



(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。 Int. Cl.

H04L 12/22 (2006.01)

H04L 12/24 (2006.01)

(11) 공개번호 10-2007-0071899

(43) 공개일자 2007년07월04일

(21) 출원번호 10-2005-0135741

(22) 출원일자 2005년12월30일

심사청구일자 없음

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 서천동 1 경희대학교 수원캠퍼스내
한국정보사회진흥원
경기 용인시 죽전동 168

(72) 발명자
홍충선
경기 용인시 상현동 성원3차상떼빌 233-101
강명수
서울 광진구 구의3동 587-82
최상현
서울 노원구 월계4동 사슴아파트 303동 1504호

(74) 대리인 특허법인다인

전체 청구항 수 : 총 8 항

(54) I P v 6 네트워크에서 I P 를 역추적하는 방법

(57) 요약

본 발명은 IPv6 네트워크에서 IP를 역추적하는 방법에 관한 것으로, 보다 구체적으로 IPv6의 확장 헤더 중 하나인 홉간 옵션(hop by hop option) 헤더에 저장되어 있는 라우터의 마킹 정보를 이용하여 IP를 역추적하는 방법에 관한 것이다.

본 발명에 따른 IP 역추적 방법은 IPv6 네트워크상에서 공격자에 의해 가해지는 공격을 감지하는 단계(a 단계), 상기 공격이 감지되는 경우 IPv6 네트워크를 통해 수신되는 패킷의 홉 간 옵션(hop by hop option) 헤더에 저장되어 있는, 상기 패킷이 통과한 라우터에 의해 마킹된 정보를 추출하는 단계(b 단계) 및 상기 추출된 마킹 정보를 통해 수신 패킷의 수신 경로를 재구성하여 공격자의 IP를 역추적하는 단계(c 단계)를 포함하는 것을 특징으로 한다.

대표도

도 6

특허청구의 범위

청구항 1.

IPv6 네트워크에서 IP를 역추적하는 방법에 있어서,

- (a) IPv6 네트워크상에서 공격자에 의해 가해지는 공격을 감지하는 단계;
- (b) 상기 공격이 감지되는 경우, IPv6 네트워크를 통해 수신되는 패킷의 홉 간 옵션(hop by hop option) 헤더에 저장되어 있는, 상기 패킷이 통과한 라우터에 의해 마킹된 정보를 추출하는 단계; 및
- (c) 상기 추출된 마킹 정보를 통해 수신 패킷의 수신 경로를 재구성하여 공격자의 IP를 역추적하는 단계를 포함하는 것을 특징으로 하는 IP 역추적 방법.

청구항 2.

제 1 항에 있어서, 상기 홉간 옵션 헤더는

코드 필드, 길이 필드 및 데이터 필드를 포함하며

상기 코드 필드에는 IP 역추적을 나타내는 옵션 값이 입력되는 것을 특징으로 하는 IP 역추적 방법.

청구항 3.

제 2 항에 있어서, 상기 데이터 필드에 저장되어 있는 마킹 정보는

마킹된 라우터로부터 공격당하는 호스트까지의 거리 정보를 나타내는 거리 필드,

마킹된 라우터의 주소를 나타내는 주소 필드 및

상기 수신되는 패킷의 소스 주소의 인터페이스 ID를 나타내는 분류 필드를 구비하는 것을 특징으로 하는 IP 역추적 방법.

청구항 4.

제 3 항에 있어서, 상기 데이터 필드는

5비트의 거리 필드, 마킹된 라우터의 네트워크 ID 중 FP와 TLA를 제외한 48 비트의 주소 필드 및 11비트로 해싱된 소스 주소의 인터페이스 ID를 구비하는 분류 필드를 포함하는 것을 특징으로 하는 IP 역추적 방법.

청구항 5.

제 3 항에 있어서, 상기 (c) 단계는

상기 수신되는 패킷의 소스 주소의 인터페이스 ID를 이용하여 수신되는 패킷을 공격자별로 분류하는 단계;

상기 공격자별로 분류된 수신 패킷에서 주소 필드의 마킹된 라우터와 거리 필드의 거리 정보를 이용하여 상기 마킹된 라우터를 순서대로 정렬하는 단계; 및

상기 정렬된 라우터에 의해 상기 수신 패킷의 수신 경로를 재구성하여 공격자의 IP를 역추적하는 단계를 포함하는 것을 특징으로 하는 IP 역추적 방법.

청구항 6.

제 3 항에 있어서,

상기 수신되는 패킷의 수신 경로를 재구성하지 못하는 경우, 마킹 정보를 획득하지 못한 라우터로 라우팅 정보를 요청하기 위한 메시지를 송신하는 단계;

상기 요청 메시지에 응답하여 라우팅 정보를 수신하는 단계; 및

상기 수신된 라우팅 정보에 기초하여 상기 획득하지 못한 라우터의 마킹 정보를 이용하여 수신 경로를 재구성하는 단계를 더 포함하는 것을 특징으로 하는 IP 역추적 방법.

청구항 7.

제 6 항에 있어서, 상기 라우팅 정보는

상기 요청 메시지를 수신한 라우터의 라우터 테이블에 저장되어 있는 패킷의 목적지 주소와 다음으로 홉되는 라우터 주소인 것을 특징으로 하는 IP 역추적 방법.

청구항 8.

제 3 항에 있어서,

상기 수신된 패킷의 크기가 상기 수신 경로의 PMTU와 동일한 경우, 상기 수신된 패킷에 홉간 옵션 헤더가 존재하는지를 판단하는 단계; 및

상기 수신된 패킷에 홉간 옵션 헤더가 존재하지 않는 경우, 상기 수신된 패킷을 폐기하는 단계를 더 포함하는 것을 특징으로 하는 IP 역추적 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 IPv6 네트워크에서 IP를 역추적하는 방법에 관한 것으로, 보다 구체적으로 IPv6의 확장 헤더 중 하나인 홉간 옵션(hop by hop option) 헤더에 저장되어 있는 라우터의 마킹 정보를 이용하여 IP를 역추적하는 방법에 관한 것이다.

