 라우팅 경로의 설정시 공격자 노드가 라우팅 정보를 변경하는 것을 탐지할 수 있도록 함으로써, 공격자 노드를 파악할 수 있도록 한다.
- <58> 일반적으로 공격자 노드가 포함되는 라우팅 경로가 최단의 라우팅 경로라고 믿도록 하기 위해, 공격자 노드가 라우팅 정보 중 변경가능한 필드는 RREQ ID의 증가, 홉수의 감소, 목적지 노드에 대한 시퀀스 번호의 증가, 근원지 노드에 대한 시퀀스 번호의 증가가 있다.
- <59> 이 중 RREQ ID는, 근원지 노드 IP 주소와 함께 RREQ 메시지를 식별할 수 있도록 하는 정보로서, 공격자 노드는 RREQ ID를 수정하여 다른 노드들에게 전달할 수 있다. 그러나 RREQ ID의 증가는 공격자 노드가 근원지 노드로부터 1홉 이내에 있을 경우에만 가능하다. 그렇지 아니할 경우, 공격자 노드로 RREQ 메시지를 전송한 노드에게도 RREQ ID가 변경된 RREQ 메시지가 전달되고, 해당 노드가 자신의 라우팅 테이블을 갱신하기 때문에 라우팅 루프가 발생하여 경로가 망가지게 된다.
- <60> 한편, 시퀀스 번호의 경우, 공격자 노드는 목적지 노드에 대한 시퀀스 번호 및 근원지 노드에 대한 시퀀스 번호를 2의 배수로 증가시켜 전송하게 되며, 이는 시퀀스 번호 값이 홀수이면 유효하지 않은 정보로 판단하고 그 패킷을 버리기 때문이다. 이렇게 시퀀스 번호 값을 2의 배수로 증가시켜서 이웃 노드들로 전달할 경우, 공격자 노드로 RREQ 메시지를 전달하였던 노드로도 시퀀스 번호가 증가된 RREQ 메시지가 제공된다. 이때, 해당 노드는 자신의 라우팅 테이블에 저장된 시퀀스 번호보다 공격자 노드로부터 제공받은 RREQ 메시지의 시퀀스 번호가 더 크므로, 자신의 라우팅 테이블을 갱신하게 된다. 즉, 공격자 노드와 공격자 노드로 RREQ 메시지를 전달한 노드 사이에 라우팅 루프가 생성되어 AODV 알고리즘에 의해 공격자 노드가 쉽게 탐지된다.
- <61> 이에 따라, RREQ ID의 증가와, 시퀀스 번호의 증가는 공격자 노드를 용이하게 탐지할 수 있기 때문에 사용되지 아니하므로, 본 발명의 센서 네트워크 시스템에서는 공격자 노드가 홉수를 감소시켜 라우팅 정보를 변경하는 경우에 대해서만 고려한다. 즉, 본 발명의 센서 네트워크 시스템에서는 홉수가 감소할 경우, 이를 탐지할 수 있는 메커니즘을 적용한다.
- <62> 도 6은 본 발명에 따라 탐지 노드가 포함된 센서 네트워크 시스템에서 RREQ 메시지의 홉수 변조를 탐지하는 과정을 보인 도면이다.
- <63> 본 센서 네트워크 시스템은, 공격자 노드의 라우팅 정보 변경을 탐지하는 탐지 노드, 싱크 노드, 공격자 여부를

판단하여 소정의 조치를 취하는 관리 노드(미도시)를 포함한다.

