(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0022469
(43) 공개일자 2009년03월04일

(51) Int. Cl.
G06F 15/00 (2006.01) *H04L 12/28* (2006.01)
H04L 9/32 (2006.01)
(21) 출원번호 10-2007-0087831
(22) 출원일자 2007년08월30일
심사청구일자 2007년08월30일

(71) 출원인
이화여자대학교 산학협력단
서울 서대문구 대현동 11-1 이화여자대학교내
(72) 발명자
김미희
서울 종로구 무악동 현대아파트 106-303
채기준
서울 성북구 돈암동 609-1 한신아파트 109-1801
(74) 대리인
김석현, 이희숙

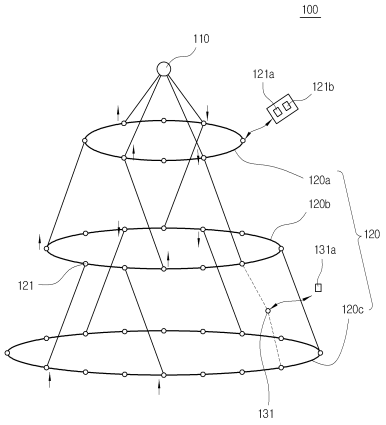
전체 청구항 수 : 총 25 항

(54) 계층적 오버레이 네트워크 시스템 및 이를 이용한 DDoS공격 대항 방법

(57) 요 약

본 발명에서, 계층적 오버레이 네트워크 시스템은 최상위 대응 시스템, 계층적 오버레이 네트워크를 포함한다. 오버레이 네트워크는, 일반동작모드를 가진 적어도 하나의 일반노드와, 오버레이 동작모드와 일반동작모드를 가진 적어도 하나의 오버레이 노드를 포함하며, 일반노드와 오버레이 노드는 복수의 계층적인 구조로 이루어져 있다. 여기에서, 오버레이 노드는 DDoS(Distributed Denial of Service) 공격을 우회하도록 라우팅한다. 최상위 시스템(110)은, DDoS 공격이 탐지되면, 피해지역 주변의 일부 오버레이 노드를 오버레이 동작모드에서 동작하도록 제어한다. 따라서, DDoS 공격 차단 과정에서 사용되는 협동을 위한 제어 트래픽의 빠르고 정상적인 전송 보장 및 공격 발생시 정상 트래픽의 피해 최소화를 할 수 있고, 나아가서 계층적인 네트워크 구조 및 다양한 처리능력의 노드가 존재함을 고려하여 다수의 계층적인 오버레이를 구성하여 오버헤드를 줄일 수 있다.

대 표 도 - 도2



특허청구의 범위

청구항 1

오버레이 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 오버레이 동작모드와 일반 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 일반동작모드를 가진 적어도 하나의 오버레이 노드를 포함하며, 상기 일반노드와 오버레이 노드는 복수의 계층적으로 구조로 이루어진 것인 오버레이 네트워크; 및

DDoS 공격이 탐지되면, 상기 오버레이 노드를 오버레이 동작모드에서 동작하도록 제어하는 최상위 대응 시스템;을 포함하며,

상기 오버레이 동작모드에서, 상기 오버레이 노드는 DDoS 공격을 우회하도록 라우팅 하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 2

제1항에 있어서,

상기 오버레이 노드는 DDoS 공격을 탐지하며, DDoS 공격을 탐지하면 상기 오버레이 동작모드하에서 상기 DDoS 공격의 피해를 받았다는 것을 나타내는 공격 탐지 메시지를 상기 최상위 대응 시스템에 통지하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 3

제1항에 있어서,

상기 오버레이 네트워크는, 일반 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 일반동작모드를 가진 적어도 하나의 일반노드를 더 포함하며,

상기 일반노드는 DDoS 공격을 탐지하며, DDoS 공격을 탐지하면 자신에게 인접한 오버레이 노드 중 상기 DDoS 공격의 피해를 받지 않은 오버레이 노드로 상기 DDoS 공격의 피해를 받았다는 것을 나타내는 공격 탐지 메시지를 통지하고,

상기 일반 노드로부터 상기 공격 탐지 메시지를 통지받은 오버레이 노드는, 통지받은 상기 공격 탐지 메시지를 상기 오버레이 동작모드하에서 상기 최상위 대응 시스템에 통지하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 4

제2항 또는 제3항에 있어서,

상기 공격 탐지 메시지는 공격 탐지 노드에 대한 정보, 공격 피해 노드에 대한 정보, 공격 탐지 노드와 공격 피해 노드의 상하관계에 대한 정보를 포함하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 5

제2항 또는 제3항에 있어서,

상기 최상위 대응 시스템은 상기 공격 탐지 메시지를 근거로 하여 상기 공격 피해 노드를 우회하는 차단 노드들로 구성된 차단 노드 집합을 결정하고, 차단 노드 집합에 대한 정보와 상기 공격 피해 노드에 대한 정보를 포함하는 차단 공지 메시지를 상기 차단 노드들로 전송하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 6

제1항에 있어서,

상기 복수의 계층에서 동일 계층에 포함된 오버레이 노드들은 데이터 패킷의 처리 용량이 서로 유사한 것임을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 7

제1항에 있어서,

상기 오버레이 라우팅 테이블은,

대응하는 오버레이 노드의 일련 번호+2^m을 저장하는 첫번째 블럭;

상기 목적지 노드에 대한 번호를 저장하는 두번째 블럭; 및

다음 노드에 대한 정보를 저장하는 세번째 블럭을 포함하고,

여기서 2^m은 오버레이 네트워크에 최대로 포함될 수 있는 오버레이 노드의 개수를 나타내며, m은 1 이상의 자연수인 것을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 8

제1항에 있어서,

상기 일반노드는, 관리자의 설정에 의한 멤버 조인 방법과, 메시지에 의한 멤버 조인 방법에 의해 상기 오버레이 노드에 조인하여 오버레이 네트워크의 멤버로 구성되는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 9

제8항에 있어서,

상기 관리자의 설정에 의한 멤버 조인 방법은, 상기 오버레이 네트워크 구성 시에 각 오버레이 노드가 포함되는 오버레이 계층 및 해당 오버레이 계층이 포함하는 처리능력 범위를 관리자가 설정하고, chord 방법에 따라 멤버로 조인시키는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 10

제8항에 있어서,

상기 메시지에 의한 멤버 조인 방법은, 오버레이 네트워크 구성 후, 추가 노드 배치 및 재배치에 의한 동적인 네트워크 환경에서 조인 탐사 메시지 및 조인 응답 메시지에 의해서 멤버 조인을 동적으로 수행하는 방법으로서,

상기 일반노드 중 상기 오버레이 노드로서 조인하고 자 하는 조인의뢰노드는, 자신의 데이터 패킷 처리 용량과 함께 상기 오버레이 노드로서 조인할 것을 요청하는 조인 탐사 메시지를 상기 오버레이 네트워크에 포함된 오버레이 노드들로 전송하고,

상기 조인 탐사 메시지를 전송받은 오버레이 노드들은 자신의 데이터 패킷 처리 용량과 자신이 소속된 오버레이 네트워크 계층에 대한 정보를 포함하는 조인 응답 메시지를 상기 조인의뢰노드로 전송하며,

상기 조인의뢰노드는, 상기 조인 응답 메시지를 참조하여 조인할 오버레이 네트워크 계층을 결정하고, 상기 결정한 오버레이 네트워크 계층에 포함된 오버레이 노드들로 조인 요청 메시지를 전송함으로써 새로운 오버레이 노드로 조인하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 11

제10항에 있어서,

상기 조인의뢰노드는, 조인 응답 메시지에 포함된 오버레이 노드들의 데이터 패킷 처리 용량을 참조하여, 자신의 데이터 패킷 처리 용량과 같거나 작은 값을 가진 노드가 속한 네트워크 계층을 조인할 네트워크 계층으로 결정하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 12

제10항에 있어서,

상기 조인 요청 메시지를 수신한 오버레이 노드들은, 상기 수신한 조인 요청 메시지를 참조하여 Chord 프로토콜에 따라 자신들의 오버레이 라우팅 테이블을 갱신하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 13

제10항에 있어서,

상기 조인의뢰노드가, 조인할 것으로 결정한 네트워크 계층의 상위 계층에 속한 오버레이 노드와 연결되어 있는 경우, 상기 조인 요청 메시지에 상기 조인의뢰노드의 계층 정보 및 연결정보가 포함된 것임을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 14

제5항에 있어서,

상기 차단 노드는 상기 오버레이 동작 모드하에서 데이터 패킷을 라우팅하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 15

제14항에 있어서,

상기 차단 노드 집합은, DDoS 공격을 탐지한 노드들, 공격 트래픽 방향으로 DDoS 공격에 의해 희생된 희생자 노드에 연결된 노드들, 및 희생자 노드들과 같은 레벨의 노드들로 이루어진 것으로 결정되는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템.

청구항 16

오버레이 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 오버레이 동작모드와 일반 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 일반동작모드를 가진 적어도 하나의 오버레이 노드를 포함하고, 상기 일반노드와 오버레이 노드는 복수의 계층적으로 구조로 이루어진 오버레이 네트워크를 구성하는 단계;

상기 일반 노드 또는 상기 오버레이 노드가 DDoS 공격을 탐지하는 단계;

상기 DDoS 공격이 탐지되면, 상기 오버레이 노드를 오버레이 동작모드에서 동작하도록 제어하는 단계; 를 포함하며,

상기 오버레이 동작모드에서, 상기 오버레이 노드는 DDoS 공격을 우회하도록 라우팅 하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템을 이용한 DDoS 공격 대항 방법.

청구항 17

제16항에 있어서

상기 오버레이 노드는 DDoS 공격을 탐지하면 상기 오버레이 동작모드하에서 상기 DDoS 공격의 피해를 받았다는 것을 나타내는 공격 탐지 메시지를 상기 최상위 대응 시스템에 통지하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템을 이용한 DDoS 공격 대항 방법.

청구항 18

제16항에 있어서,

상기 오버레이 네트워크는 일반 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 일반동작모드를 가진 적어도 하나의 일반노드를 더 포함하며,

상기 일반노드는 DDoS 공격을 탐지하면 자신에게 인접한 오버레이 노드 중 상기 DDoS 공격의 피해를 받지 않은 오버레이 노드로 상기 DDoS 공격의 피해를 받았다는 것을 나타내는 공격 탐지 메시지를 통지하고,

상기 일반 노드로부터 상기 공격 탐지 메시지를 통지받은 오버레이 노드는, 통지받은 상기 공격 탐지 메시지를 상기 오버레이 동작모드하에서 상기 최상위 대응 시스템에 통지하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템을 이용한 DDoS 공격 대항 방법.

청구항 19

제16항에 있어서,

상기 복수의 계층에서 동일 계층에 포함된 오버레이 노드들은 데이터 패킷의 처리 용량이 서로 유사한 것임을 특징으로 하는 계층적 오버레이 네트워크 시스템을 이용한 DDoS 공격 대항 방법.

청구항 20

제16항에 있어서,

상기 일반노드 중 상기 오버레이 노드로서 조인하고 자 하는 조인의뢰노드는, 자신의 데이터 패킷 처리 용량과 함께 상기 오버레이 노드로서 조인할 것을 요청하는 조인 탐사 메시지를 상기 오버레이 네트워크에 포함된 오버레이 노드들로 전송하고,

상기 조인 탐사 메시지를 전송받은 오버레이 노드들은 자신의 데이터 패킷 처리 용량과 자신이 소속된 오버레이 네트워크 계층에 대한 정보를 포함하는 조인 응답 메시지를 상기 조인의뢰노드로 전송하며,

상기 조인의뢰노드는, 상기 조인 응답 메시지를 참조하여 조인할 오버레이 네트워크 계층을 결정하고, 상기 결정한 오버레이 네트워크 계층에 포함된 오버레이 노드들로 조인 요청 메시지를 전송함으로써 새로운 오버레이 노드로 조인하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템을 이용한 DDoS 공격 대항 방법.

청구항 21

제20항에 있어서,

상기 조인의뢰노드는, 조인 응답 메시지에 포함된 오버레이 노드들의 데이터 패킷 처리 용량을 참조하여, 자신의 데이터 패킷 처리 용량과 같거나 작은 값을 가진 노드가 속한 네트워크 계층을 조인할 네트워크 계층으로 결정하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템을 이용한 DDoS 공격 대항 방법.

