(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년12월23일
(11) 등록번호 10-1475935
(24) 등록일자 2014년12월17일

(51) 국제특허분류(Int. Cl.)
H04L 12/22 (2006.01) *H04L 12/70* (2013.01)
(21) 출원번호 10-2013-0071147
(22) 출원일자 2013년06월20일
심사청구일자 2013년06월20일
(56) 선행기술조사문헌
IEEE 논문 이희조 외 1인, "PFS Against Distributed DoS Attacks" (2011.10.)

(73) 특허권자
고려대학교 산학협력단

(72) 발명자
이희조
서동원

(74) 대리인
특허법인엠에이피에스

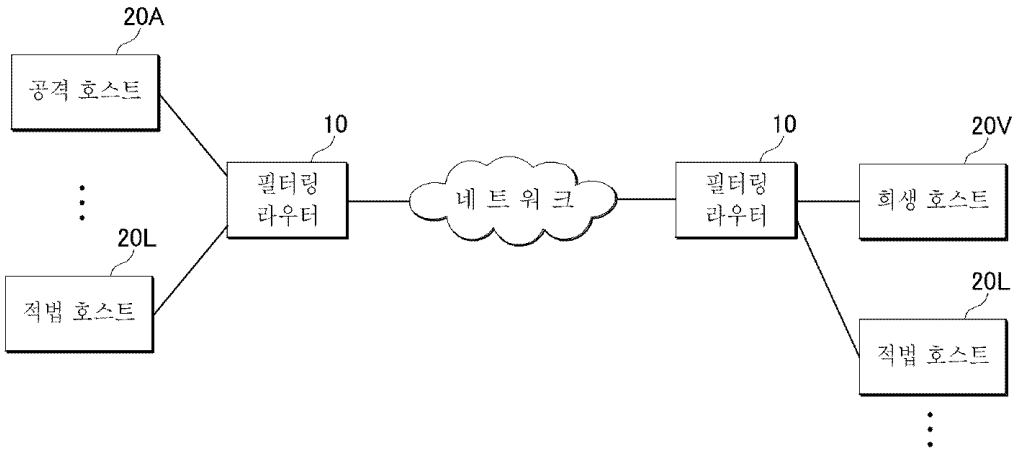
전체 청구항 수 : 총 8 항 심사관 : 문형섭

(54) 발명의 명칭 **적응적 확률 기반 패킷 필터링 라우터 및 그 방법**

(57) 요 약

본 발명은 동적으로 설정되는 패킷 마킹 확률에 기초하여, 상기 라우터가 수신한 패킷에 상기 라우터의 주소를 기초로 생성한 마킹 정보를 삽입하는 패킷 마킹부;및 상기 라우터의 필터링 효율성을 산출하고, 상기 필터링 효율성에 기초하여 상기 패킷 마킹 확률을 결정하는 마킹 확률 결정부;를 포함하는 라우터을 제공한다.

대 표 도



특허청구의 범위

청구항 1

필터링 라우터에 있어서,

적응적으로 설정되는 패킷 마킹 확률에 따라서, 상기 필터링 라우터가 수신한 패킷에 상기 라우터의 주소를 기초로 생성한 마킹 정보를 삽입하는 패킷 마킹부;및

상기 필터링 라우터의 필터링 효율성을 산출하고, 상기 필터링 효율성에 기초하여 적응적으로 상기 패킷 마킹 확률을 결정하는 마킹 확률 결정부;를 포함하되,

상기 마킹 정보는 상기 마킹 정보를 포함하고 있는 패킷을 수신한 장치에 의해 상기 필터링 라우터의 주소를 도출하는 데 사용되고,

상기 필터링 효율성은 상기 패킷의 송신지와 상기 필터링 라우터와의 거리가 가까울수록 높아지거나, 상기 필터링 라우터가 수용 가능한 필터가 많을수록 높아지거나, 상기 필터링 라우터에 연결된 링크 수가 많을수록 높아지는 필터링 라우터.

청구항 2

삭제

청구항 3

제 1 항에 있어서,

상기 패킷 마킹부는

상기 마킹 정보를 IP 헤더의 미사용 필드에 삽입하는 필터링 라우터.

청구항 4

제 1 항에 있어서,

상기 마킹 정보는 분할된 상기 필터링 라우터의 주소를 기초로 복수의 유형으로 생성되어, 각 패킷별로 다른 유형의 마킹 정보가 삽입되며,

상기 마킹 정보가 포함되어 있는 일련의 패킷을 수신한 장치 또는 다른 라우터에 의해 재조립되어 사용되는 필터링 라우터.