- <64> 도 6에 도시된 본 실시예에 따른 센서 네트워크 시스템에서는, 탐지 노드와 싱크 노드가 행과 열을 따라 각각 5개의 노드가 배열된 형태로 구성되어 있으며, 각 노드는 0번에서 24번까지의 명명된다. 여기서, 24번 노드는 싱크 노드이고, 0번 노드에서 23번 노드들은 탐지 노드이며, 탐지 노드들은 5초마다 CBR 트래픽을 싱크 노드로 전송한다.
- <65> 각 탐지 노드는 라우팅 테이블을 가지며, 홉수 산출 모드와 탐지모드를 수행할 수 있다.
- <66> 홉수 산출 모드는, 임의의 두 노드 사이에 형성된 최단 라우팅 경로의 홉수를 산출하는 기능으로서, 탐지 노드는 임의의 두 노드의 ID를 알면 두 노드 사이의 최단 홉수를 계산할 수 있다. 본 발명에서는 홉수 산출 모드의 구현방법에 대해 상세히 설명하지는 아니하나, 위치기반기술과 관련된 라우팅 프로토콜 분야에서 홉수 산출에 대해 많이 연구되어 왔고 현재도 계속 연구되고 있기 때문에 충분히 구현가능한 기술이다.
- <67> 이러한 홉수 산출 모드의 동작시, 각 탐지 노드는 다른 노드로부터 RREQ 메시지 또는 RREP 메시지를 전달받으면, RREQ 메시지 또는 RREP 메시지를 발생시킨 근원지 노드의 ID와, RREQ 메시지를 해당 탐지 모드에 전달해준 이전 노드의 ID를 이용하여, 근원지 노드와 이전 노드와의 최단 홉수를 산출한다. 산출된 최단 홉수는 탐지모드시 이전 노드가 공격자 노드인지를 판단하기 위해 사용된다.
- <68> 탐지모드는, 공격자 노드에 의해 라우팅 정보 중 홉수가 변경되는 것을 탐지할 수 있는 기능으로서, RREQ 메시지와 RREP 메시지에 포함된 홉수가 변경되면, 각 탐지 노드는 홉수를 변경한 노드를 공격자 노드로 보고 공격자 노드를 탐지했다는 탐지 메시지를 관리 노드로 제공한다.
- <69> 탐지모드의 수행시, 탐지 노드는, 홉수 산출 모드에 의해 산출된 근원지 노드와 이전 노드와의 최단 홉수를 제공받으면, 홉수 산출 모드에 의해 산출된 최단 홉수와, 이전 노드로부터 전달된 RREQ 메시지 또는 RREP 메시지에 포함된 홉수를 비교한다.
- <70> 비교결과, 산출된 최단 홉수보다 RREQ 메시지 또는 RREP 메시지에 포함된 홉수가 작으면, 이전 노드가 공격자 노드라고 판단한다. 이는 공격자 노드의 경우, 공격자 노드를 경유하는 라우팅 경로가 타 노드들에게 최단 라우팅 경로로 인지되도록 하기 위해, RREQ 메시지 또는 RREP 메시지에 포함된 홉수를 감소시켜 제공하기 때문이다. 즉, 공격자 노드에서 홉수가 변조된 RREQ 메시지 또는 RREP 메시지에 포함된 홉수는, 산출된 최단 홉수보다 작게 된다. 이렇게 이전 노드가 공격자 노드라고 판단되면, 탐지 노드는 공격자 노드에 대한 정보를 관리 노드로 전달한다.
- <71> 관리 노드는, 탐지 노드로부터 제공된 공격자 노드에 대한 정보를 제공받아 해당 노드가 공격자 노드인지를 다시 판단하고, 공격자 노드라고 판단되면 공격자 노드에 대한 정보를 각 탐지 노드와 싱크 노드로 전달하여 공격자 노드를 경유하는 라우팅 경로가 생성되지 아니하도록 한다.
- <72> 이때, 관리 노드가 공격자 노드인지를 다시 판단하는 이유는 다음과 같다.
- <73> 일반적으로 센서 네트워크 시스템의 고장이 발생할 경우, 새로운 노드가 투입되거나 고장난 노드가 교체될 수 있다. 이러한 새로운 노드의 투입이나 고장난 노드의 교체로 인해, 기존에 설정된 라우팅 경로보다 더 짧은 라우팅 경로가 생성될 수 있으며, 탐지 노드가 이러한 정보를 가지고 있지 않다면, 탐지 노드는 새로이 생성된 짧은 라우팅 경로를 공격자 노드에 의한 공격으로 판단할 수 있다.
- <74> 관리 노드는 미리 새로운 노드의 투입이나 고장난 노드의 교체를 공지하여 탐지 노드에 의한 잘못된 탐지를 방지할 수도 있고, 새로운 노드의 투입이나 고장난 노드의 교체에 의해 공격자 노드가 탐지된 경우, 탐지 노드로부터 판단된 공격자 노드에 대한 정보를 무시함으로써, 잘못된 탐지에 의한 피해를 감소시킬 수 있다.
- <75> 한편, 베이스 스테이션이나 클러스터 헤드 등의 중앙 관리 노드를 구비하는 센서 네트워크에서는 중앙 관리 노드를 관리 노드로 사용할 수 있다.
- <76> 도 6에서는 16번 노드가 공격자 노드인 경우를 예로 들어 공격자 노드를 탐지하는 과정이 도시되어 있다.
- <77> 0번 노드에서 24번 노드로의 라우팅 경로를 설정하기 위해, 0번 노드에서 RREQ 메시지를 전송하는 경우, 15번 노드는 16번 노드를 포함한 이웃 노드들로 RREQ 메시지를 전달한다. 15번 노드가 16번 노드로 전달한 RREQ 메시지에는 근원지 노드의 ID(Or i.), 목적지 노드의 ID(Dst.), 홉수(Hop)가 포함되어 있으며, 시작노드의 ID는 0, 목적지 노드의 ID는 24, 홉수는 4로 되어 있다.