청구항 22

제20항에 있어서,

상기 조인 요청 메시지를 수신한 오버레이 노드들은, 상기 수신한 조인 요청 메시지를 참조하여 Chord 프로토콜에 따라 자신들의 오버레이 라우팅 테이블을 갱신하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템을 이용한 DDoS 공격 대항 방법.

청구항 23

제20항에 있어서,

상기 조인의뢰노드가, 조인할 것으로 결정한 네트워크 계층의 상위 계층에 속한 오버레이 노드와 연결되어 있는 경우, 상기 조인 요청 메시지에 상기 조인의뢰노드의 계층 정보 및 연결정보가 포함된 것임을 특징으로 하는 계층적 오버레이 네트워크 시스템을 이용한 DDoS 공격 대항 방법.

청구항 24

제20항에 있어서,

상기 최상위 대응 시스템은, 상기 공격 탐지 메시지를 수신하면, 상향 또는 하향 트래픽이 우회할 차단 노드 집합을 결정하고, 상기 결정한 차단 노드 집합의 정보를 포함한 차단 공지 메시지를 상기 차단 노드 집합에 포함된 차단 노드로 전송하며,

상기 차단 노드는 상기 오버레이 동작 모드하에서 데이터 패킷을 라우팅하는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템을 이용한 DDoS 공격 대항 방법.

청구항 25

제24항에 있어서,

상기 차단 노드 집합은, DDoS 공격을 탐지한 노드들, 공격 트래픽 방향으로 DDoS 공격에 의해 희생된 희생자 노드에 연결된 노드들, 및 희생자 노드들과 같은 레벨의 노드들로 이루어진 것으로 결정되는 것을 특징으로 하는 계층적 오버레이 네트워크 시스템을 이용한 DDoS 공격 대항 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 네트워크 시스템에 관한 것으로, 더욱 상세하게는 공격에 대항할 수 있는 계층적 오버레이 네트워크 시스템 및 이를 이용한 DDoS 공격 대항 방법에 관한 것이다.

배 경 기 술

<2> 일반적으로, 서비스 거부(Denial of Service: DoS) 공격은 그 처리 용량을 초과하는 많은 양의 트래픽으로 웹 사이트, 인터넷 서비스 제공자(ISP) 및 다른 서버와 같은 네트워크 노드를 망가뜨리고, 그에 따라 공격 지속 기간동안 네트워크에서 망가뜨려진 노드를 파괴하는 것으로 정의된다.

<3> 또한, DoS 보다 강한 공격을 하는 분산형 서비스 거부 공격(DDoS)에서는 공격을 시작하고자 하는 공격자가 잘 알려진 보안 허점(loopholes)을 거쳐 많은 노드를 파괴한다. 이렇게 손상된 노드는 반드시 공격자의 종속 제어자가 되고, 네트워크로 트래픽을 주입하는 시작(launch) 지점처럼 행동한다. 따라서, 공격자는 다수의 시작 지점으로부터 트래픽을 캐스캐이딩(cascading)함으로써 대규모 네트워크에 폭 넓은 공격을 시작할 수 있다.

<4> DDoS 공격은 다수의 공격 에이전트를 분산 설치해 두고 동시에 공격함으로써 하나의 시스템 자원뿐 아니라 네트워크 자원까지도 고갈시킬 수 있는 간단하면서도 매우 강력한 공격이다. 실제로 웜 바이러스와 함께 DDoS 공격으로 인한 대량의 이상 트래픽으로 인해 인터넷 사용에 있어서 연결 실패나 속도 저하 등의 문제를 일으키는 사례가 증가하고 있으며, 이로 인한 피해는 점점 더 심각해지고 있는 실정이다. 특히 많은 근거리 통신 네트워크(LAN)가 트리와 같은 계층적인 네트워크 구조를 띄고 있는데, 이러한 경우 특정 라우터가 공격에 의해 마비되면 그 하위 네트워크 또한 인터넷으로의 연결을 잃게 되어 통신이 두절될 수 있어 그 피해 지역은 더욱 커질 수 있다.

<5> 도 1은 DoS 공격을 받는 종래의 네트워크 시스템을 나타낸 도면이다.

<6> 도 1을 참조하면, 대다수의 종래의 네트워크 시스템(10)은 트리와 같은 계층적인 구조를 갖는다. 즉, 네트워크 시스템의 최상위에는 다른 인터넷과 연결되고, 네트워크 시스템에 포함된 모든 노드들을 관리하는 최상위 노드(11)가 구비된다. 최상위 노드를 기준으로 단계적으로 라우팅할 수 있는 라우터(12)가 존재하고, 각 라우터에는 일반 노드들이 연결된다.

<7> 도 1에 도시된 바와 같이, 특정 계층에 속하는 라우터에 공격이 가해지면, 공격에 희생된 라우터(14)가 완전히 마비되어, 상기한 라우터(14)에 연결된 하위 노드들(13)은 인터넷과의 연결이 차단되게 된다. 즉, 종래의 계층적 네트워크 시스템(10)에서는 라우터가 공격에 의해서 마비되면, 하위 노드들의 통신에도 영향을 미치게 된다.

<8> 종래 DDoS 공격에 대한 대응책을 마련하기 위해서, 최근 DoS(Denial of Service) 공격 혹은 DDoS 공격에 대한 다각적인 연구들이 진행되어 왔다. 그러나 현재까지 제안된 보안 메커니즘들은 이에 대한 탐지, 공격 트래픽의 필터링, 그리고 공격 에이전트의 추적 등에 집중되어 있고, 특히 도 1과 같은 계층적인 구조에서는 분산 공격에 대한 협동 대응을 위한 제어 트래픽 전송도 원활하지 못할 수 있다는 문제가 있다. 또한 그러한 네트워크 구조에서는 필터링 기능을 수행한다고 하더라도 일반적인 라우팅으로는 완전히 공격 에이전트를 제거하기 전까지 공격 트래픽에 의해 다른 노드들의 트래픽 전송에 영향을 줄 수 있기 때문에 전체적인 피해가 커지게 된다.

<9> 따라서, DDoS 공격 차단 과정에서 사용되는 협동을 위한 제어 트래픽의 빠르고 정상적인 전송 보장 및 공격 발생시 정상 트래픽의 피해 최소화를 할 수 있고, 나아가서 계층적인 네트워크 구조 및 다양한 처리능력의 노드가 존재함을 고려하여 오버헤드를 줄일 수 있는 방안이 필요하다.

발명의 내용

해결 하고자하는 과제

<10> 본 발명의 목적은 DDoS 공격 차단 과정에서 사용되는 협동을 위한 제어 트래픽의 빠르고 정상적인 전송 보장 및 공격 발생시 정상 트래픽의 피해 최소화를 할 수 있고, 나아가서 계층적인 네트워크 구조 및 다양한 처리능력의 노드가 존재함을 고려하여 오버헤드를 줄일 수 있는 계층적 오버레이 네트워크 시스템을 제공하는

것이다.

<11> 본 발명의 다른 목적은 상기한 계층적 오버레이 네트워크 시스템의 DDoS 공격 대항 방법을 제공하는 것이다.

과제 해결수단

<12> 본 발명의 일 실시예에 따른 계층적 오버레이 네트워크 시스템은, 오버레이 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 오버레이 동작모드와 일반 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 일반동작모드를 가진 적어도 하나의 오버레이 노드를 포함하며, 상기 일반노드와 오버레이 노드는 복수의 계층적으로 구조로 이루어진 것인 오버레이 네트워크; 및 DDoS 공격이 탐지되면, 상기 오버레이 노드를 오버레이 동작모드에서 동작하도록 제어하는 최상위 대응 시스템;을 포함하며, 상기 오버레이 동작모드에서, 상기 오버레이 노드는 DDoS 공격을 우회하도록 라우팅 한다.

<13> 상술한 오버레이 노드는 DDoS 공격을 탐지하는 동작을 수행하며, DDoS 공격을 탐지하면 상기 오버레이 동작모드하에서 상기 DDoS 공격의 피해를 받았다는 것을 나타내는 공격 탐지 메시지를 상기 최상위 대응 시스템에 통지할 수 있다.

<14> 한편, 상기 오버레이 네트워크는, 일반 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 일반동작모드를 가진 적어도 하나의 일반노드를 더 포함하며, 상기 일반노드는 DDoS 공격을 탐지하는 동작을 수행하여, DDoS 공격을 탐지하면 자신에게 인접한 오버레이 노드 중 상기 DDoS 공격의 피해를 받지 않은 오버레이 노드로 상기 DDoS 공격의 피해를 받았다는 것을 나타내는 공격 탐지 메시지를 통지하고, 상기 일반 노드로부터 상기 공격 탐지 메시지를 통지받은 오버레이 노드는, 통지받은 상기 공격 탐지 메시지를 상기 오버레이 동작모드하에서 상기 최상위 대응 시스템에 통지할 수 있다.

<15> 상술한 공격 탐지 메시지는 공격 탐지 노드에 대한 정보, 공격 피해 노드에 대한 정보, 공격 탐지 노드와 공격 피해 노드의 상하관계에 대한 정보를 포함할 수 있다.

<16> 한편, 상술한 최상위 대응 시스템은 상기 탐지 결과 메시지를 근거로 하여 상기 공격 피해 노드를 우회하는 차단 노드들로 구성된 차단 노드 집합을 결정하고, 차단 노드 집합에 대한 정보와 상기 공격 피해 노드에 대한 정보를 포함하는 차단 공지 메시지를 상기 차단 노드들로 전송할 수 있다.

<17> 또한, 상술한 복수의 계층에서 동일 계층에 포함된 오버레이 노드들은 데이터 패킷의 처리 용량이 서로 유사할 수 있다.

<18> 한편, 상기 오버레이 라우팅 테이블은, 대응하는 오버레이 노드의 일련 번호+2^m을 저장하는 첫번째 블럭; 상기 목적지 노드에 대한 번호를 저장하는 두번째 블럭; 및 다음 노드에 대한 정보를 저장하는 세번째 블럭을 포함하고, 여기서 2^m은 오버레이 네트워크에 최대로 포함될 수 있는 오버레이 노드의 개수를 나타내며, m은 1 이상의 자연수이다.

<19> 또한, 상기 일반노드는, 관리자의 설정에 의한 멤버 조인 방법과, 메시지에 의한 멤버 조인 방법에 의해 상기 오버레이 노드에 조인하여 오버레이 네트워크의 멤버로 구성될 수 있다.

<20> 한편, 상기 관리자의 설정에 의한 멤버 조인 방법은, 상기 오버레이 네트워크 구성 시에 각 오버레이 노드가 포함되는 오버레이 계층 및 해당 오버레이 계층이 포함하는 처리능력 범위를 관리자가 설정하고, chord 방법에 따라 멤버로 조인시킬 수 있다.

<21> 또한, 상기 메시지에 의한 멤버 조인 방법은, 오버레이 네트워크 구성 후, 추가 노드 배치 및 재배치에 의한 동적인 네트워크 환경에서 조인 탐사 메시지 및 조인 응답 메시지에 의해서 멤버 조인을 동적으로 수행하는 방법으로서, 상기 일반노드 중 상기 오버레이 노드로서 조인하고 자 하는 조인의뢰노드는, 자신의 데이터 패킷 처리 용량과 함께 상기 오버레이 노드로서 조인할 것을 요청하는 조인 탐사 메시지를 상기 오버레이 네트워크에 포함된 오버레이 노드들로 전송하고,

<22> 상기 조인 탐사 메시지를 전송받은 오버레이 노드들은 자신의 데이터 패킷 처리 용량과 자신이 소속된 오버레이 네트워크 계층에 대한 정보를 포함하는 조인 응답 메시지를 상기 조인의뢰노드로 전송하며, 상기 조인의뢰노드는, 상기 조인 응답 메시지를 참조하여 조인할 오버레이 네트워크 계층을 결정하고, 상기 결정한 오버레이 네트워크 계층에 포함된 오버레이 노드들로 조인 요청 메시지를 전송함으로써 새로운 오버레이 노드로 조인할 수 있다.