청구항 5

제 1 항에 있어서,

상기 필터링 라우터는 하나 이상의 필터를 저장하는 필터 저장소;

상기 필터 저장소에 저장되어 있는 필터의 사용 여부 및 폐기 여부를 결정하는 필터 관리부; 및

상기 필터 저장소에 저장되어 있는 필터를 다른 라우터로 전파하는 필터 전파부;를 더 포함하는 필터링 라우터.

청구항 6

제 5 항에 있어서,

상기 필터 저장소는

패킷 차단에 사용되는 필터가 저장되는 필터 리스트; 및

상기 필터 리스트에 저장되거나 폐기될 수 있는 후보 필터가 저장되는 고스트 리스트;를 포함하며,

상기 필터링 라우터가 수신한 필터는 상기 고스트 리스트에 저장되고,

상기 필터 관리부는

주기적으로 상기 필터 저장소에 저장되어 있는 각 필터의 필터 점수를 산출하고, 상기 필터 점수에 기초하여, 상기 각 필터를 상기 고스트 리스트로 이동시킬 것인지 상기 필터 리스트로 이동시킬 것인지 또는 폐기할 것인지 결정하는 필터링 라우터.

청구항 7

네트워크에 연결되어 있는 호스트에 있어서,

수신한 패킷이 차단되어야 할 트래픽의 패킷이라고 판단되는 경우, 상기 패킷에 포함되어 있는 마킹 정보로부터 상기 패킷의 전송 경로 상에 위치한 필터링 라우터를 식별하고, 상기 필터링 라우터로 상기 트래픽을 차단하기 위한 필터 또는 필터 요청을 발송하되,

상기 마킹 정보는 상기 필터링 라우터가 자신의 필터링 효율성을 산출하고, 상기 필터링 효율성에 기초하여 적응적으로 설정한 패킷 마킹 확률에 따라서, 상기 필터링 라우터가 자신의 주소를 기초로 생성한 것이고,

상기 필터링 효율성은 상기 패킷의 송신지와 상기 필터링 라우터와의 거리가 가까울수록 높아지거나, 상기 필터링 라우터가 수용 가능한 필터가 많을수록 높아지거나, 상기 필터링 라우터에 연결된 링크 수가 많을수록 높아지는 것인 호스트.

청구항 8

제 7 항에 있어서,

상기 호스트는 상기 트래픽의 일련의 패킷으로부터 추출한 여러 유형의 마킹 정보를 재조립하여 상기 필터링 라우터의 주소를 산출하는 호스트.

청구항 9

패킷 필터링 방법에 있어서,

필터링 라우터의 필터링 효율성을 산출하고, 상기 필터링 효율성에 기초하여 적응적으로 패킷 마킹 확률을 결정하는 단계;

상기 패킷 마킹 확률에 기초하여, 상기 필터링 라우터가 수신한 패킷에 상기 필터링 라우터의 주소를 기초로 생성한 마킹 정보를 삽입하는 단계;

장치가 상기 마킹 정보에 기초하여 산출한 상기 필터링 라우터의 주소를 이용하여 상기 필터링 라우터로 필터 또는 필터 요청을 발송하는 단계;

상기 필터링 라우터가 상기 필터를 사용하여 패킷을 차단하는 단계;

상기 필터링 라우터가 상기 필터를 다른 라우터로 전파하는 단계; 및

상기 필터의 사용 여부 및 폐기 여부를 결정하는 단계;를 포함하되,

상기 필터링 효율성은 상기 패킷의 송신지와 상기 필터링 라우터와의 거리가 가까울수록 높아지거나, 상기 필터링 라우터가 수용 가능한 필터가 많을수록 높아지거나, 상기 필터링 라우터에 연결된 링크 수가 많을수록 높아지는 것인 패킷 필터링 방법.

청구항 10

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 패킷 필터링 라우터 및 그 방법에 관한 것이다.

배 경 기 술

[0002] 서비스 거부 공격(DDoS: Distributed Denial-of-Service)은 대표적인 네트워크 공격으로 매우 치명적인 피해를 입힐 수 있다. 따라서 이를 방어하기 위한 효과적인 방법이 필요하다.

[0003] 아래 도 1을 통해 후술하겠지만, 네트워크 공격을 방어하는 방법은 방어 지점에 따라 분류할 수 있는데, 여러 방어 지점 중에서 라우터에서 방어하는 것이 효율적이다.

[0004] 공격 트래픽을 차단하는 일종의 규칙인 필터(filter)를 라우터에 저장하고, 이를 사용하여 특정 트래픽에 해당하는 패킷을 차단하는 것이다.