인터넷을 통해 장소와 시간에 구분없이 다양한 정보를 교류하는 등 인터넷의 순기능과 함께 분산 시스템들의 증가와 인터넷의 확산으로 인해 네트워크를 통한 시스템의 해킹, 정보 유출, 불법 침입, 악성 바이러스 유포 등 역기능도 점차 확대되고 있다.

상기 인터넷의 역기능 중에서 대표적인 것은 서비스 거부 공격(Denial of Service)으로 최근에는 분산 공격을 통해 호스트 및 네트워크 자원을 급격히 소진하여 서비스 성능 저하 및 불가를 유발한다. 이와 같은 공격 형태는 인터넷을 통해 공격 프로그램을 이용하여 손쉽게 구현할 수 있는 반면 방어 및 추적 방법은 어려운 실정이다. 이는 TCP/IP 프로토콜의 특성상 DoS 공격 등에 대처할 수 있는 보안 구조가 제공되지 않았기 때문이다. DoS 공격자는 손쉽게 IP 패킷의 송신자 주소를 변경(이하 스푸핑이라 언급한다)하여 피해자 시스템에 보낼 수 있다. 이 경우 실제 IP 패킷이 보내진 송신자 주소가 아니기 때문에 DoS 패킷에 기록된 송신자 주소만을 가지고는 스푸핑된 패킷의 실제 공격자 추적이 곤란하다.

도 1은 네트워크상에서 피해자 호스트에 행하여지는 DDoS 공격의 형태를 보여주고 있다. 도 1을 참고로, 공격자 1 내지 공격자 2가 DDoS 공격을 피해자 호스트에 하고 있다. 실제 DDoS 공격은 훨씬 많은 수의 공격자들에 의해 행해질 수 있으며 그에 따라 피해자 호스트 측에서 받는 트래픽의 양은 엄청날 것이다. 공격에 대한 대처가 빠르게 이행되지 않는다면 피해자 호스트는 곧 서비스 불능상태가 될 것이다.

상기 설명한 DDoS 공격을 막기 위해 지금까지 존재하는 방화벽과 침입탐지 시스템과 같은 수동적인 방어는 근본적인 문제를 해결하지 못한다. 따라서 공격자를 찾아내어 근본적인 위협요소를 차단하는 능동적인 기술이 요구되고 있다. 공격 근원지를 정확하게 찾기 위한 노력으로 IP 역추적 기술이 연구되고 있다. 현재 여러 가지 IP 역추적 기술이 제안되고 있는데 확률적 패킷 마킹, ICMP, 해쉬 기반 역추적 방법 등이 있다.

도 2는 확률적 패킷 마킹 방법을 설명하고 있는 IPv4 네트워크를 도시한다. 도 2를 참고로, 상기 IPv4 네트워크에는 공격자 컴퓨터와 상기 공격자 컴퓨터가 전송하는 패킷을 피해자 호스트로 전송하는 다수의 라우터를 구비하고 있다. 공격자로부터 전송되는 패킷이 라우터 R1, R2, R7 및 R10을 통과하여 피해자 호스트로 전달되는 경우, 상기 패킷이 통과한 각 라우터는 패킷의 IP 헤더에서 변형이 가능한 필드에 자신의 IP 주소를 마킹한다. 각 라우터에서 모든 패킷에 자신의 IP 주소를 마킹하면 엄청난 오버헤드가 발생하므로 원활한 네트워크 상태를 유지하기 위해 패킷에 자신의 IP 주소를 마킹할 때 일정한 확률로 패킷을 샘플링하여 마킹한다.

도 3은 상기 확률적 패킷 마킹 방법을 이용하여 IPv4 네트워크에서 공격자 IP를 역추적하는 방법을 설명하는 흐름도이다.

IPv4 네트워크에서 피해자 호스트로 순간적으로 많은 양의 패킷이 전송되어 과부하가 발생하는 경우, 상기 피해자 호스트에 접속되어 있는 라우터(R10)를 관리하는 에이전트는 DDoS 공격을 감지한다(단계 1). 상기 DDoS 공격을 감지하면, 상기 수신된 패킷의 헤더에서 식별자 필드(Identification field, ID)를 분석한다(단계 3). 라우터에서 패킷에 정보를 기록할 때 패킷 헤더의 식별자 필드에 기록한다. 이것은 IP 헤더의 분할을 위하여 패킷의 동일성을 표시하는 식별자 필드를 사용할 확률이 0.25% 정도밖에 되지 않기 때문에 상기 라우터의 IP를 식별자 필드에 마킹한다. 상기 식별자 필드는 5비트의 거리 필드와 11비트의 에지 필드를 구비하고 있다. 상기 거리 필드는 마킹을 하는 라우터까지의 거리를 나타내며 상기 에지 필드는 마킹한 라우터의 주소를 나타낸다. 상기 32비트의 라우터 주소는 해쉬(hash) 함수를 사용하여 11비트로 암호화된 후 에지 필드에 마킹된다.