<23> 한편, 상기 조인의뢰노드는, 조인 응답 메시지에 포함된 오버레이 노드들의 데이터 패킷 처리 용량을 참조하여, 자신의 데이터 패킷 처리 용량과 같거나 작은 값을 가진 노드가 속한 네트워크 계층을 조인할 네트워크 계층으로 결정할 수 있다.

<24> 또한, 상기 조인 요청 메시지를 수신한 오버레이 노드들은, 상기 수신한 조인 요청 메시지를 참조하여 Chord 프로토콜에 따라 자신들의 오버레이 라우팅 테이블을 갱신할 수 있다.

<25> 한편, 상기 조인의뢰노드가, 조인할 것으로 결정한 네트워크 계층의 상위 또는 하위 계층에 속한 오버레이 노드와 연결되어 있는 경우, 상기 조인 요청 메시지에 상기 조인의뢰노드의 계층 정보 및 연결정보가 포함된다.

<26> 또한, 상기 차단 노드는 상기 오버레이 동작 모드하에서 데이터 패킷을 라우팅할 수 있다.

<27> 한편, 상기 차단 노드 집합은, DDoS 공격을 탐지한 노드들, 공격 트래픽 방향으로 DDoS 공격에 의해 희생된 희생자 노드에 연결된 노드들, 및 희생자 노드들과 같은 레벨의 노드들로 이루어진 것으로 결정될 수 있다.

<28> 본 발명의 또 다른 실시예에 따른 계층적 오버레이 네트워크 시스템을 이용한 DDoS 공격 대항 방법은, 오버레이 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 오버레이 동작모드와 일반 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 일반동작모드를 가진 적어도 하나의 오버레이 노드를 포함하고, 상기 일반노드와 오버레이 노드는 복수의 계층적으로 구조로 이루어진 오버레이 네트워크를 구성하는 단계; 상기 일반 노드 또는 상기 오버레이 노드가 DDoS 공격을 탐지하는 단계; 상기 DDoS 공격이 탐지되면, 상기 오버레이 노드를 오버레이 동작모드에서 동작하도록 제어하는 단계; 를 포함하며, 상기 오버레이 동작모드에서, 상기 오버레이 노드는 DDoS 공격을 우회하도록 라우팅할 수 있다.

<29> 한편, 상기 오버레이 노드는 DDoS 공격을 탐지하면 상기 오버레이 동작모드하에서 상기 DDoS 공격의 피해를 받았다는 것을 나타내는 공격 탐지 메시지를 상기 최상위 대응 시스템에 통지할 수 있다.

<30> 또한, 상기 오버레이 네트워크는 일반 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 일반동작모드를 가진 일반노드를 더 포함하고, 상기 일반노드는 DDoS 공격을 탐지하면 자신에게 인접한 오버레이 노드 중 상기 DDoS 공격의 피해를 받지 않은 오버레이 노드로 상기 DDoS 공격의 피해를 받았다는 것을 나타내는 공격 탐지 메시지를 통지하고, 상기 일반 노드로부터 상기 공격 탐지 메시지를 통지받은 오버레이 노드는, 통지받은 상기 공격 탐지 메시지를 상기 오버레이 동작모드하에서 상기 최상위 대응 시스템에 통지할 수 있다.

<31> 한편, 상기 복수의 계층에서 동일 계층에 포함된 오버레이 노드들은 데이터 패킷의 처리 용량이 서로 유사할 수 있다.

<32> 또한, 상기 일반노드 중 상기 오버레이 노드로서 조인하고 자 하는 조인의뢰노드는, 자신의 데이터 패킷 처리 용량과 함께 상기 오버레이 노드로서 조인할 것을 요청하는 조인 탐사 메시지를 상기 오버레이 네트워크에 포함된 오버레이 노드들로 전송하고, 상기 조인 탐사 메시지를 전송받은 오버레이 노드들은 자신의 데이터 패킷 처리 용량과 자신이 소속된 오버레이 네트워크 계층에 대한 정보를 포함하는 조인 응답 메시지를 상기 조인의뢰노드로 전송하며, 상기 조인의뢰노드는, 상기 조인 응답 메시지를 참조하여 조인할 오버레이 네트워크 계층을 결정하고, 상기 결정한 오버레이 네트워크 계층에 포함된 오버레이 노드들로 조인 요청 메시지를 전송함으로써 새로운 오버레이 노드로 조인할 수 있다.

<33> 한편, 상기 조인의뢰노드는, 조인 응답 메시지에 포함된 오버레이 노드들의 데이터 패킷 처리 용량을 참조하여, 자신의 데이터 패킷 처리 용량과 같거나 작은 값을 가진 노드가 속한 네트워크 계층을 조인할 네트워크 계층으로 결정할 수 있다.

<34> 또한, 상기 조인 요청 메시지를 수신한 오버레이 노드들은, 상기 수신한 조인 요청 메시지를 참조하여 Chord 프로토콜에 따라 자신들의 오버레이 라우팅 테이블을 갱신할 수 있다.

<35> 한편, 상기 조인의뢰노드가, 조인할 것으로 결정한 네트워크 계층의 상위 또는 하위 계층에 속한 오버레이 노드와 연결되어 있는 경우, 상기 조인 요청 메시지에 상기 조인의뢰노드의 계층 정보 및 연결정보가 포함될 수 있다.

<36> 또한, 상기 최상위 대응 시스템은, 상기 공격 탐지 메시지를 수신하면, 상향 또는 하향 트래픽이 우회할 차단 노드 집합을 결정하고, 상기 결정한 차단 노드 집합의 정보를 포함한 차단 공지 메시지를 상기 차단 노드 집합에 포함된 차단 노드로 전송하며, 상기 차단 노드는 상기 오버레이 동작 모드하에서 데이터 패킷을 라우팅할 수 있다.

<37> 한편, 상기 차단 노드 집합은, DDoS 공격을 탐지한 노드들, 공격 트래픽 방향으로 DDoS 공격에 의해 희생된 희생자 노드에 연결된 노드들, 및 희생자 노드들과 같은 레벨의 노드들로 이루어진 것으로 결정될 수 있다.

효 과

<38> 이러한 계층적 오버레이 네트워크 시스템 및 이를 이용한 DDoS 공격 대항 방법에 따르면, DDoS 공격 차단 과정에서 사용되는 협동을 위한 제어 트래픽의 빠르고 정상적인 전송 보장 및 공격 발생시 정상 트래픽의 피해 최소화를 할 수 있고, 나아가서 계층적인 네트워크 구조 및 다양한 처리능력의 노드가 존재함을 고려하여 다수의 계층적인 오버레이를 구성하여 오버헤드를 줄일 수 있다.

발명의 실시를 위한 구체적인 내용

<39> 이하, 첨부한 도면들을 참조하여 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다.

<40> 도 2는 본 발명의 일 실시예에 따른 계층적 오버레이 네트워크 시스템을 나타낸 도면이다. 도 3a는 공격 피해 노드가 오버레이 노드일 때 공격 탐지 메시지의 전달 경로를 나타내고, 도 3b는 공격 피해 노드가 일반 노드일 때 공격 탐지 메시지의 전달 경로를 나타낸다.

<41> 도 2를 참조하면, 계층적 오버레이 네트워크 시스템(100)은 최상위 대응 시스템(110)과 다수의 오버레이 노드(121)를 포함하는 계층적 오버레이 네트워크(120)를 포함한다.

<42> 상기 오버레이 네트워크(120)는, 일반 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 일반동작모드를 가진 적어도 하나의 일반노드와, 오버레이 라우팅 테이블을 참조하여 데이터 패킷을 라우팅하는 오버레이 동작모드와 상기 일반동작모드를 가진 적어도 하나의 오버레이 노드를 포함하며, 상기 일반노드와 오버레이 노드는 복수의 계층적으로 구조로 이루어져 있다. 여기에서, 상기 오버레이 동작모드에서, 상기 오버레이 노드는 DDoS 공격을 우회하도록 라우팅 한다.

<43> 상기 최상위 시스템(110)은, DDoS 공격이 탐지되면, 상기 오버레이 노드를 오버레이 동작모드에서 동작하도록 제어한다.

<44> 상기 오버레이 노드는 DDoS 공격을 탐지하는 동작을 수행하며, DDoS 공격을 탐지하면 상기 오버레이 동작모드하에서 상기 DDoS 공격의 피해를 받았다는 것을 나타내는 공격 탐지 메시지를 상기 최상위 대응 시스템에 통지하며, 상기 일반노드는 DDoS 공격을 탐지하는 동작을 수행하여, DDoS 공격을 탐지하면 자신에게 인접한 오버레이 노드 중 상기 DDoS 공격의 피해를 받지 않은 오버레이 노드로 상기 DDoS 공격의 피해를 받았다는 것을 나타내는 공격 탐지 메시지를 통지하고, 상기 일반 노드로부터 상기 공격 탐지 메시지를 통지받은 오버레이 노드는, 통지받은 상기 공격 탐지 메시지를 상기 오버레이 동작모드하에서 상기 최상위 대응 시스템에 통지한다.

<45> 최상위 대응 시스템(110)은 계층적 오버레이 네트워크 시스템(100)에 포함된 모든 노드들을 책임지는 노드로써, 그 위치는 계층적인 오버레이 네트워크 시스템(100)의 일 실시예와 다를 수 있다. 최상위 대응 시스템(110)은 기 설정된 탐지 메커니즘을 통해 각 노드에서 공격을 탐지하도록 지시한다.

<46> 공격 탐지 방법에는 예를 들어, 중간 노드들이 네트워크 구성정보를 이용해 패킷의 송수신 IP 주소를 검사하거나 송신자의 IP 주소와 MAC 주소의 변화율을 감시하는 방법(Mihui Kim, Kijoon Chae, “Detection and Identification Mechanism against Spoofed Traffic Using Distributed Agents,” ICCSA2004, LNCS 3043, pp.673-682, May, 2004.), 또는 데이터 마이닝 방식을 이용하여 정상적인 트래픽 패턴을 구성하고, 이를 이용해 트래픽 패턴을 검사하는 방법(Mihui Kim, Hyunjung Na, Kijoon Chae, Hyochan Bang, Jungchan Na, “A Combined Data Mining Approach for DDoS Attack Detection,” ICOIN2004, LNCS 3090, pp.943- 950, Feb., 2004) 등이 있다. 이외에도, 네트워크의 중간 노드들에서 분산 공격 탐지를 수행하는 다른 방법을 사용할 수 있다.

<47> 공격 탐지 노드는 상기에서 제시한 공격 탐지 방법을 이용하여 특정 노드에서 공격이 발생하였는지 판단하고, 공격 탐지 메시지를 최상위 대응 시스템(110)으로 전달한다. 예를 들면, 공격 탐지 노드는 자신이 속한 오버레이 계층에서 상위 계층에 연결된 다음 노드(H_TB)에게 자신의 핑거 테이블(라우팅 테이블)을 이용하여 공격 탐지 메시지를 전달하며, 공격 탐지 메시지를 전달 받은 H_TB 노드는 자신에 연결된 상위 계층 노드에게 수신한 메시지를 전달하고, 이를 수신한 노드도 마찬가지로 자신의 H_TB 노드에게 해당 메시지를 전달하게 된다. 이 과정을 반복하여 최상위 대응 시스템(110)에게 해당 공격 탐지 메시지를 전달한다.

<48> 공격 탐지 메시지에는 공격 탐지 노드 정보(IP 주소, 오버레이 계층), 공격 피해 노드에 대한 정도(IP 주소, 있다면 오버레이 계층), 공격 탐지 노드와 공격 피해 노드와의 관계에 대한 정보(상/하, 하/상, 동일계층), 탐지 노드의 주변 노드 정보(상, 하, 또는 동일계층으로 연결된 정보) 등이 저장된다.

<49> 상술한 공격 탐지노드는 제안된 오버레이 구조에서 오버레이노드로 가정하고, 희생자 또는 피해(victim) 노드는 오버레이노드일 수도 아닐 수도 있다. 첫 번째 희생자노드가 오버레이노드인 경우, 탐지노드는 자신이 만든 공격 탐지 메시지를 상위 계층에 연결된 다음 노드(H_TB)로 공격 탐지 메시지를 전달하여 상술한 메커니즘 대로 계층 오버레이를 거쳐 최상위 대응 시스템에게 공격 탐지 메시지를 전달한다. 두 번째 희생자노드가 오버레이노드가 아닌 경우, 자신이 감지한 희생자노드의 정보(IP 주소)와 함께 공격 탐지노드의 정보를 담아 공격 탐지 메시지를 계층 오버레이를 거쳐 최상위 공격 차단노드에게 전송한다. 후술하는 도 3a 와 도 3b는 탐지노드가 희생자노드를 탐지한 경우 최상위 대응 시스템에 공격 탐지 메시지를 전달하는 경로를 예시하였다.