- <78> 이러한 RREQ 메시지를 전달받은 공격자 노드인 16번 노드는 RREQ 메시지에 포함된 홉수를 1 감소시켜 3으로 변조한다. 그런 다음, 이웃 노드인 15번 노드, 11번 노드, 17번 노드, 21번 노드로 변조된 RREP 메시지를 전달한다. 각 이웃 노드는 탐지 노드로서 홉수 산출 모드와 탐지모드를 가지므로, 각각 공격자 노드를 탐지할 수 있다.
- <79> 이중 17번 노드에서 수행되는 탐지 과정을 살펴보면 다음과 같다.
- <80> 17번 노드는 16번 노드로부터 RREQ 메시지가 전달되면, 홉수 산출 모드를 작동시켜 시작노드인 0번 노드와 이전 노드인 16번 노드 사이의 최단 홉수(10~16)를 산출한다. 이때, 최단 홉수는 4가 된다. 그런 다음, 17번 노드는 탐지 기능을 동작시켜 산출된 최단 홉수와 16번 노드로부터의 RREQ 메시지에 포함된 홉수(16's RREQ Hop)를 비교한다. 비교결과, 산출된 최단 홉수가 16번 노드로부터의 RREQ 메시지에 포함된 홉수보다 큰 경우, 17번 노드는 16번 노드가 공격자 노드라고 판단한다. 여기서, 산출된 최단 홉수는 4이고, 16번 노드로부터의 RREQ 메시지에 포함된 홉수는 3이므로, 17번 노드는 16번 노드를 공격자 노드라고 판단한다.
- <81> 17번 노드는 탐지결과를 관리 노드로 전송하고, 관리 노드는 16번 노드가 새로운 노드의 투입이나 고장난 노드가 교체된 것인지 아닌지를 판단한다. 16번 노드가 새로운 노드의 투입이나 고장난 노드의 교체가 아닌 경우, 관리 노드는 16번 노드를 공격자 노드로 판단한다. 그런 다음, 관리 노드는 각 탐지 노드로 16번 노드가 공격자 노드임을 알림으로써, 16번 노드를 경유하는 라우팅 경로가 생성되지 않도록 한다.
- <82> 도 7은 본 발명에 따른 탐지 노드가 포함된 센서 네트워크 시스템에서 RREP 메시지의 홉수 변조를 탐지하는 과정을 보인 도면이다.
- <83> 도 7에는 16번 노드가 공격자 노드인 센서 네트워크 시스템에서 0번 노드로부터 24번 노드로의 라우팅 경로가 설정된 경우를 도시하고 있으며, 0번 노드로부터 24번 노드로의 라우팅 경로는, 0번 노드(근원지 노드) → 5번 노드 → 10번 노드 → 15번 노드 → 16번 노드(공격자 노드) → 17번 노드 → 18번 노드 → 19번 노드 → 24번 노드(목적지 노드)로 설정되어 있다.