상기 에지 필드의 라우터의 주소와 상기 거리 필드의 마킹한 라우터까지의 거리를 이용하여 상기 공격 패킷이 수신된 경로를 재구성하고(단계 5), 상기 재구성된 패킷의 수신 경로를 이용하여 공격자 호스트의 IP를 역추적한다(단계 7)

발명이 이루고자 하는 기술적 과제

상기 설명한 IPv4 네트워크에서 확률적 패킷 마킹을 이용한 IP 역추적 방법은 IP 헤더의 식별자 필드를 이용하여 공격자 호스트의 IP를 역추적하는 방법을 제공한다. 그러나 IPv6 헤더의 구조와 IPv4 헤더의 구조가 서로 상이하기 때문에 상기 설명한 IPv4 네트워크에서의 확률적 패킷 마킹을 이용한 IP 역추적 방법을 IPv6 네트워크에서 동일하게 사용하지 못하는 문제점이 있다.

따라서 본 발명이 이루고자 하는 목적은 IPv6 네트워크에서 확률적 패킷 마킹을 이용하여 공격자 호스트의 IP를 역추적하는 방법을 제공하는 것이다.

발명의 구성

상기 본 발명의 목적을 달성하기 위한 IP 역추적 방법은 IPv6 네트워크상에서 공격자에 의해 가해지는 공격을 감지하는 단계(a 단계), 상기 공격이 감지되는 경우 IPv6 네트워크를 통해 수신되는 패킷의 홉 간 옵션(hop by hop option) 헤더에 저장되어 있는, 상기 패킷이 통과한 라우터에 의해 마킹된 정보를 추출하는 단계(b 단계) 및 상기 추출된 마킹 정보를 통해 수신 패킷의 수신 경로를 재구성하여 공격자의 IP를 역추적하는 단계(c 단계)를 포함하는 것을 특징으로 한다.

바람직하게, 상기 홉 간 옵션 헤더는 코드 필드, 길이 필드 및 데이터 필드를 포함하며 상기 코드 필드에는 IP 역추적을 나타내는 옵션 값이 입력되는 것을 특징으로 한다.

바람직하게, 상기 데이터 필드에 저장되어 있는 마킹 정보는 마킹된 라우터로부터 공격당하는 호스트까지의 거리 정보를 나타내는 거리 필드, 마킹된 라우터의 주소를 나타내는 주소 필드 및 상기 수신되는 패킷의 소스 주소의 인터페이스 ID를 나타내는 분류 필드를 구비하는 것을 특징으로 한다.

바람직하게, 상기 (c) 단계는 상기 수신되는 패킷의 소스 주소의 인터페이스 ID를 이용하여 수신되는 패킷을 공격자별로 분류하는 단계, 상기 공격자별로 분류된 수신 패킷에서 주소 필드의 마킹된 라우터와 거리 필드의 거리 정보를 이용하여 상기 마킹된 라우터를 정렬하는 단계 및 상기 정렬된 라우터에 의해 상기 수신 패킷의 수신 경로를 재구성하여 공격자의 IP를 역추적하는 단계를 포함하는 것을 특징으로 한다.

바람직하게, 상기 IP 역추적 방법은 상기 수신되는 패킷의 수신 경로를 재구성하지 못하는 경우, 마킹 정보를 획득하지 못한 라우터로 라우팅 정보를 요청하기 위한 메시지를 송신하는 단계, 상기 요청 메시지에 응답하여 라우팅 정보를 수신하는 단계 및 상기 수신된 라우팅 정보에 기초하여 상기 획득하지 못한 라우터의 마킹 정보를 이용하여 수신 경로를 재구성하는 단계를 더 포함하는 것을 특징으로 한다.

바람직하게, 상기 IP 역추적 방법은 상기 수신된 패킷의 크기가 상기 수신 경로의 PMTU와 동일한 경우, 상기 수신된 패킷에 홉간 옵션 헤더가 존재하는지를 판단하는 단계 및 상기 수신된 패킷에 홉간 옵션 헤더가 존재하지 않는 경우, 상기 수신된 패킷을 폐기하는 단계를 더 포함하는 것을 특징으로 한다.

이하 첨부된 도면을 참고로 본 발명에 따른 IPv6 네트워크에서 IP 역추적 방법에 대해 보다 구체적으로 설명한다.

도 4는 본 발명의 일 실시예에 상응하는, IPv6 네트워크에서 IP를 역추적하는 방법을 설명하는 흐름도이다. 도 4를 참고로, IPv6 네트워크에서 공격자 호스트에 의해 가해지는 공격을 감지한다(단계 11). 상기 공격자 호스트에 의해 가해지는 공격은 DoS 또는 DDoS 공격인 것을 특징으로 한다. 상기 DoS 또는 DDoS 공격시 공격자 호스트로부터 피해자 호스트가 수신하는 패킷의 양은 순간적으로 많이 증가한다. 따라서 상기 피해자 호스트가 접속되어 있는 라우터는 트래픽의 증가로 인해 다운되며 피해자 호스트는 정상적으로 패킷을 수신하지 못한다.

공격이 감지되는 경우, 상기 라우터가 다운되기 전 수신된 패킷에서 홉간 옵션 헤더를 추출한다(단계 12). 본 발명의 일 실시예에 상응하는 홉간 옵션 헤더의 구조가 도 5에 도시되어 있다.

도 5를 참고로, 상기 도 5의 (a)는 IPv6 네트워크의 헤더를 도시하고 있으며, 도 5의 (b)는 IPv6 네트워크의 확장 헤더 중 하나인 홉간 옵션 헤더의 구조를 도시하고 있다. 도 5의 (b)를 참고로, 상기 홉간 옵션 헤더는 코드(code) 필드, 길이(length) 필드 및 데이터 필드를 구비하고 있다. 상기 코드 필드의 타입(type) 필드 값은 IP 역추적 기능을 나타내는 소정의 값으로 설정된다. 상기 데이터 필드의 보다 상세한 구조가 도 6에 도시되어 있다.