<50> 도 3a 및 도 3b에서는, 공격 탐지 노드를 오버레이 노드(121)로 가정하고, 공격 피해 노드를 오버레이 노드(121)이거나 일반 노드(131)인 경우로 구분하여 설명한다.

<51> 도 3a를 참조하면, 공격 피해 노드가 오버레이 노드(121)일 때 공격 탐지 노드는 공격 탐지 메시지를 상위 오버레이 네트워크에 연결된 다음 노드로 전달하는 메카니즘을 이용하여 최상위 대응 시스템(110)으로 전달한다. 도 3b에 도시된 바와 같이, 공격 피해 노드가 일반 노드(131)일 때 공격 탐지 노드는 계층적 오버레이 네트워크(120)를 거쳐 공격 탐지 메시지는 최상위 대응 시스템(110)으로 전달한다.

<52> 최상위 대응 시스템(110)는 이와 같이 전달된 공격 탐지 메시지를 근거로 하여 공격 피해 노드의 위치를 판단하고, 공격 피해 노드가 탐지되면, 공격 피해 노드를 우회할 수 있도록 차단 노드 집합을 설정한다. 이후, 최상위 대응 시스템(110)은 차단 노드의 구성 정보와 공격 피해 노드에 대한 정보를 포함하는 차단 공지 메시지를 계층적 오버레이 네트워크(120)를 이용하여 차단 노드들로 전송한다. 이와 같은 메시지를 수신한 차단 노드들은 계층적 오버레이 네트워크(120)를 통해 공격 피해 노드를 우회하도록 오버레이 라우팅을 이용하는 오버레이 모드로 동작한다. 공격 피해 노드를 우회한 이후에는 일반 라우팅을 이용하는 일반 모드로 동작한다.

<53> 최상위 대응 시스템(110)에서의 공격 피해노드 및 차단 노드 결정하는 방법에 대하여 상세히 설명한다.

<54> 최상위 대응 시스템은 하나 이상의 공격 탐지 메시지를 수신하면, 이 메시지에 담긴 탐지 정보를 근거로 희생자 노드 및 공격 유형, 실제 공격 트래픽을 차단하고 정상 트래픽을 우회시킬 차단노드 집합을 선정한다. 희생자 노드 또는 지역에 대한 정보를 수집한 최상위 대응 시스템은 희생자노드 및 지역을 판단한다(희생자노드 집합 = x | 희생자노드 x $\in \forall ADM$)(여기서: ADM은 공격 탐지 메시지). 이때, 희생자노드는 공격 트래픽 방향(상향/하향)에 상관없이 아예 라우터의 기능을 멈춘 경우(강한 공격)와 특정 공격 트래픽 방향에 의해 희생자 노드의 특정 인터페이스만이 원활한 전송을 할 수 없는 경우(약한 공격)로 나누어 볼 수 있다. 아래 표 1과 같이 전자의 경우, 탐지 노드의 위치는 희생자 노드를 중심으로 상위/하위/동일 계층일 것이며, 후자의 경우에는 상위/동일 계층 또는 하위/동일 계층에서의 탐지노드가 공격 탐지 메시지를 전달할 것이다. 이러한 탐지 노드와 희생자 노드와의 관계 분석에 의해 전자의 경우에는 희생자 노드 혹은 지역을 전체적으로 우회할 수 있도록 상/하향 트래픽을 우회할 차단노드 집합을 결정하고, 후자의 경우에는 특정 방향(상향 혹은 하향)의 트래픽을 우회할 수 있도록 차단노드 집합을 결정한다.

표 1

<55>

```
if ((minD_layer ≥ maxV_layer ) or (DV_rel ⊆ UD, S))
        AttackType = Weak_Down
else if ((maxD_layer ≤ minV_layer ) or (DVrel ⊆ DU, S))
        AttackType = Weak_Up
else
        AttackType = Strong
```

■ $minD_{layer}/maxD_{layer}$: 탐지노드 집합의 오버레이 계층 최소값/최대값
■ $minV_{layer}$ /$maxV_{layer}$: 희생자노드 집합의 오버레이 계층 최소값/최대값
■ DV_{rel} : 탐지노드와 희생자노드의 연결 관계 집합 (UD: 상하, DU: 하상, S: 동일)
■ AttackType : 공격유형 (Strong: 강한 공격,
Weak_Down : 하향 공격 트래픽에 의한 약한 공격
Weak_Up: 상향 공격 트래픽에 의한 약한 공격)

<56> 본 발명의 일 실시예에 따르면, 공격 탐지 메시지들 정보에 의해 희생자노드 집합과 공격 유형이 결정되면, 최상위 대응 시스템은 아래의 표 2의 원칙으로 차단노드 집합을 결정할 수 있다.

표 2

<57>

차단노드 집합 = 탐지노드들, 공격 트래픽 방향으로 희생자노드에 연결된 노드들, 희생자노드와 같은 레벨의 노드들

<58> 차단노드 집합을 결정한 후, 최상위 대응 시스템(110)은 계층적인 오버레이 네트워크를 통해 차단노드 구성 정보와 희생자노드 집합의 정보(IP 주소, 계층 정보 등)를 포함한 차단 공지 메시지(Defense Notification Message, DNM)를 차단노드 집합에게 전송한다. 이를 수신한 차단노드 집합은 정상 트래픽으로 판단되는 트래픽을 그림 4에서처럼 오버레이 네트워크를 이용하여 공격 피해 지역을 우회한다. 즉, 상향공격인 경우 피해 지역을 피해 오버레이의 한 계층 위로 패킷을 우회시킨 뒤, 그 뒤의 경로는 일반 라우팅을 이용하도록 하고, 마찬가지로 하향공격인 경우에도 피해 지역을 피해 오버레이의 한 계층 아래로 패킷을 우회시킨 뒤 그 뒤의 경로는 일반 라우팅을 이용하도록 한다. 특히 그림 4a에서의 노드(1)처럼 희생자노드와 같은 레벨의 차단노드들은 자신에게 연결된 일반노드(노드(2))들의 트래픽을 자신을 통해 우회할 수 있도록 일반 라우팅 프로토콜을 사용하여 트래픽을 우회시킨다. 그림 4a와 도 4b와는 달리 공격유형이 Strong인 경우에도 비슷한 원칙대로 차단노드 집합을 결정하여 상/하향 정상 트래픽을 오버레이 네트워크를 통해 우회시킬 수 있다.

<59> 도 2에서의 최상위 대응 시스템(110)은 가장 높은 오버레이 네트워크에 연결되어 있고 그 개수는 한 개이지만, 이에 제한되는 것은 아니며, 최상위 대응 시스템(110)의 위치 및 개수는 변화될 수 있다.

<60> 다시 도 2를 참조하면, 계층적 오버레이 네트워크(120)는 최상위 대응 시스템(110)으로부터 계층적으로 분할되고, 최상위 대응 시스템(110)은 계층적 오버레이 네트워크(120) 중 최상위 오버레이 네트워크(120a)와 연결된다. 각 오버레이 네트워크(120a, 120b, 120c)에는 서로 논리적으로 연결된 다수의 오버레이 노드(121)를 구비한다. 여기서, 논리적으로 연결된다는 것은 물리적으로 연결된 것을 배제하지 않는다. 즉, 각 오버레이 노드(121)는 인접한 오버레이 노드와 직접적으로 연결되거나 또는 일반 노드(131)를 통해 연결될 수 있다.

<61> 여기서, 오버레이 네트워크의 예를 들면 P2P(Peer to Peer) 네트워크에서 데이터 공유를 위한 네트워크 구조(Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek, Hari Balakrishnan, “Chord: A Scalable Peer to peer Lookup Service for Internet Applications,” SIGCOMM’01, pp.149-160, Aug., 2001; M. Kaashoek, D. Karger, “Koorde: A Simple Degree Optimal Distributed Hash Table,” Second Int’l Workshop Peer to Peer Systems, Feb., 2003.)일 수 있다.

<62> 한편, 서로 동일한 오버레이 네트워크에 포함되는 오버레이 노드들(121)은 서로 비슷한 처리능력을 갖는 것이 바람직하다. 즉, 계층적 오버레이 네트워크(120)는 처리능력에 따라서 계층적으로 분할된다고 할 수 있다. 하지만, 오버레이 노드들(121)이 비슷한 처리능력을 갖지 않더라도 본원 발명의 목적은 달성될 수 있다. 따라서, 오버레이 노드들(121)이 비슷한 처리능력을 반드시 가질 필요는 없다.

<63> 또한, 계층적 오버레이 네트워크(120)는 서로 인접하는 오버레이 네트워크와 두 개 이상의 오버레이 노드를 통해서 연결된다. 각 오버레이 네트워크 계층에 포함된 두 개 이상의 오버레이 노드는 상위 네트워크 계층으로 패킷을 라우팅하는 하이 오버레이 노드 및 하위 네트워크 계층으로 패킷을 라우팅하는 로우 오버레이 노드를 포함할 수 있다.

<64> 각 오버레이 노드(121)는 공격 피해 노드가 탐지되지 않은 일반 모드로 동작할 때 패킷을 라우팅하기 위하여 이용하는 일반 라우팅 테이블(121a)과 공격 피해 노드가 탐지되어 오버레이 모드로 동작할 때 패킷을 라우팅하기

위하여 이용하는 오버레이 라우팅 테이블(121b)을 구비한다. 한편, 일반 노드는 일반 모드로 패킷을 라우팅하기 위하여 이용하는 일반 라우팅 테이블(131a)만을 구비한다.

<65> 도 5는 하나의 오버레이 네트워크를 형성하는 오버레이 노드들과 각 오버레이 노드에 이용되는 오버레이 테이블의 구조를 나타낸 도면이다.

<66> 도 5를 참조하면, 하나의 오버레이 네트워크는 다수의 오버레이 노드를 포함한다. 여기서, 오버레이 네트워크의 크기는 2^m으로 정의되고, m은 1 이상의 정수로 이루어진다. 도 5에서는 m은 최대 5의 값을 갖고, 그 결과 도 5에 도시된 오버레이 네트워크는 최대 32개의 오버레이 노드를 구비할 수 있다.

<67> 도 5에서는 제7 오버레이 노드(N7) 및 제16 오버레이 노드(N16) 각각의 제7 및 제16 오버레이 라우팅 테이블(N7-1, N16-1)이 도시된다.

<68> 도 5에 도시된 바와 같이, 제7 및 제16 오버레이 라우팅 테이블(N7-1, N16-1) 각각의 첫번째 블럭인 스타트 블럭(FB)에는 "자기 노드번호+2^m"이 저장되고, 여기서, m은 0부터 4까지의 자연수이다. 제7 및 제16 오버레이 라우팅 테이블(N7-1, N16-1) 각각의 두번째 블럭(SB)인 목적지 블럭에는 목적지 노드에 대한 번호가 저장된다. 목적지 블럭(SB)에는 예를 들어, [8, 9), [9,11)등의 형태로 번호가 저장된다. 여기서, [8, 9)는 8은 포함하고, 9는 포함하지 않는다는 것을 뜻하고, [9,11)는 9, 10은 포함하고, 11은 포함하지 않는다는 것을 뜻한다.

<69> 마지막으로, 제7 및 제16 오버레이 라우팅 테이블(N7-1, N16-1) 각각의 세번째 블럭(TB)인 다음 노드 블럭에는 이동할 다음 노드의 번호가 저장된다. 예를 들어, 제7 오버레이 라우팅 테이블(N7-1)에 따르면, 목적지 노드의 번호가 8인 경우에는 10번 노드로 이동하고, 목적지 노드의 번호가 11, 12, 13, 또는 14인 경우에는 12번 노드로 이동한다. 예를 들어, 제16 오버레이 라우팅 테이블(N16-1)에 따르면, 목적지 노드의 번호가 17인 경우에는 17번 노드로 이동하고, 목적지 노드의 번호가 20, 21, 22, 또는 23인 경우에는 22번 노드로 이동한다.