- <84> 이 상태에서 12번 노드가 24번 노드로 CBR 트래픽을 전송하고자 하는 경우, 12번 노드는 RREQ 메시지를 각 이웃 노드인 7번 노드, 13번 노드, 11번 노드, 17번 노드로 브로드캐스트한다. 여기서, 24번 노드로의 라우팅 경로상에 위치한 17번 노드는 24번 노드까지의 라우팅 경로에 대한 정보를 가지고 있으므로, 17번 노드는 RREQ 메시지를 받으면 이웃 노드로 브로드캐스팅하지 않고 직접 RREP 메시지를 작성하여 12번 노드로 제공한다. 그리고 7번 노드와 13번 노드는 24번 노드로의 라우팅 경로에 대한 정보를 가지고 있지 아니하므로, 일단 공격자 노드인 16번 노드를 탐지하는 과정에서는 제외하기로 한다.
- <85> 한편, 16번 노드와 이웃하고 있는 11번 노드는, 12번 노드로부터 전달받은 RREQ 메시지의 홉수를 증가시켜 16번 노드로 전달한다. 공격자 노드인 16번 노드는 24번 노드로의 라우팅 경로상에 위치하므로, 16번 노드의 라우팅 테이블에는 24번 노드까지의 라우팅 경로가 저장되어 있다. 따라서, 16번 노드는 RREP 메시지를 작성하여 11번 노드로 전달한다. 이때, 16번 노드는 공격자 노드이기 때문에 RREP 메시지내의 홉수를 1 감소시킨 후 11번 노드로 전달한다.
- <86> 11번 노드는 16번 노드로부터 전달받은 RREP 메시지를 12번 노드로 전달하기 전, 홉수 산출 모드와 탐지모드를 동작시켜 16번 노드가 공격자 노드인지를 탐지한다. 먼저, 홉수 산출 모드의 동작에 의해 11번 노드는 RREP 메시지를 전달한 16번 노드와 12번 노드 사이의 최단 홉수를 산출하고, 16번 노드로부터의 RREP 메시지에 포함된 홉수와, 산출된 최단 홉수를 비교한다. 이때, 산출된 최단 홉수는 2가 되고, 16번 노드로부터의 RREP 메시지에 포함된 홉수는 1이다. 이에 따라, 16번 노드로부터의 RREP 메시지에 포함된 홉수가 산출된 최단 홉수보다 작으므로, 11번 노드는 16번 노드가 공격자 노드라고 판단한다.
- <87> 그런 다음, 11번 노드는 관리 노드로 16번 노드가 공격자 노드임을 알리고, 관리 노드는 16번 노드가 진정한 공격자 노드임을 판단한다. 판단결과 16번 노드가 공격자 노드인 경우 관리 노드는 각 탐지 노드로 16번 노드가 공격자 노드임을 알려 16번 노드를 포함하는 라우팅 경로가 생성되지 않도록 한다.
- <88> 한편, 상술한 실시예에서는 공격자 노드에 이웃하는 탐지 노드에서만 공격자 노드를 탐지하는 과정을 설명하고 있으나, 다른 탐지 노드에서도 공격자 노드인지 여부를 탐지할 수 있음은 물론이다. 예를 들어, 도 7에 도시된 실시예에서 11번 노드가 16번 노드를 공격자 노드라고 탐지한 다음, 홉수가 변조된 RREP 메시지를 12번 노드에 제공하면, 12번 노드에서도 다시 한번 홉수 산출 모드와 탐지모드를 동작시켜 16번 노드가 공격자 노드인지 여부를 판단할 수 있다. 이 경우, 12번 노드는 16번 노드가 공격자 노드라고 판단할 것이며, 이에 대한 정보를