도 6을 참고로, 상기 데이터 필드는 마킹된 라우터로부터 피해자 호스트까지의 거리 정보를 나타내는 거리(distance) 필드, 마킹된 라우터의 주소를 나타내는 주소(Address of Marking Point) 필드 및 상기 수신되는 패킷의 소스(source) 주소의 인터페이스 ID를 나타내는 분류 필드를 구비하고 있다. 바람직하게, 상기 거리 필드는 5비트이며, 상기 주소 필드는 마킹된 라우터의 네트워크 ID 중 FP와 TLA를 제외한 48비트이며 및 상기 분류 필드는 수신되는 패킷의 소스 주소의 인터페이스 ID를 해싱하여 암호화한 11비트인 것을 특징으로 한다. 상기 네트워크 ID에서 FP와 TLA에는 3ffe, 2001, 2002의 3개 값만이 사용되기 때문에 FP와 TLA의 16비트가 없더라도 라우터의 식별에 큰 영향을 미치지 않는다.

다시 도 4를 참고로, 상기 홉간 옵션 헤더에서 마킹 정보를 추출한다(단계 14). 상기 홉간 옵션 헤더의 데이터 필드에 마킹된 거리 필드, 주소 필드 및 분류 필드를 추출한다. 상기 추출된 분류 필드에 의해 수신 패킷을 공격자 호스트별로 분류한다(단계 16).

도 7은 분류 필드에 의해 분류된 수신 패킷의 일 예를 도시하고 있다. 예를 들어, 3개의 공격자 호스트(1 내지 3)로부터 패킷을 수신하는 경우 상기 수신 패킷의 데이터 필드에 저장되어 있는 각 패킷의 소스 주소의 인터페이스 ID를 통해 각 공격자 호스트를 분류한다.

다시 도 4를 참고로, 상기 공격자별로 분류된 수신 패킷에서 거리 필드를 이용하여 거리 순서대로 마킹된 라우터를 정렬한다(단계 17). 상기 거리 필드에 마킹된 거리 값은 재구성 시점에서 패킷의 홉 제한(Hop-Limited) 값과 각 라우터의 고유

홉 값의 차이를 나타낸다. 상기 홉 제한 값은 패킷이 라우터 송신되는 각 라우터에서 홉할 때마다 1씩 증가한다. 따라서, 상기 마킹된 거리 값에 의해 라우터를 정렬할 때 거리 필드의 거리 값이 클수록 마킹된 라우터가 공격자 호스트에 가까운 위치를 존재한다는 것을 의미한다.

상기 거리 필드의 거리 값에 의한 내림차순으로 마킹된 라우터를 정렬하는 경우, 맨 마지막에 위치하는 라우터, 즉 피해자 호스트에 가장 근접하다고 판단되는 라우터의 주소를 인접한 라우터의 네트워크 ID와 비교하여 같을 경우 수신 경로 상의 하나의 라우터로 채택한다. 그리고 다음에 위치하는 라우터에서 가장 근접하다고 판단되는 라우터의 주소를 인접한 라우터의 Network ID와 비교하여 수신 경로 상의 다음 라우터로 채택한다. 이러한 과정을 정렬된 처음 라우터까지 반복하여 수신 경로를 재구성한다.

상기 공격자별로 마킹된 라우터의 정렬을 통해 수신 경로의 재구성이 성공하였는지를 판단하여(단계 18), 수신 경로의 재구성이 성공한 경우 상기 재구성된 수신 경로를 통해 공격자 호스트의 IP를 역추적한다(단계 20).

한편, 수신 경로의 재구성이 성공하지 못한 경우 오류 정정 알고리즘을 실행하여 마킹되지 않은 라우터의 정보를 수신하여 패킷의 수신 경로를 다시 재구성한다(단계 19). 확률적 패킷 마킹을 이용하는 경우 패킷이 통과하는 각 라우터의 마킹 확률을 높이면 경로 재구성이 정확하게 될 확률은 높아진다. 그러나 라우터를 통과하는 많은 수의 패킷에 마킹 정보를 하는 경우 네트워크의 성능 측면에서 오히려 해가 된다. 따라서 마킹 확률을 적당한 수준에서 정해야 할 필요가 있다. 이러한 이유로 마킹 확률이 낮아져 거리 필드의 거리 값이 연속되지 않을 경우 경로의 재구성은 완벽하게 이루어지지 못한다. 도 10에 도시되어 있는 것과 같이, 라우터(R7)에서의 마킹 정보가 없기 때문에 라우터(R4)와 라우터(R12) 사이의 경로를 알 수가 없다. 위와 같은 경우를 위해 경로 재구성시 오류 정정 기법이 필요하다.

도 8은 본 발명의 일 실시예에 상응하는 상기 오류 정정 알고리즘을 보다 구체적으로 설명하는 흐름도이다. 도 8을 참고로, 수신 경로의 재구성 중 마킹되지 않은 라우터의 정보를 요청하는 메시지를 마킹되지 않은 라우터로 송신한다(단계 23). 예를 들어, 도 9에 도시되어 있는 것과 같이 라우터(R7)에서의 마킹 정보가 없는 경우, 피해자 호스트 측의 에이전트는 라우터(R4)로 라우팅 정보를 요구하는 메시지를 송신한다.

상기 라우팅 정보 요구 메시지에 응답하여 상기 라우터(R4)는 라우터(R4)에 기록되어 있는 라우팅 테이블에 기초하여 라우터(R4)에서 패킷이 다음으로 홉되는 라우터와 상기 패킷이 송신되는 최종 목적지 주소를 구비하는 라우팅 정보 제공 메시지를 상기 피해자 호스트 측의 에이전트로 송신한다.

상기 송신된 라우팅 정보 제공 메시지에서 라우터 정보를 추출하여(단계 27), 라우터(R4)에서 라우터(R12)까지의 수신 경로를 재구성한다.