<70> 오버레이 라우팅 테이블은 일반 라우팅 테이블과는 다르게 오버레이 노드들의 번호가 저장되어 있어서, 각 오버레이 노드는 대응하는 오버레이 라우팅 테이블을 참조하여, 패킷에 저장된 목적지 번호에 따라서 라우팅할 다음 오버레이 노드의 번호를 선택할 수 있다. 이로써, 공격 피해 노드를 우회하기 위하여, 오버레이 노드들로만 이루어진 계층적 오버레이 네트워크를 이용하여 패킷을 라우팅할 수 있다.

<71> 도 5에서 예시적으로 설명한 오버레이 라우팅 테이블은, Chord 프로토콜에 의해 정의된 테이블이다.

<72> Chord 프로토콜은 P2P 네트워크에서 데이터가 저장된 노드를 찾기 위한 대표적인 분산 라우팅 프로토콜로 일부 노드에 대한 정보, 즉 N 개의 노드로 구성된 네트워크에서 각 노드는 단지 O(logN)의 다른 노드 정보만 저장하고 있으면 되며, 목적지에 도달하기 위해 O(logN)의 메시지 전송이 요구되고, 노드 조인/탈퇴 시 $O(\log^2 N)$ 메시지를 전송하면 모든 노드의 라우팅이 재구성 되는 특징을 갖고 있다.

<73> Chord 라우팅에 대해 자세히 설명하면, 각 노드는 [0, 2^{m-1}] 범위에서 해쉬 함수에 의해 노드 아이디를 할당받고, 각 노드들은 개념적으로 노드 아이디에 의해 도 5에서처럼 한 사이클을 구성하고 있다. 오버레이 네트워크에 조인된 각 노드 x는 핑커 테이블이라는 m개의 다른 노드에 대한 라우팅 정보를 저장하고 있고, 각 라우팅의 i번째 정보는 노드 아이디 $x+2^{i-1} (\mathrm{mod}\ 2^m)$ 대한 가장 가까운 다음 오버레이노드에 대한 정보이다. 상술한 바와 같이, 도 5의 7번 오버레이노드의 핑거 테이블을 설명하면, Interval("SB"로 표시함) [8,9) 즉 8번 노드를 책임지는 노드는 successor 노드("TB"로 표시함)인 10번 노드가 되고, Interval [9,11) 즉 9,10번 노드를 책임지는 노드도 역시 successor 노드인 10번 노드이므로 이 Interval에 포함되는 노드로의 패킷은 10번 노드에게 전송된다. 패킷 라우팅 방법은 노드 x가 노드 y로 향하는 패킷을 수신하면, y가 포함되는 Interval 값을 갖는 라우팅 엔트리의 후위자(successor) 노드로 전송하면 된다. 후위자 노드란 그 패킷을 책임지고 있는 대표 노드를 말한다. 예를 들어 도 5에서 노드 7이 20으로 향하는 패킷을 수신했을 때 20은 Interval [15,23)에 포함되므로 노드 16으로 전송하고, 이를 수신한 노드 16에서는 패킷 20으로 향하는 패킷은 Interval [20,24)에 포함되므로 노드 22에게 전송한다. 노드 22는 20이 자신의 ID 번호보다 작으므로 자신이 이 패킷을 책임져야 할 목적지임을 알게 된다.

<74> 이제, 계층적 오버레이 구성에 대하여 설명한다. 본 발명에 따른 계층적 오버레이 구성은 아래와 같은 특징을 가지고 있다.

<75> ■ 공격 탐지 후, 최상위 대응 시스템에 탐지 정보의 빠른 전달

<76> ■ 공격 피해 지역의 판단 후, 차단노드를 선정하여 다른 노드의 정상 트래픽 및 제어 트래픽을 빠르게 우회시킴으로써 피해를 최소화

<77> ■ 계층적인 오버레이 구조의 사용으로 관리 비용의 최소화 및 확장성(Scalability) 제공

<78> 본 발명의 일 실시예에 따른 계층적 오버레이 구성은 다수의 Chord 오버레이 네트워크를 이용하여 최상위 대응 시스템으로의 공지 및 정상 트래픽의 우회를 유도하여 공격의 피해를 최소화하는 구조이다. 이를 위해 각 노드의 처리능력(capacity) 및 연결 구조에 따라 적당한 계층의 오버레이 네트워크에 조인하여 계층적인 오버레이 네트워크를 구성한다.

<79> 노드가 오버레이에 조인하여 오버레이 네트워크의 멤버로 구성되기 위한 방법은 두 가지로 관리자의 설정에 의한 멤버 조인과 메시지에 의한 멤버 조인으로 수행될 수 있다. 오버레이 구성 초기에는 각 노드의 오버레이 계층 및 해당 오버레이 계층이 포함하는 처리능력 범위 등을 설정하여 멤버로 조인하는 관리자 설정에 의한 조인 방법을 사용할 수 있다. 관리자 설정에 의한 조인 방법은, 관리자가 해당 정보를 설정한 후 멤버로 조인시키며 예를 들어 Chord 방법을 활용한다.

<80> 한편 초기 오버레이 네트워크 구성 후, 추가 노드 배치 및 재배치에 의한 동적인 네트워크 환경에서는 조인 탐사 메시지 및 조인 응답 메시지에 의해서 멤버 조인이 동적으로 수행된다. 이하에서, 도 6을 참조하여 동적으로 노드가 조인되는 과정을 설명한다.

<81> 도 6은 오버레이 네트워크에 노드가 조인되는 과정을 나타낸 도면이다.

<82> 도 6을 참조하면, 조인하고자 하는 새로운 노드(n_{new})("조인의뢰노드"라고도 함)는 자신의 용량(capacity)을 담은 조인 탐사 메시지를 주변노드에게 브로드케스팅한다. 상기 주변노드라 함은 자신과 직접 연결된 상, 하위노드들과 이더넷과 같은 매체 공유 네트워크에 연결된 경우, 브로드케스트로 전달될 수 있는 이웃 노드들을 칭한다. 각 오버레이 노드(n_{ij}, $n_{i(j+1)}$, $n_{(i+1)j}$)는 조인 탐사 메시지를 수신하면, 자신의 용량과 자신이 소속된 오버레이 네트워크 계층에 대한 정보를 포함하는 조인 응답 메시지를 조인하고자하는 새로운 노드(n_{new})로 전송한다. 여기에서 오버레이 노드 n_{ij}는 i번째 오버레이 네트워크의 j 노드를 나타내고, 오버레이 노드 $n_{(i+1)j}$는 (i+1)번째 오버레이 네트워크의 j 노드를 나타내며, 최상위 계층의 오버레이 네트워크가 1번째 오버레이 네트워크이다. 새로운 노드(n_{new})는 조인 응답 메시지를 참고하여 조인하고자 하는 오버레이 네트워크 계층을 결정한다. 만약, 새로운 노드(n_{new})는 일정 시간 내에 조인 응답 메시지를 수신하지 못하면, 조인 탐사 메시지를 최상위 대응 시스템에 직접전달 할 수 있다.

<83> 또한, 새로운 노드(n_{new})는 조인 응답 메시지에 포함된 용량에 따라서 자신이 조인될 오버레이 네트워크 계층을 결정한다. 본 발명의 일 실시예에 따른 오버레이 네트워크 계층 결정방법을 표 3을 참조하여 설명한다.

표 3

<84>

if ($Capacity_i \le Capacity_{new} < Capacity_{(i+1)}$)	$Level_{new} = Level_i$
else if ($Capacity_1 \ge Capacity_{new}$)	$Level_{new} = Level_1$
else if ($Capacity_K \le Capacity_{new}$)	$Level_{new} = Level_K$
■ n_i ($1 \le i \le K$, K : 조인응답메시지를 보낸 노드 개수)	
■ $Capacity_i$: 노드 n_i의 용량 (용량으로 오름차순 정렬하여 $Capacity_i \le Capacity_{(i+1)}$ 임)	
■ $Level_i$: 노드 n_i의 오버레이 계층	
■ $Capacity_{new}$: 새로 조인하는 노드의 용량	
■ $Level_{new}$: 새로 조인하는 노드의 결정된 레벨	

<85> 즉, 수신된 조인 응답 메시지의 용량을 정렬시켜, 자신의 용량이 포함되는 구간을 결정하고, 자신의 용량이 포함되는 구간이 존재하는 경우, 그 구간이 자신의 용량과 같거나 작은 값을 조인 응답 메시지로 보낸 노드들이 속하는 계층을 자신의 계층으로 결정한다. 또는, 자신의 용량이 포함되는 구간이 없고, 수신된 조인 응답 메시지의 모든 용량이 자신의 용량보다 작다면, 가장 작은 용량을 조인 응답 메시지로 보낸 계층을 자신의 계층으로 결정한다. 반대로, 자신의 용량이 포함되는 구간이 없고, 수신된 조인 응답 메시지의 모든 용량이 자신의 용량

보다 크면, 가장 큰 용량을 조인 응답 메시지로 보낸 계층을 자신의 계층으로 결정한다.

<86> 이와 같은 방식으로, 자신의 오버레이 네트워크 계층을 결정하면, 새로운 노드(n_{new})는 결정된 오버레이 네트워크 계층에 소속된 오버레이 노드들(n_{ij}, $n_{i(j+1)}$)에 조인 요청 메시지를 전송한다. 이때, 조인 과정은 상술한 바 있는 도 5와 같은 Chord 프로토콜에 따라서 이루어질 수 있다.

<87> 한편, 조인하고자 하는 새로운 노드(n_{new})가, 조인할 네트워크 계층의 상위(High) 계층의 오버레이와 이미 연결되어 있거나, 하위(Low) 계층의 오버레이 노드와 이미 연결되어 있는 상태라면, 조인 요청 메시지에, 자신의 계층정보 및 연결 정보를 함께 전송한다. 상기한 오버레이 네트워크 계층에 이미 소속된 오버레이 노드들(n_{ij}, $n_{i(j+1)}$)은 새로운 노드(n_{new})로부터 제공된 계층 정보 및 연결 정보를 근거로 하여 자신이 가지고 있는 정보, 예를 들어, 이전 노드에 대한 정보, 오버레이 라우팅 테이블, 상위 계층에 직접 연결되는 동일 계층의 다음 노드(H_TB) 및 하위 계층에 직접 연결되는 동일 계층의 다음 노드(L_TB) 등을 갱신한다. H_TB/L_TB 노드는 자신을 포함하여 링이 시계방향으로 돌아갈 때 상위/하위 오버레이노드와 연결이 존재하는 첫 번째 노드이다. 상기와 같은 과정을 거쳐서, 조인 과정이 완료된다. 한편, 도 6에서, 설명되지 않은 도면부호 'N_i' 및 'N_{i+1}'은 일반노드를 나타낸다.

<88> 상위 오버레이 노드와 하위 오버레이 노드가 존재하는 경우에, 조인과정을 상세히 설명한다.

<89> 조인 과정은 1) 새로이 조인하고자 하는 노드 n_{new}의 이전 노드(predecessor)와 핑거 테이블(라우팅 테이블을 의미함) 및 상/하위 계층에 연결된 다음 노드를 구성하고, 2)노드 n_{new}의 추가로 인해 영향을 받는 기존 노드들의 이전 노드와 핑거테이블, H_TB/L_TB를 조정한다. 이때, 이전 노드와 핑거 테이블을 구성하는 방법은 Chord 프로토콜에 따른다. 한편, 계층적인 오버레이 구성을 위해 추가적으로 관리되는 상/하위 계층의 노드에 직접 연결이 존재하는 동일 계층의 다음 노드를 구성하는 방법은 다음과 같다.

<90> 새로이 조인하고자 하는 노드 n_{new}에서 송신한 조인 요청 메시지에 포함된 상/하위 계층에 연결된 노드 정보(H_TB/L_TB)가 있는 경우, 기존 노드 n_{*x}(임의 계층의 x 노드)들은 자신이 갖고 있는 상/하위 다음 노드 정보(H_TB_x/L_TB_x)와 비교하여 자신을 기준으로 시계방향 순번에서 먼저 있는 경우, 즉 H_TB_x> new > x 또는 L_TB_x> new > x인 경우, 자신의 정보를 갱신한다. 도 7과 도8을 참조하여, 상위 오버레이 노드와 하위 오버레이 노드가 존재하는 경우에, 조인과정을 설명한다.