관리모드로 전달한다. 그러면 관리모드는 11번 노드와 12번 노드로부터 제공받은 정보에 기초하여 16번 노드가 공격자 노드인지를 다시 한번 판단할 수 있다. 이렇게 여러 탐지 노드로부터 동일한 정보를 제공받게 되면, 관리모드는 공격자 모드를 보다 정확하고 신속하게 판단할 수 있다.

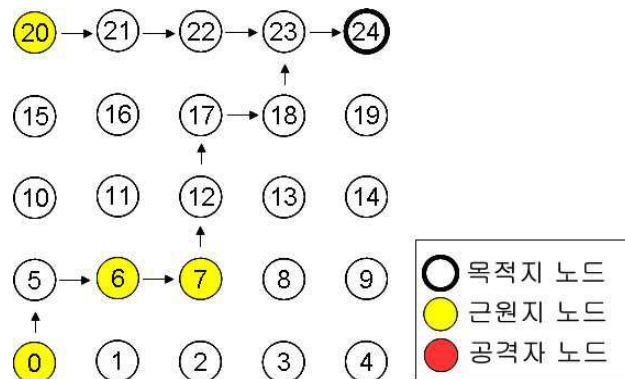
- <89> 이와 같이, 본 센서 네트워크 시스템에서는 각 노드에 라우팅 정보의 변조를 탐지할 수 있는 탐지모드를 부여함으로써, 라우팅 경로의 설정시 홉수를 변조하는 공격자 노드를 탐지할 수 있도록 한다. 공격자 노드의 탐지에 의해, 공격자 노드를 경유하는 라우팅 경로의 설정을 방지할 수 있으며, 공격자 노드를 경유하는 라우팅 경로를 통해 다른 공격이 이루어지는 것을 방지할 수 있다. 이에 따라, 공격자 노드를 통한 정보의 유출이나 오염을 차단하여 보안성을 향상시킬 수 있을 뿐만 아니라, 패킷 전송 지연 시간이 증가되는 것을 감소시킬 수 있다.

도면의 간단한 설명

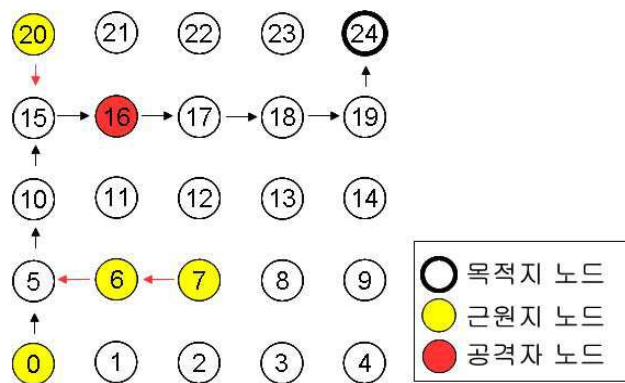
- <90> 도 1은 공격자 노드가 존재하지 않는 정상적인 환경에서 설정된 라우팅 경로가 표시된 센서 네트워크의 구성도,
- <91> 도 2는 공격자 노드가 존재할 경우 설정된 라우팅 경로를 표시한 센서 네트워크의 구성도,
- <92> 도 3은 각 노드들이 정상노드인 경우와 공격자 노드인 경우에 각 노드를 경유하는 패킷의 수를 나타낸 그래프,
- <93> 도 4는 도 3의 각 노드들이 정상노드인 경우와 공격자 노드인 경우에 각 노드를 경유하는 패킷의 수를 비율로 나타낸 그래프,
- <94> 도 5는 11번 노드가 공격자 노드인 경우, 주변 노드들의 패킷 전송 지연 시간을 나타낸 그래프,
- <95> 도 6은 본 발명에 따라 탐지 노드가 포함된 센서 네트워크 시스템에서 RREQ 메시지의 홉수 변조를 탐지하는 과정을 보인 도면,
- <96> 도 7은 본 발명에 따른 탐지 노드가 포함된 센서 네트워크 시스템에서 RREP 메시지의 홉수 변조를 탐지하는 과정을 보인 도면이다.