한편, 도 10은 본 발명의 일 실시예에 상응하는 PMTUD(Path Maximum Transitions Unit Discovery) 방법을 설명하는 네트워크의 개요도를 도시하고 있다.

IPv4 네트워크의 라우터는 각 라우터의 데이터 송신 용량을 초과하는 패킷이 송신되는 경우, 상기 패킷의 용량을 분할하여 송신한다. 그러나 IPv6 네트워크의 라우터는 IPv4 네트워크의 라우터와는 달리 패킷의 분할 기능을 수행할 수가 없다. 따라서, 공격자 호스트가 PMTU의 값만큼의 데이터를 전송하였을 때 라우터의 마킹 정보를 추가하는 경우 PMTU에 의해 "Packet too Big" 메시지를 받고 마킹된 패킷은 폐기(Drop)된다.

따라서, 도 10에 도시되어 있는 것과 같이 본 발명에서 송신되는 패킷은 PMTUD에서 정해지는 PMTU에서 추가되는 홉간 옵션 헤더의 저장 공간을 확보하여 패킷을 송신한다. 송신자 호스트는 수신 경로의 PMTU에서 홉간 옵션 헤더의 크기를 뺀 양의 데이터를 포함하는 패킷을 생성하여 송신한다.

도 11은 상기 본 발명에 따른 IP 역추적 방법에서 수신 경로 역추적에 사용되는 패킷을 수신하는 단계를 보다 구체적으로 설명하는 흐름도이다.

도 11을 참고로, 피해자 호스트가 접속되어 있는 라우터는 공격자 호스트로부터 패킷을 수신한다(단계 31). 상기 수신된 패킷에 홉간 옵션 헤더가 존재하는지 판단한다(단계 33). IPv6 네트워크에서 공격자 호스트의 공격이 감지되는 경우, 상기 홉간 옵션 헤더가 존재하는 패킷에서 홉간 옵션 헤더를 추출하여 수신 경로를 재구성한다(단계 35). 한편, 상기 홉간 옵션 헤더가 존재하지 않는 패킷은 폐기한다(단계 37).

한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터로 읽을 수 있는 기록 매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

상기 컴퓨터로 읽을 수 있는 기록 매체는 마그네틱 저장 매체(예를 들어, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장 매체를 포함한다.

본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

발명의 효과

본 발명에 따른 IP 역추적 방법은 IPv6 네트워크의 확장 헤더인 홉간 옵션 헤더에 마킹된 정보를 이용하여 패킷의 수신 경로를 재구성하여 공격자 호스트의 IP를 역추적할 수 있다.

또한, 오류 정정 알고리즘을 통해 마킹되지 않은 라우터가 존재하는 경우에도 상기 마킹되지 않은 라우터로부터 라우팅 정보를 수신하여 수신 경로를 재구성할 수 있다.

도면의 간단한 설명

도 1은 네트워크상에서 피해자 호스트에 행하여지는 DDoS 공격의 형태를 보여주고 있다.

도 2는 확률적 패킷 마킹 방법을 설명하고 있는 IPv4 네트워크를 도시하다.

도 3은 확률적 패킷 마킹 방법을 이용하여 IPv4 네트워크에서 공격자 IP를 역추적하는 방법을 설명하는 흐름도이다.

도 4는 본 발명의 일 실시예에 상응하는, IPv6 네트워크에서 IP를 역추적하는 방법을 설명하는 흐름도이다.

도 5는 본 발명의 일 실시예에 상응하는 홉간 옵션 헤더의 구조를 도시하고 있다.

도 6은 본 발명의 일 실시예에 상응하는 상기 데이터 필드를 더욱 상세하게 도시하고 있다.

도 7은 분류 필드에 의해 분류된 수신 패킷의 일 예를 도시하고 있다.

도 8은 본 발명의 일 실시예에 상응하는 상기 오류 정정 알고리즘을 보다 구체적으로 설명하는 흐름도이다.

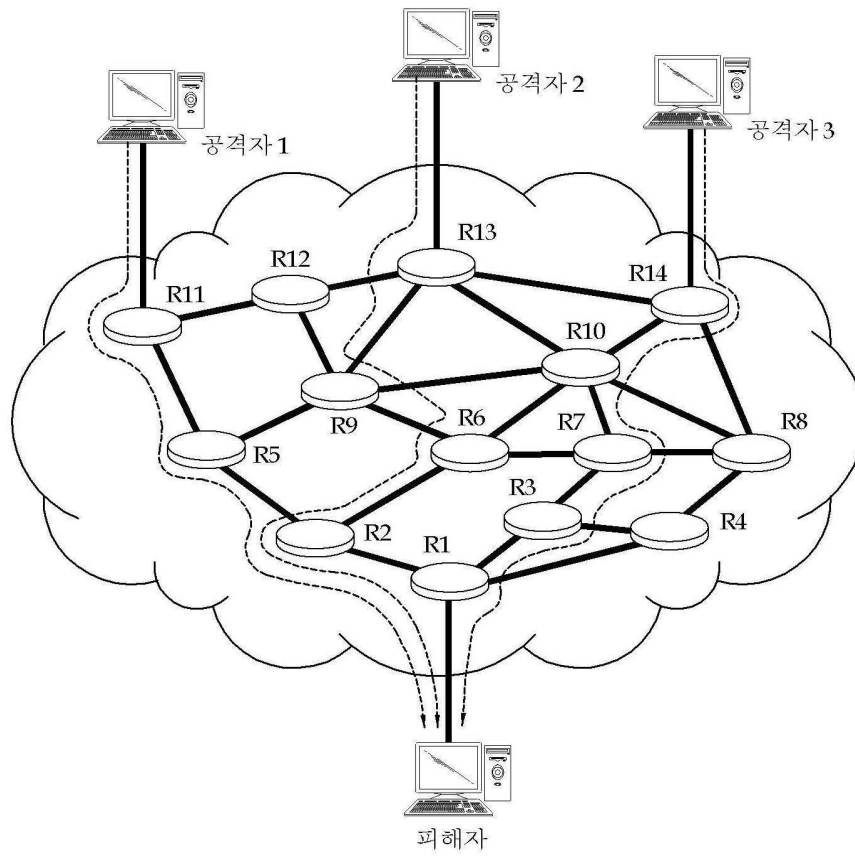
도 9는 수신 경로의 재구성에 실패하는 경우 오류 정정 알고리즘을 설명하기 위한 시스템을 도시하고 있다.