[0005] 빠르게 필터를 전파시킬 수 있고, 종래의 시스템과 호환되어 설치 및 사용이 용이한 필터링 라우터 및 필터링 라우터를 사용하여 효과적으로 패킷을 차단할 수 있는 방법이 필요하다.

[0006] 본 발명과 관련하여 한국공개특허 10-2006-0128734호("다양한 네크워크 공격들에 대한 적응적 방어")에는 여러 가지 기준에 따라 필터의 공격 감도를 적응적으로 조절하는 구성이 개시되어 있다.

[0007] 또한, 한국등록특허 10-1228288호("네트워크 감시 방법 및 그 장치")는 패킷 트래픽 흐름을 차단하여 제어하는 기준을 적응적으로 조절하는 구성이 개시되어 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 전술한 문제를 해결하기 위한 것으로서, 그 목적은 효과적인 패킷 필터링 라우터 및 그 방법을 제공하는 것이다.

과제의 해결 수단

[0009] 상기와 같은 목적을 달성하기 위한 본 발명의 제 1 측면에 따른 라우터는 동적으로 설정되는 패킷 마킹 확률에 기초하여, 상기 라우터가 수신한 패킷에 상기 라우터의 주소를 기초로 생성한 마킹 정보를 삽입하는 패킷 마킹부;및 상기 라우터의 필터링 효율성을 산출하고, 상기 필터링 효율성에 기초하여 상기 패킷 마킹 확률을 결정하는 마킹 확률 결정부;를 포함하는 것을 특징으로 한다.

[0010] 상기와 같은 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 네트워크에 연결되어 있는 호스트는 수신한 패킷이 차단되어야 할 트래픽의 패킷이라고 판단되는 경우, 상기 패킷에 포함되어 있는 마킹 정보로부터 상기 패킷의 전송 경로 상에 위치한 라우터를 식별하고, 상기 라우터로 상기 트래픽을 차단하기 위한 필터 또는 필터 요청을 발송하는 것을 특징으로 한다.

[0011] 상기와 같은 목적을 달성하기 위한 본 발명의 제 3 측면에 따른 패킷 필터링 방법은 라우터의 필터링 효율성을 산출하고, 상기 필터링 효율성에 기초하여 패킷 마킹 확률을 결정하는 단계; 상기 패킷 마킹 확률에 기초하여, 상기 라우터가 수신한 패킷에 상기 라우터의 주소를 기초로 생성한 마킹 정보를 삽입하는 단계; 장치가 상기 마킹 정보에 기초하여 산출한 상기 라우터의 주소를 이용하여 상기 라우터로 필터 또는 필터 요청을 발송하는 단계; 상기 라우터가 상기 필터를 사용하여 패킷을 차단하는 단계; 상기 라우터가 상기 필터를 다른 라우터로 전파하는 단계; 및 상기 필터의 사용 여부 및 폐기 여부를 결정하는 단계;를 포함하는 것을 특징으로 한다.

발명의 효과

[0012] 본 발명은 네트워크 공격을 빠르고 효율적으로 차단한다는 효과를 갖는다.

[0013] 본 발명은 필터링 효율이 높은 필터링 라우터에 높은 패킷 마킹 확률을 설정하여, 공격이 감지될 경우 필터 또는 필터 요청을 해당 필터링 라우터로 바로 보낼 수 있으므로, 종래 기술보다 빠르게 필터를 전파할 수 있다는 장점을 가진다.

[0014] 희생 호스트가 필터를 필터링 효율이 가장 높은 최적의 필터링 라우터로 바로 보내므로, 희생 호스트에서의 공격 트래픽을 78% 감소시킬 수 있다.

[0015] 희생 호스트에 대한 공격 뿐아니라, 링크에 대한 공격도 방어할 수 있다.

[0016] 본 발명의 일실시예에 따른 필터링 라우터는 레거시 라우터 및 기존 프로토콜(예: IPv4)와 호환되므로, 현재의 네트워크에 쉽게 설치되고 사용될 수 있다. 즉, 설치 및 운영 비용이 낮다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 필터링 라우터를 포함하는 네트워크를 도시함.

도 2는 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 필터링 라우터의 구조를 도시함.

도 3은 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 필터링 라우터와 연계하여 동작하는 호스트의 구조를 도시함.

도 4는 본 발명의 일실시예에 따른 확률 기반 패킷 마킹의 개념을 도시함.

도 5는 종래의 고정 확률 기반 패킷 마킹의 예를 도시함.

도 6은 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 마킹의 예를 도시함.