도면

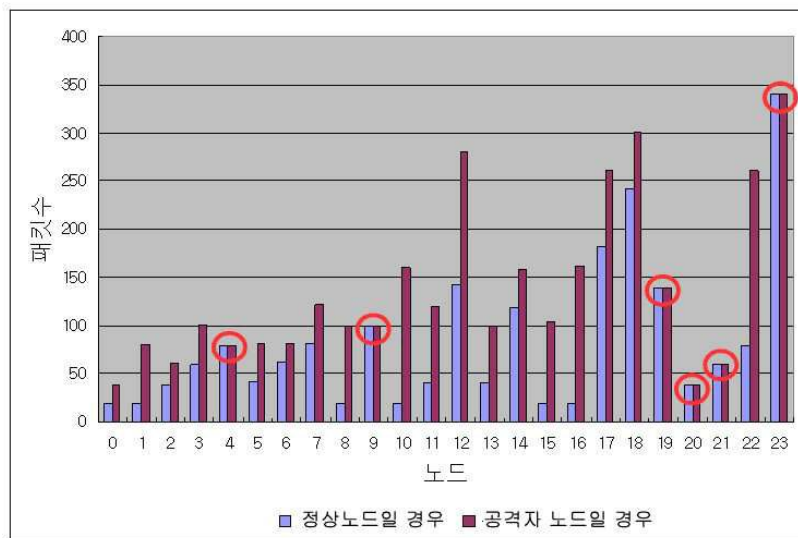
도면1



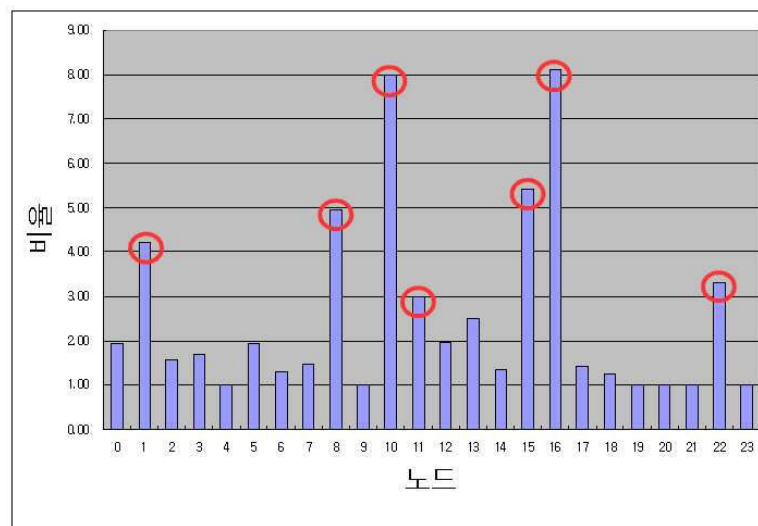
도면2



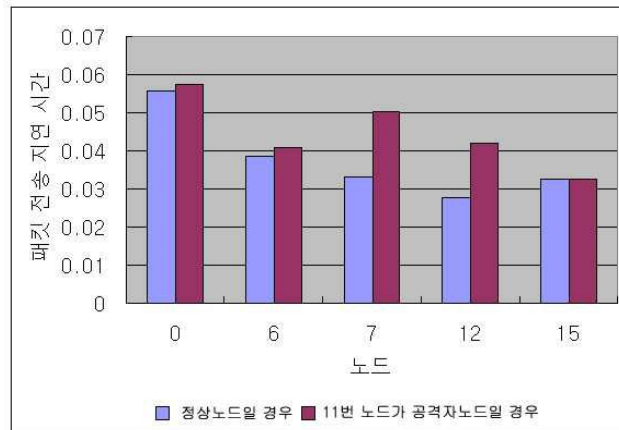
도면3



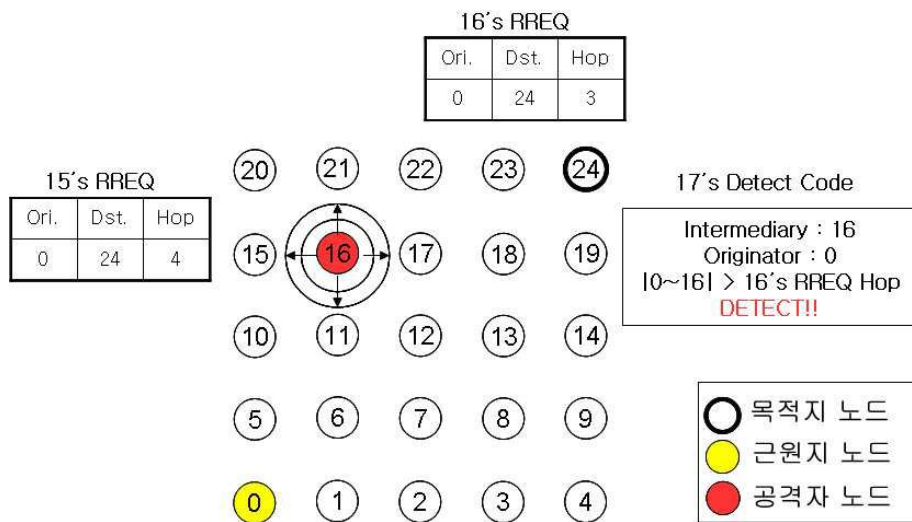
도면4



도면5



도면6



도면7