<91> 도 7은 새로운 노드가 조인되기 이전 오버레이 네트워크에 포함된 오버레이 노드의 오버레이 라우팅 테이블을 나타낸 도면이고, 도 8은 새로운 노드가 조인된 후 갱신된 오버레이 라우팅 테이블을 나타낸 도면이다.

<92> 도 7에 도시된 오버레이 네트워크의 크기를 결정하는 상수 m은 3이고, 따라서, 상기한 오버레이 네트워크에는 최대 8개의 오버레이 노드가 구비될 수 있다. 도 7에 도시된 바와 같이, 오버레이 네트워크에는 연결되는 오버레이 노드는 제 0 오버레이 노드(N0), 제1 오버레이 노드(N1) 및 제3 오버레이 노드(N3)로 이루어진다. 여기서, 제1 오버레이 노드(N1)는 상위 계층에 연결되는 상위 오버레이 노드이고, 제3 오버레이 노드(N3)는 하위 계층에 연결되는 하위 오버레이 노드이다. 또한, 제2, 제4, 제5, 제6 및 제7 노드(N2, N4, N5, N6, N7)은 일반노드이다.

<93> 도 7에서는, 제0, 제1 및 제3 오버레이 노드(N0, N1, N3)에 대응하는 제0, 제1 및 제3 오버레이 라우팅 테이블(N0-1, N1-1, N3-1)을 제시한다. 제0, 제1 및 제3 오버레이 라우팅 테이블(N0-1, N1-1, N3-1)을 참조하면, 예를 들어 시작 노드가 제0 오버레이 노드(N0)이고, 목적지 노드가 제4 노드(N4)인 경우, 다음 노드는 제0 오버레이 노드(N0)로 나타났다. 또한, 시작 노드가 제1 오버레이 노드(N1)이고, 목적지 노드가 제5 노드(N5)인 경우, 다음 노드는 제0 오버레이 노드(N0)로 나타났다. 뿐만 아니라, 시작노드가 제3 오버레이 노드(N3)이고, 목적지 노드가 제4, 제5, 제6 및 제7 노드(N4, N5, N6, N7)인 경우, 다음 노드는 모두 제0 오버레이 노드(N0)로 나타났다.

<94> 그러나, 도 8에 도시된 바와 같이, 상기한 오버레이 네트워크에 제6 노드(N6)가 조인되고, 상기 제6 노드(N6)가 상위 계층에 연결되는 하이 오버레이 노드로 결정되면, 상기한 제0, 제1 및 제3 오버레이 라우팅 테이블(N0-1, N1-1, N3-1)이 모두 갱신된다.

<95> 도 8을 참조하면, 시작 노드가 제0 오버레이 노드(N0)이고, 목적지 노드가 제4 노드(N4)인 경우, 다음 노드는 제6 오버레이 노드(N6)로 나타났고, 시작 노드가 제1 오버레이 노드(N1)이고, 목적지 노드가 제5 노드(N5)인 경

우, 다음 노드는 제6 노드(N6)로 나타났다. 뿐만 아니라, 시작노드가 제3 오버레이 노드(N3)이고, 목적지 노드가 제4, 제5, 및 제6 노드(N4, N5, N6)인 경우, 다음 노드는 모두 제6 노드(N6)로 나타났다. 즉, 이처럼 제6 노드(N6)가 현 오버레이 네트워크 계층에 추가되면, 기존에 속해 있던 제0, 제1 및 제3 오버레이 라우팅 테이블(N0-1, N1-1, N3-1)이 모두 갱신된다.

<96> 이제, 이하에서는 본 발명의 일 실시예에 따른 오버레이 네트워크 시스템에 대해 오버헤드 분석과 공격 탐지 시 빠른 공격 탐지 전달의 가능성 및 신속성을 분석하고, 마지막으로 오버레이를 이용한 정상 트래픽 우회에 대한 전송률 분석을 통해 본 시스템의 효과를 설명한다.

<97> **<오버헤드 분석>**

<98> 본 발명에서는 공격 탐지 시, 공격 차단에 필요한 제어 트래픽 우회를 통해 빠른 처리를 가능하게 해 주며 정상 트래픽 우회를 통해 DDoS 공격으로 인한 피해를 최소화시키고자 오버레이 네트워크를 구성한다. 이 오버레이 네트워크는 노드의 이질성(heterogeneity) 및 많은 노드 수 지원(scalability)을 위하여 각 노드의 용량(capacity)에 따라 계층적인 오버레이 네트워크를 이용한다. 이 오버레이는 기존의 Chord 오버레이 기본 구성방법을 따르므로 전체 노드 수가 N이라고 했을 때, 멤버 조인 및 탈퇴에 $O(\log^2 N)$이 의 메시지 전송이 필요하며, 이는 실용적인 옵티마이징에 의해 O(logN)으로 구성 오버헤드를 줄일 수 있다(Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek, Hari Balakrishnan, "Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications," SIGCOMM'01, pp.149-160, Aug., 2001.). 본 발명의 일 실시예에 따르면 계층적인 다른 노드 수에 의한 오버레이 네트워크 구조를 가정했으므로 그 구성 오버헤드는 아래의 표 4와 같은 관계식에 의해 하나의 오버레이로 구성하는 경우보다 더 작은 오버헤드를 요구함을 알 수 있고, 여러 개의 오버레이로 구성되는 경우에는 같은 수의 노드로 구성하는 것이 최소의 오버헤드를 요구함을 알 수 있다. 표 4에서 α_i는 β개의 각 오버레이의 노드 수이다. 또한 도 9은 이러한 관계식에 의해 N의 증가에 따른 오버헤드 비교 그림으로 이는 N이 커질수록 계층적인 오버레이의 오버헤드와 하나의 오버레이로 구성될 때의 오버헤드 차이가 증가함을 알 수 있다. 이 그림에서 계층적인 오버레이는 3계층으로 구성되어 있고, 1000개의 노드로 구성된 계층적인 오버레이(1:10:100)인 경우에는 10개의 노드, 100개의 노드, 890개의 노드가 각각의 오버레이로 구성되었을 때의 오버헤드를 도시하였다.

표 4

<99>

하나의 오버레이 구성 ≥ β개의 서로 다른 수의 노드로 구성된 오버레이 구성 ≥ β개의 서로 같은 수의 노드로 구성된 오버레이 구성
$N \cdot \log N \geq \sum_{i=1}^{\beta} \alpha_i \cdot \log \alpha_i \geq \beta \cdot N/\beta \cdot \log(N/\beta)$

<100> **< 공격탐지 전달의 신속성>**

<101> 공격 탐지 시, 제어 패킷의 신속한 전달 가능성을 시뮬레이션 하기 위해 유무선 네트워크 시스템에서 광범위한 네트워크 시뮬레이션을 가능하게 해 주는 Glomosim[GloMoSim (Global Mobile Information Systems Simulation Library), http://pcl.cs.ucla.edu/projects/glomosim/] 시뮬레이터를 사용하여 도 10과 같은 네트워크를 구성하였다. 이는 3개의 계층으로 구성된 오버레이 네트워크를 구성하고 있고, 최상위 대응 시스템은 오버레이 계층 1에 연결되어 있다. 도 10에는 주 라우팅 경로는 실선으로 표시했으며, 한 오버레이 계층에 소속된 노드들 사이에는 간접적인 연결이 존재하고, 오버레이노드가 공격 탐지 시 공격 탐지 메시지를 1초 단위로 5개까지 최상위 대응 노드에게 전달한다고 가정한다. 표 5는 공격 시나리오 및 정상 트래픽에 대한 내용을 설명하고 있다.

표 5

<102>

공격 유형	트래픽
강한 공격 (Strong)	- 5개 Attack Agent 공격트래픽(노드29 -> 노드26), 1ms 주기, 공격시간 10~150s - 5개 Attack Agent 공격트래픽(노드31 -> 노드26), 1ms 주기, 공격시간 10~150s - 정상 트래픽 노드30 ->노드16, 1ms 주기, 트래픽발생시간 0~150s 노드32 ->노드16, 1ms 주기, 트래픽발생시간 0~150s
약한 공격 (weak up)	- 1개 Attack Agent 공격트래픽(노드29 -> 노드26), 1ms 주기, 공격시간 10~150s - 1개 Attack Agent 공격트래픽(노드31 -> 노드26), 1ms 주기, 공격시간 10~150s - 정상 트래픽 : 노드30 -> 노드16, 1ms 주기, 트래픽발생시간 0~150s 노드32 -> 노드16, 1ms 주기, 트래픽발생시간 0~150s

<103> 공격 트래픽, 정상 트래픽이 모두 노드 10의 라우터를 경유하고, 노드 10의 링크 용량이 트래픽에 비해 작다고 설정하여, 노드 10에서 트래픽 과부하로 인한 병목현상이 발생하고 이를 노드 12,13이 탐지하여 공격 탐지 메시지를 오버레이를 통해 최상위 대응 시스템에 전달하게 된다. 예를 들어 12번 노드는 H_TB 노드가 자신이 되므로, 자신에 연결된 상위 오버레이노드 11에게 전달이 되고, 이는 13번 노드도 마찬가지여서 해당 공격 탐지 메시지를 노드 11을 통해 노드 2, 결국 최상위 탐지 시스템인 노드 1에게 전달이 된다. 본 발명에 따른 오버레이 네트워크 시스템을 사용하지 않은 경우(비교예)와 사용하는 경우(본 실시예)에 대하여 공격 탐지 트래픽 전달시간 및 전송률의 결과를 비교하면 표 6과 같다. 실험 결과, 오버레이 감내 구조를 사용하지 않은 경우 공격 탐지 메시지가 희생자 노드를 거쳐야 하므로 전송 손실 가능성을 보여 주었고, 오버레이 감내 구조를 사용하는 경우 공격 탐지 메시지 전달의 높은 가능성 및 속도 향상으로 인해 빠른 공격의 차단 가능성을 입증할 수 있었다.

표 6

<104>

공격유형	전송률		전송시간(Sec)	
	비교예	본 실시예	비교예	실시예
강한 공격	20%	100%	4.139377	0.006121
약한 공격	20%	100%	2.219606	0.006121

<105> **< 정상 트래픽 전송량>**

<106> DDoS 공격 시 정상 트래픽의 전송량을 비교한 결과는 아래의 표 7과 같다. 실험 결과 오버레이 차단 구조를 사용하는 경우 공격 강도에 큰 영향 없이 정상 트래픽 전송량이 제공되므로 공격 피해의 최소화를 가능하게 함을 알 수 있다.

표 7

<107>

공격 유형	비교예	실시예
강한 공격	5639	12364
약한 공격	7771	12364

<108> 이상 본원 명세서에서 언급한 논문들은 본원 명세서의 일부로서 결합됨을 이해하여야 한다.

도면의 간단한 설명

<109> 도 1은 DoS 공격을 받는 종래의 계층적 네트워크 시스템을 나타낸 도면이다.

<110> 도 2는 본 발명의 일 실시예에 따른 계층적 오버레이 네트워크 시스템을 나타낸 도면이다.

<111> 도 3a는 공격 피해 노드가 오버레이 노드일 때 공격 탐지 메시지의 전달 경로를 나타낸 도면이다.

<112> 도 3b는 공격 피해 노드가 일반 노드일 때 공격 탐지 메시지의 전달 경로를 나타낸 도면이다.

<113> 도 4a와 4b는 공격 탐지시 차단 노드 집합에 의한 정당 트래픽 우회를 예시한 도면이다.

<114> 도 5는 하나의 오버레이 네트워크를 형성하는 오버레이 노드들과 각 오버레이 노드에 이용되는 오버레이 테이블의 구조를 나타낸 도면이다.

<115> 도 6는 오버레이 네트워크에 노드가 조인되는 과정을 나타낸 도면이다.

<116> 도 7은 새로운 노드가 조인되기 이전 오버레이 네트워크에 포함된 오버레이 노드의 오버레이 라우팅 테이블을 나타낸 도면이다.