도 10은 본 발명의 일 실시예에 상응하는 PMTUD(Path Maximum Transitions Unit Discovery) 방법을 설명하는 네트워크의 개요도를 도시하고 있다.

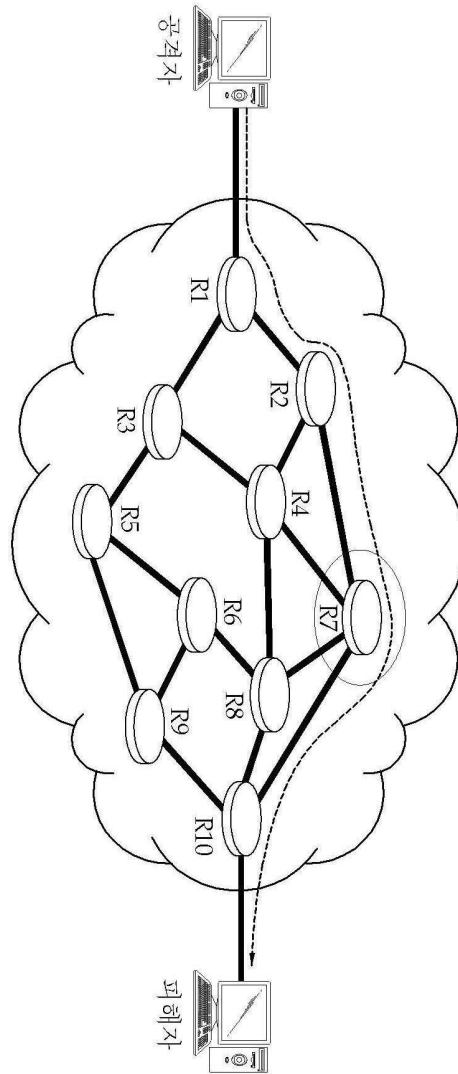
도 11은 상기 본 발명에 따른 IP 역추적 방법에서 수신 경로 역추적에 사용되는 패킷을 수신하는 단계를 보다 구체적으로 설명하는 흐름도이다.