도 7은 본 발명의 일실시예에 따른 패킷 마킹 정보의 실시예를 도시함.

도 8은 본 발명의 일실시예에 따른 패킷 마킹 확률을 산출하는 실시예를 도시함.

도 9는 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 필터링 방법의 흐름을 도시함.

도 10 및 도 11은 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 필터링의 성능을 분석한 그래프를 도시함.

발명을 실시하기 위한 구체적인 내용

[0018] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0019] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0020] 도 1은 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 필터링 라우터(이하 "필터링 라우터")를 포함하는 네트워크를 도시하고 있다.

[0021] 네트워크는 인터넷 또는 임의의 다른 종류의 네트워크일 수 있다. 네트워크는 하나 이상의 본 발명의 일실시예에 따른 필터링 라우터(10)를 포함하며, 네트워크는 하나 이상의 레거시 라우터(미도시)를 포함할 수 있다. 레거시 라우터란 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 필터링 기능을 구비하고 있지 않은 종래 라우터를 의미한다. 즉, 본 발명의 일실시예에 따른 필터링 라우터(10)는 레거시 라우터와 호환 가능하므로, 기존의 네트워크에 용이하게 설치되어 운영될 수 있다.

[0022] 호스트(20L, 20A, 20V)는 네트워크에 연결되어 있는 임의의 장치 또는 시스템으로, 예를 들어, 서버 또는 클라이언트일 수 있다. 편의상 이들 중 다른 호스트에 대해 네트워크 공격(예: 서비스 거부 공격)을 행하는 호스트를 공격 호스트(20A), 공격을 받는 호스트를 희생 호스트(20V), 그 이외의 호스트를 적법(legitimate) 호스트(20L)라고 하자.

[0023] 대표적인 네트워크 공격 중 하나인 서비스 거부 공격(DDoS: Distributed Denial-of-Service attack)을 방어하기 위한 다양한 방법이 연구되어 왔는데, 방어 지점에 따라 공격 호스트(20A) 단에서 차단하는 방법, 희생 호스트(20V) 단에서 차단하는 방법, 및 양단을 연결하는 중간 네트워크에서 차단하는 방법으로 분류할 수 있다. 공격 호스트(20A), 즉, 공격의 원천지 쪽에서 차단하는 것이 악성 코드가 널리 퍼지기 전에 차단하므로 가장 효율적일 것이지만 그러한 방법을 설계하고 채용하는 것이 용이하지 않으며, 희생 호스트(20V) 단에서 차단하는 방법은 방어 범위가 희생 호스트(20V) 자신 또는 주위의 소규모 네트워크에 한정된다는 문제가 있다. 따라서 본 발명은 중간지에서 공격을 차단하는 방법을 제공하는 것을 목적으로 한다.

[0024] 이를 위해 본 발명은 라우터를 사용하는데, 이는 라우터가 희생 호스트(20V)에 대한 공격 및 네트워크 링크에 대한 공격 모두를 효율적으로 방어할 수 있는 지점이기 때문이다. 필터링 라우터(10)는 필터(filter)를 사용하여, 공격 패킷이 네트워크로 퍼지거나 희생 호스트(20V)에 도달하는 것을 막는다. 즉, 필터는 원치 않는 트래픽

흐름(flow)를 차단하기 위한 일종의 규칙(rule)으로, 어떤 패킷이 폐기(drop)될 것인지 전달(forward)될 것인지를 결정한다. 필터링 라우터(10)는 자신이 가지고 있는 필터에 기초하여 패킷을 폐기시키거나 통과시킨다.

[0025] 이러한 필터 기반(filter-based) 방어 기법에서는 공격 호스트(20A)와 희생 호스트(20V) 사이에 많은 필터링 라우터가 존재하며, 필터가 네트워크로 제대로 전파되지 않거나 많은 필터링 라우터가 동일한 필터를 중복해서 가지고 있을 수 있다. 따라서 효율적인 필터 전파(filter propagation) 및 필터 관리(filter managerment)가 필터 기반 방어의 중요한 과제이다.

[0026] 종래의 필터 기반 방어 기법 중 하나인 AITF(Active Internet Traffic Filtering)은 필터를 전파시키기 위하여 레코드 라우트(record route)를 사용하고, 필터의 수를 관리하기 위하여 비율 제한(rate limiting)을 사용한다. 그러나 레코드 라우트는 IP 옵션을 사용해야 하므로, 현재 네트워크에 설치되어 사용되고 있는 많은 레거시 라우터와 호환되지 않는다는 문제를 가지고 있다. 레거시 라우터는 이를 지원하지 않기 때문이다. 또한 비율 제한은 필터 수를 줄이기는 하지만 어떤 필터를 설치하고 어떤 필터를 설치하지 않을 것인지를 결정해주지는 않는다. 또한, 필터 전파가 1홉씩(hop-by-hop) 이루어지므로, 공격 호스트(20A)와 희생 호스트(20V) 사이에 많은 필터링 라우터(10)가 있을 경우 공격 호스트(20A)를 차단하는 필터가 전파되는 속도가 느려, 공격을 신속하게 차단하지 못할 수 있다.