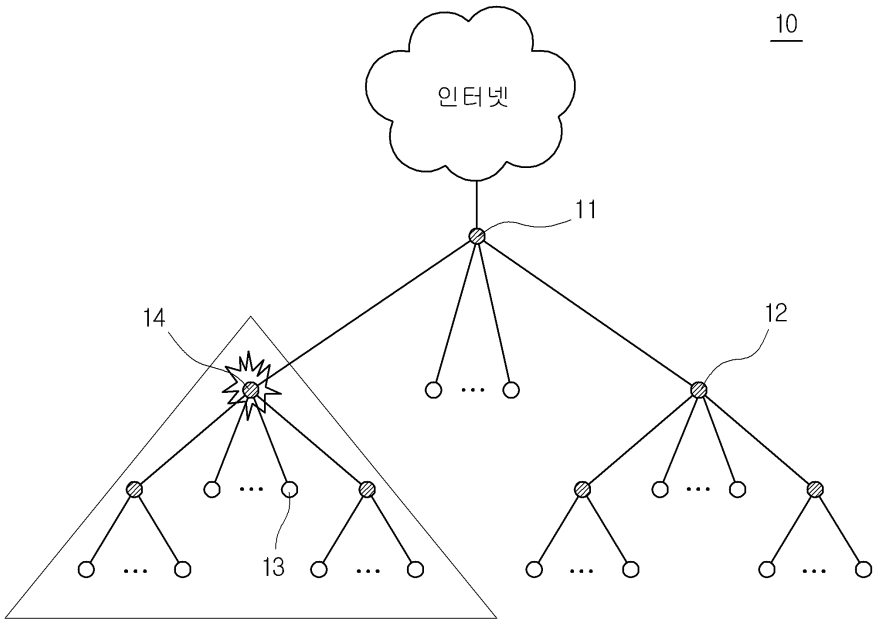
<117> 도 8은 새로운 노드가 조인된 후 갱신된 오버레이 라우팅 테이블을 나타낸 도면이다.

<118> 도 9은 하나의 오버레이 구성과 다수의 계층적인 오버레이 구성에서의 오버헤드 비교한 도면이다.

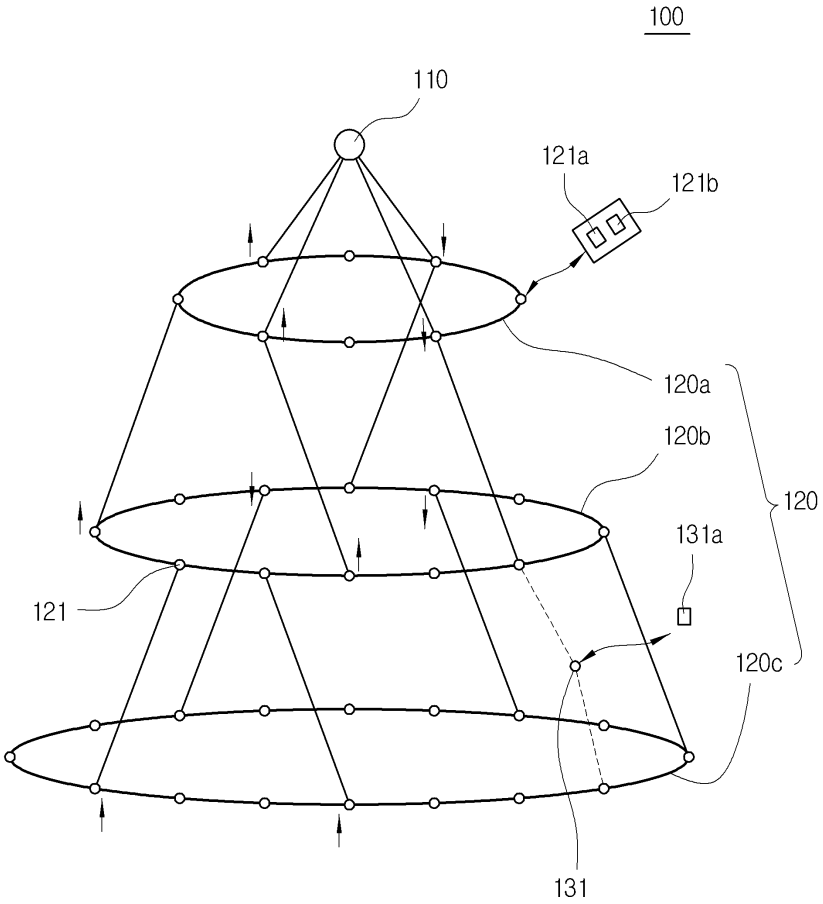
<119> 도 10은 시뮬레이션을 위한 네트워크 구성도를 나타낸 도면이다.