도면

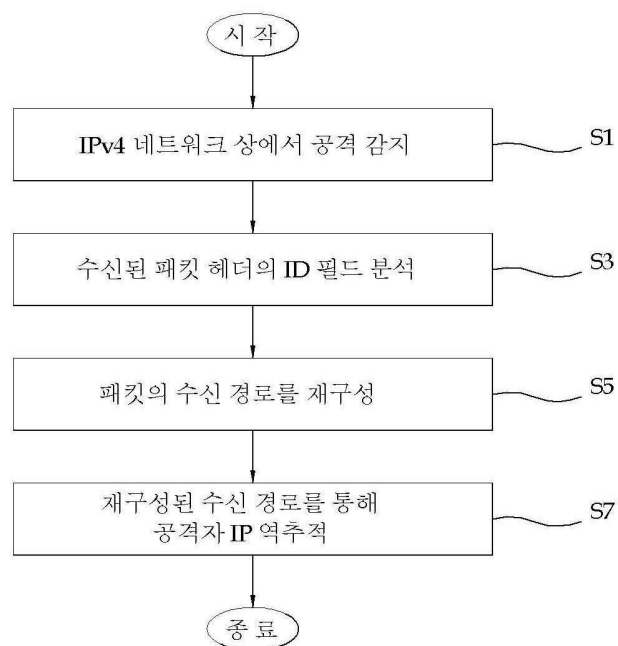
도면1



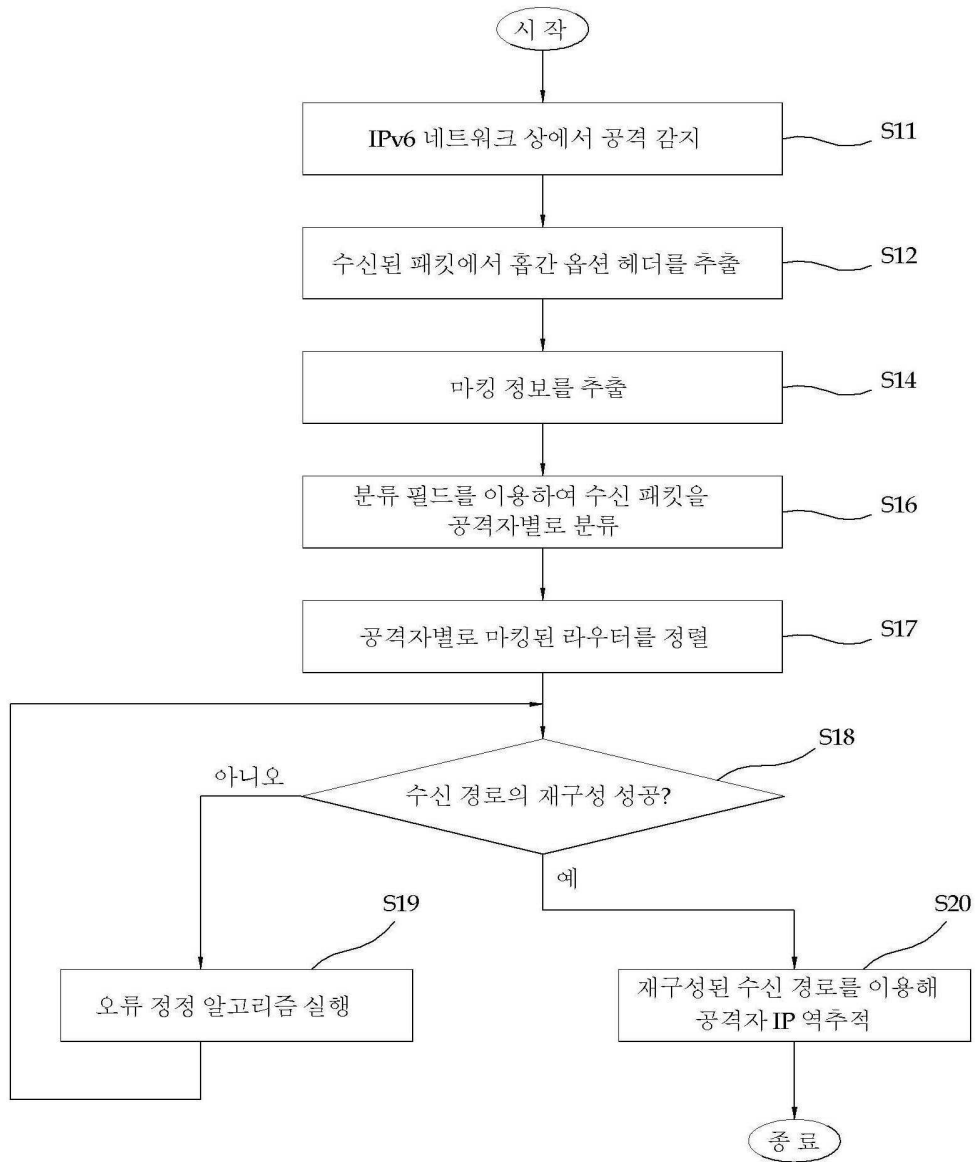
도면2



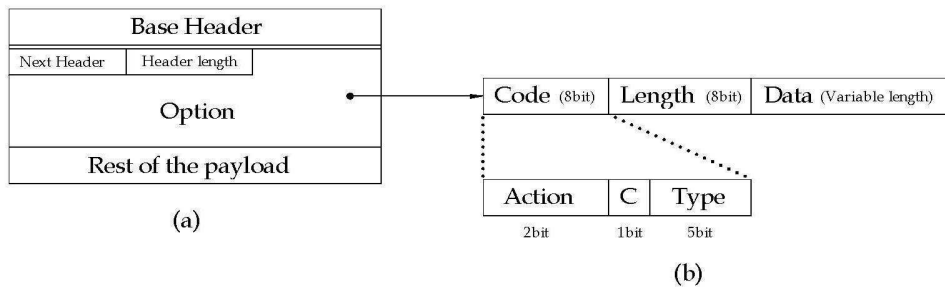
도면3



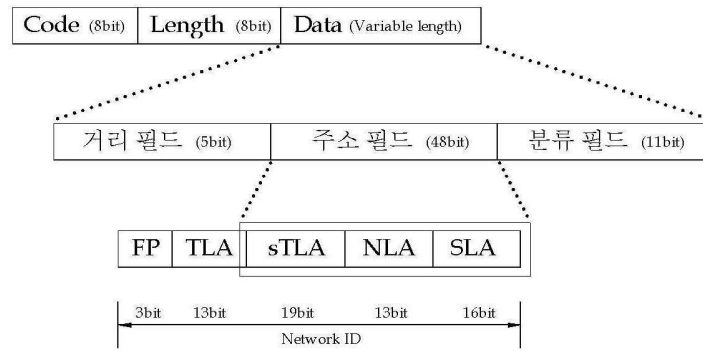
도면4



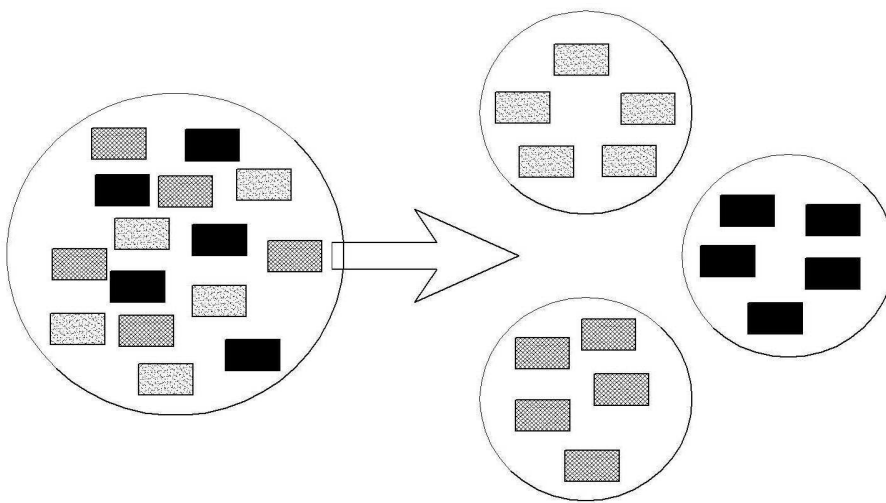
도면5



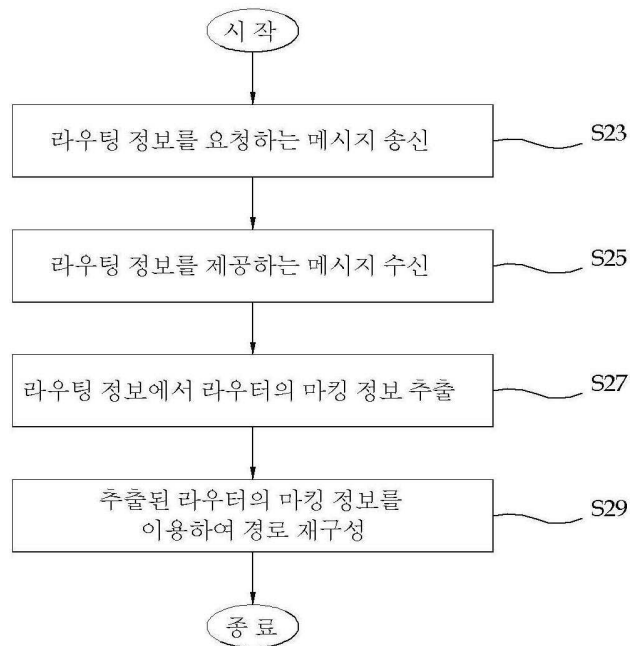
도면6



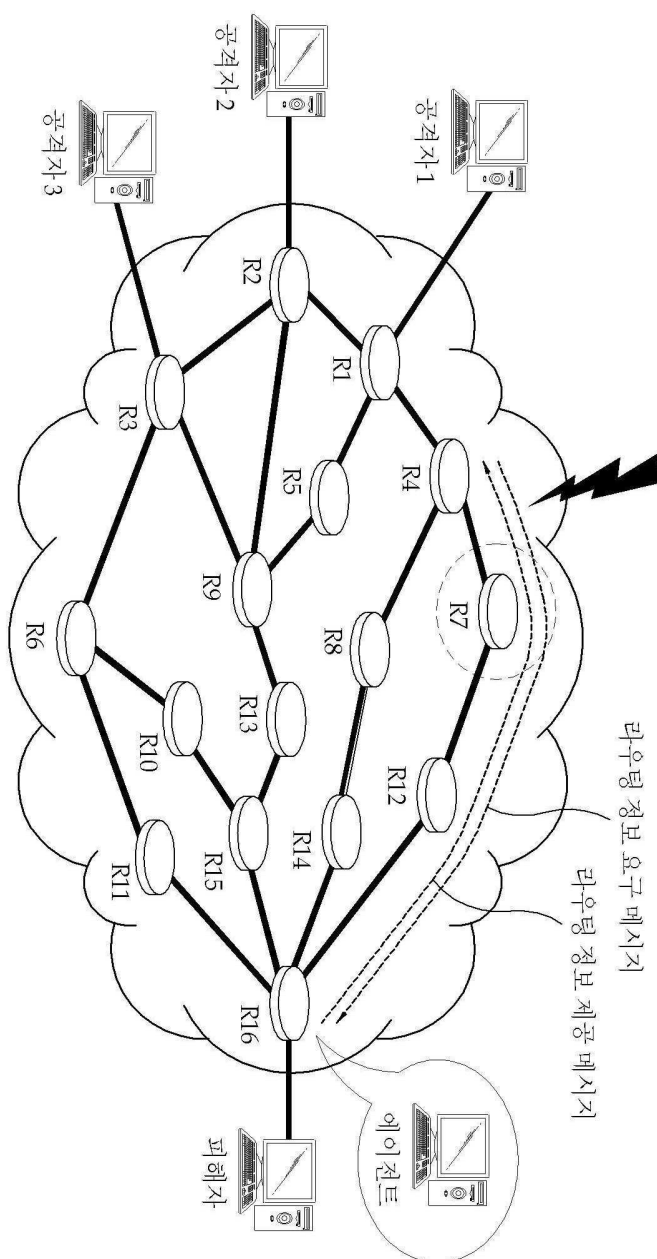
도면7



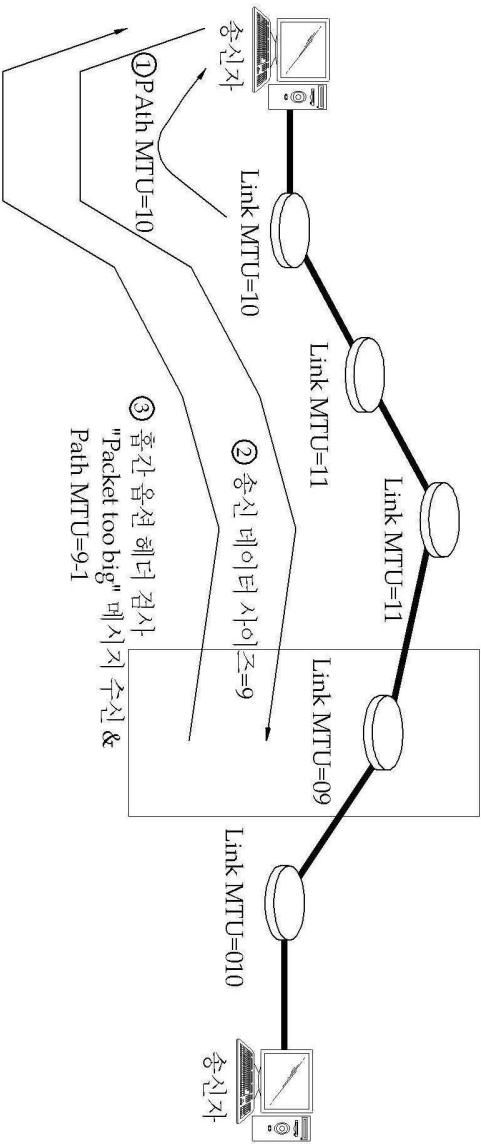
도면8



도면9



도면10



도면11