도면

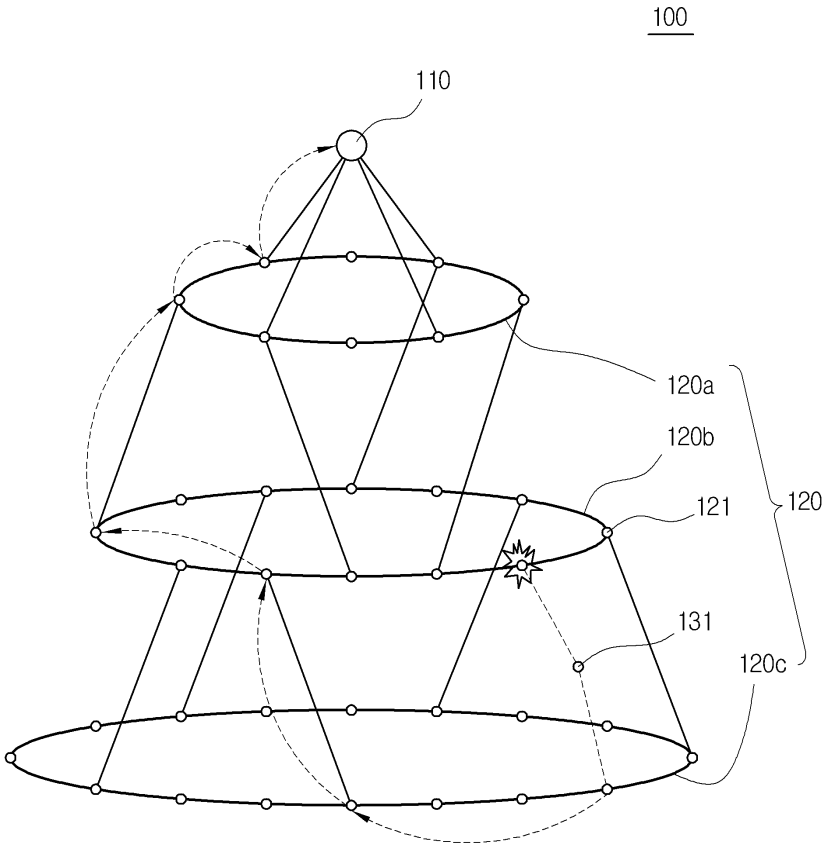
도면1



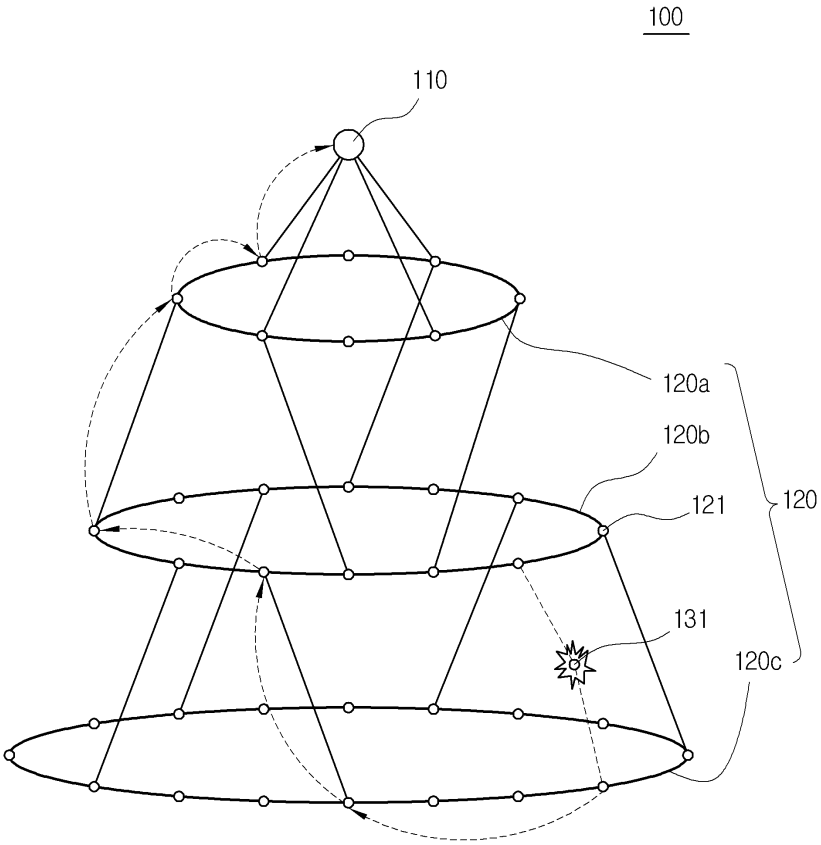
도면2



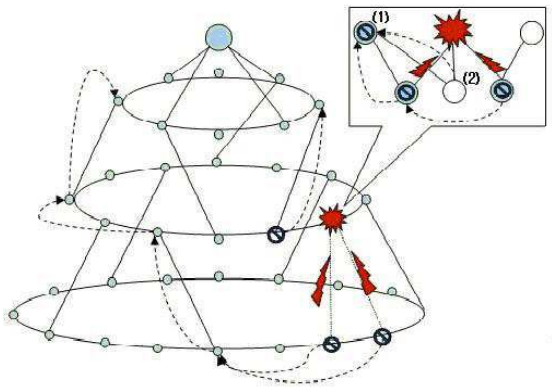
도면3a



도면3b

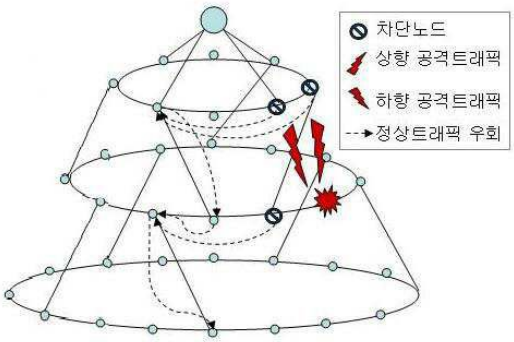


도면4a



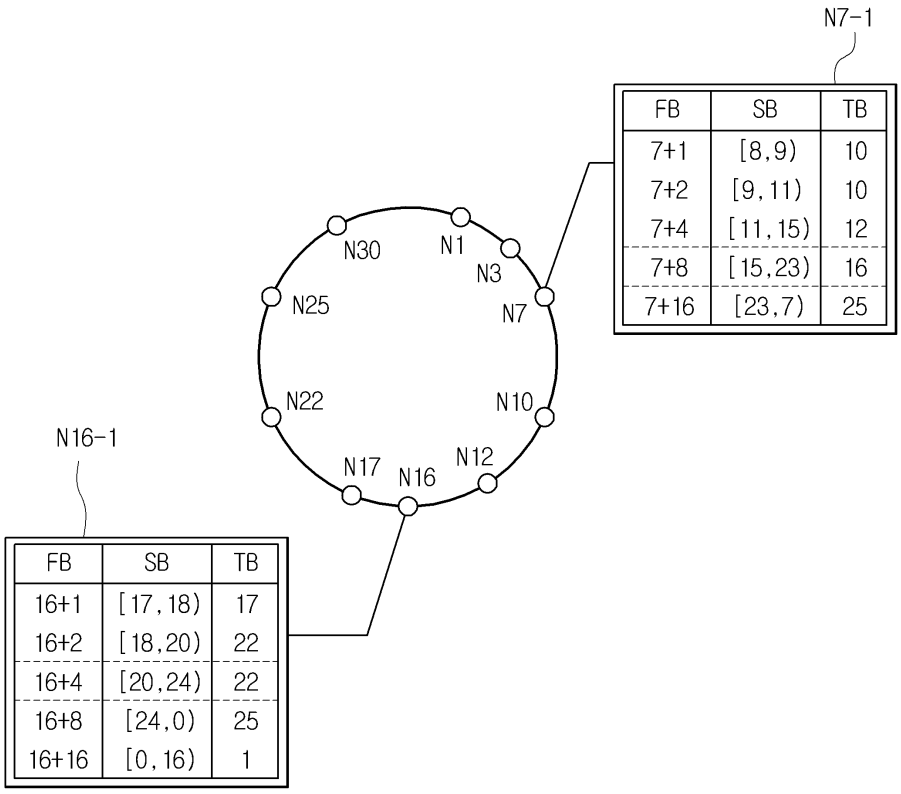
공격유형이 Weak_Up인 경우

도면4b

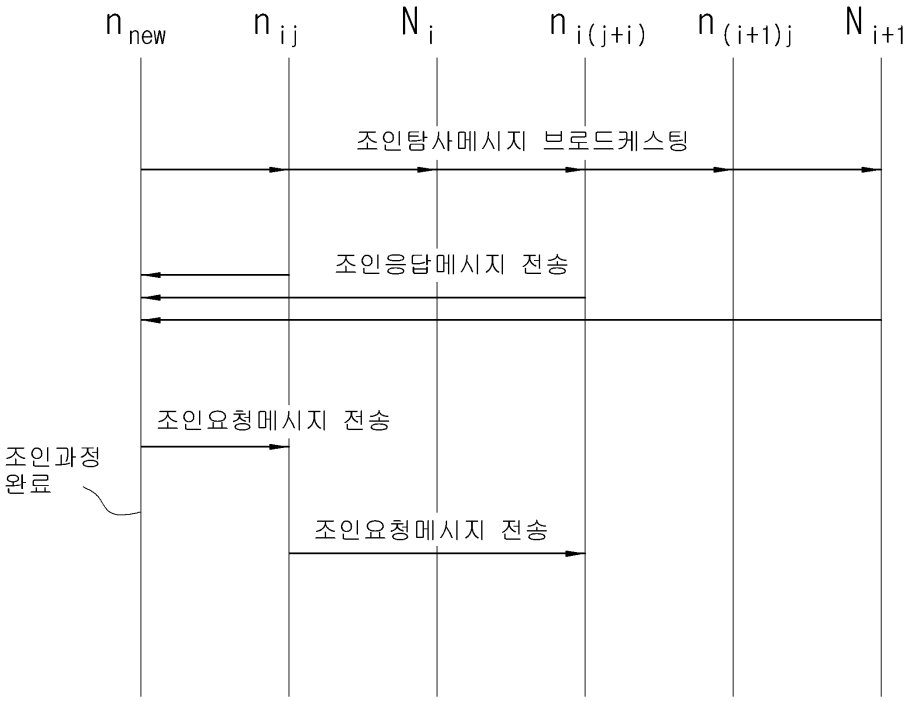


공격유형이 Weak_Down인 경우

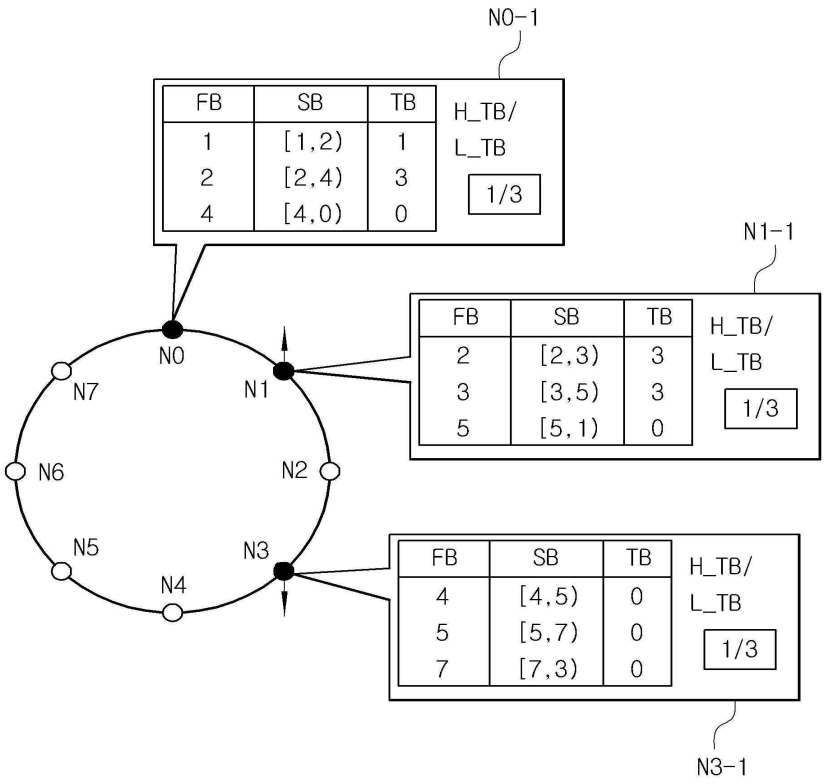
도면5



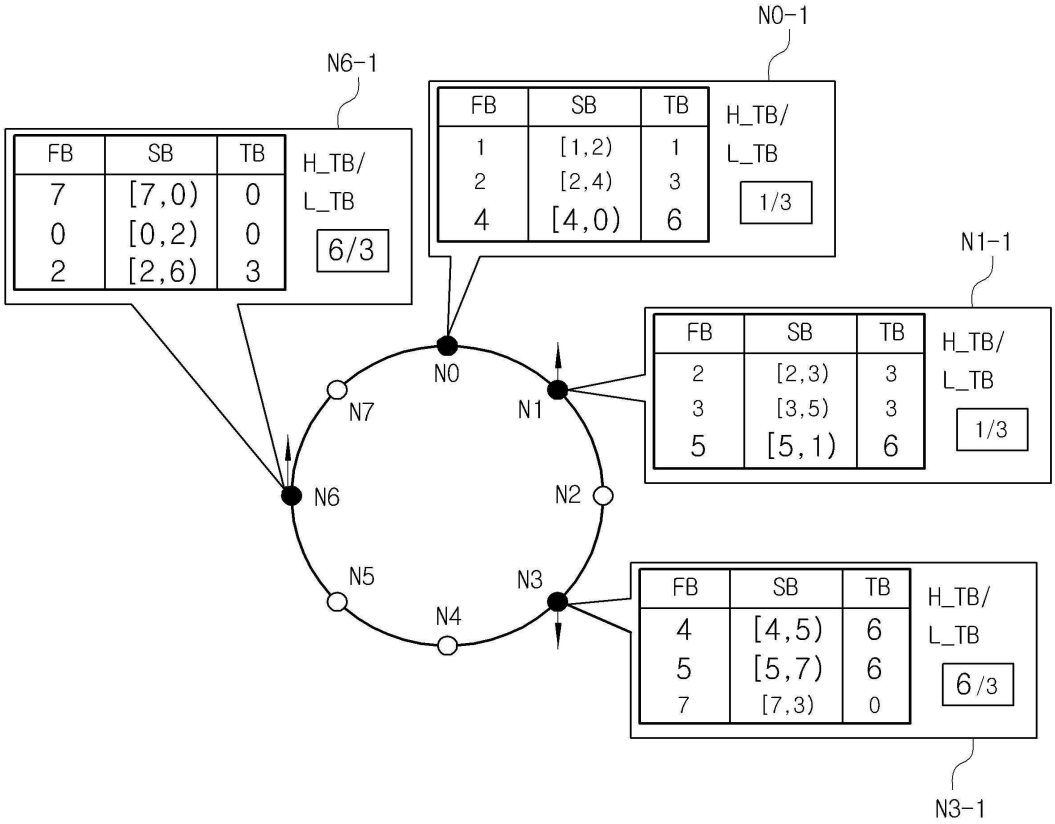
도면6


n new
n ij
N i
n i(j+i)
n (i+1)j
N i+1
조인탐사메시지 브로드케스팅
조인응답메시지 전송
조인요청메시지 전송
조인과정
완료
조인요청메시지 전송

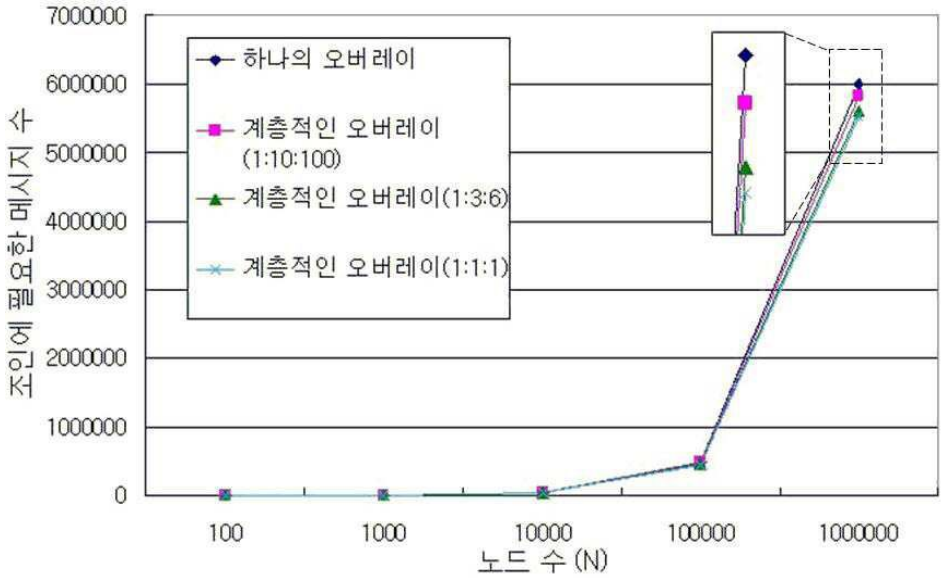
도면7


N0-1
FB SB TB
1 [1,2) 1
2 [2,4) 3
4 [4,0) 0
H_TB/
L_TB
1/3
N1-1
FB SB TB
2 [2,3) 3
3 [3,5) 3
5 [5,1) 0
H_TB/
L_TB
1/3
N0
N1
N2
N3
N4
N5
N6
N7
FB SB TB
4 [4,5) 0
5 [5,7) 0
7 [7,3) 0
H_TB/
L_TB
1/3
N3-1

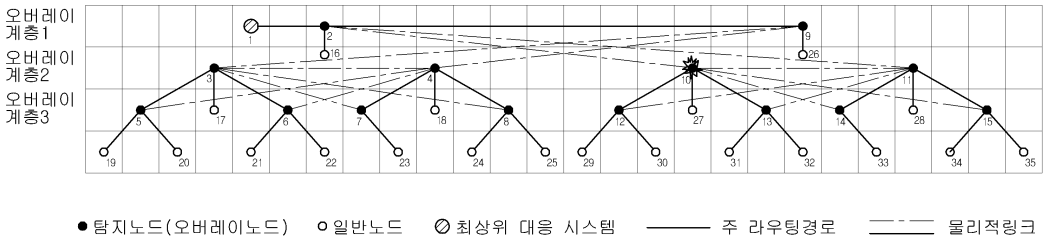
도면8


N0-1
FB SB TB
1 [1,2) 1
2 [2,4) 3
4 [4,0) 6
H_TB/ L_TB
1/3
N6-1
FB SB TB
7 [7,0) 0
0 [0,2) 0
2 [2,6) 3
H_TB/ L_TB
6/3
N1-1
FB SB TB
2 [2,3) 3
3 [3,5) 3
5 [5,1) 6
H_TB/ L_TB
1/3
N3-1
FB SB TB
4 [4,5) 6
5 [5,7) 6
7 [7,3) 0
H_TB/ L_TB
6/3
N0
N1
N2
N3
N4
N5
N6
N7

도면9


하나의 오버레이
계층적인 오버레이 (1:10:100)
계층적인 오버레이(1:3:6)
계층적인 오버레이(1:1:1)
조인에 필요한 메시지 수
7000000
6000000
5000000
4000000
3000000
2000000
1000000
0
100
1000
10000
100000
1000000
노드 수 (N)

도면10



● 탐지노드(오버레이노드) ○ 일반노드 ⊘ 최상위 대응 시스템 ——— 주 라우팅경로 — - — 물리적링크