[0027] 따라서 어떻게 필터를 공격 경로를 따라 전파할 것인가(경로 식별: path identification), 어떻게 필터를 전파하여 필터가 필터링 라우터(10)에 설치되게 할 것인가(필터 전파: filter propagation), 및 필터링 라우터(10)의 제한된 자원을 가지고 어떻게 필터를 관리할 것인가(filter management)라는 세가지 과제를 해결할 필요가 있다.

[0028] 이러한 세가지 과제를 필터 스케줄링 문제(filter scheduling problem)이라고 정의할 수 있다. 본 발명의 일실시예에 따른 필터링 라우터(10)는 필터 스케줄링 문제를 적응적 패킷 마킹(adaptive packet marking) 및 필터 스케줄링 정책(filter scheduling policy)를 사용하여 해결한다.

[0029] 본 발명의 일실시예에 따른 필터링 라우터(10)는 공격 경로 식별을 위해, 사용되지 않는 IP 헤더 필드에 자신의 주소에 기초하여 생성된 마킹(marking) 정보를 적응적으로 산출되는 마킹 확률에 따라 삽입한다. 마킹 확률은 필터링 효율성에 따라 동적으로 변한다. 필터링 효율성은 예를 들어, 필터링 라우터(10)가 얼마나 공격 호스트(20A)와 가깝게 있는가, 필터링 라우터(10)가 얼마나 많은 필터를 수용할 수 있는가, 및 필터링 라우터(10)가 얼마나 많은 링크를 가지고 있는가 등에 근거하여 판단할 수 있다. 희생 호스트(20V)는 필터링 효율성이 높아 높은 확률을 가지는 필터링 라우터(10)로부터 마킹을 수신하므로, 필터는 효율적인 필터링 라우터(10)에 먼저 도달할 수 있다. 따라서 본 발명은 종래 기술보다 빠르게 필터를 전파할 수 있다는 장점을 가진다.

[0030] 또한 본 발명의 일실시예에 따른 필터링 라우터(10)는 필터 스케줄링 정책에 따라 필터를 선별하여, 지나치게 많은 필터 요청으로 발생할 수 있는 오버헤드를 방지한다. 필터 스케줄링 정책은 어떤 필터가 필터링 라우터(10)에 설치되고, 어떤 필터가 필터링 라우터(10)에서 쫓겨나야 하는지를 결정한다. 각 필터링 라우터(10)는 자신이 가지고 있는 필터가 얼마나 자주, 얼마나 최근에 사용되었는지에 따라 필터 점수(우선 순위)를 산출하여, 활발하게 사용되고 있는 필터를 유지하고 쓸모없는 필터를 쫓아낼 수 있다. 따라서 본 발명은 종래 기술보다 효율적으로 필터를 관리할 수 있다는 장점을 가진다.

[0031] 이하 도면들을 통해 좀더 자세히 설명하기 전에, 본 발명이 가정하고 있는 몇가지 사항을 먼저 살펴본다.

[0032] 먼저, 공격 호스트(20A)는 패킷 스푸핑(packet spoofing) 능력이 있다. 즉, 공격 호스트(20A)는 IP 소스 주소를 스푸핑하여, 추적을 어렵게 하고 방어 체계를 무너뜨릴 수 있다. 또한 공격 호스트(20A)는 필터 플러딩(flooding) 능력이 있다. 즉, 공격 호스트(20A)는 가짜 필터(forged filter)를 필터링 라우터(10)에 보내어, 필터링 라우터(10)가 적법 호스트(20L)로부터의 패킷을 차단하게 할 수 있으며, 많은 수의 필터를 보내어 필터링 라우터(10)의 필터 저장소를 쓸모없는 필터로 가득차게 할 수 있다. 필터링 라우터(10)의 필터 저장소는 크기가 유한한 자원이므로, 이러한 공격은 필터링 라우터(10)의 방어 체계를 무너뜨릴 수 있다.

[0033] 그러나 공격 호스트(20A)는 전역적인 공격을 행할 수 없다. 공격 호스트(20A)가 네트워크의 모든 경로의 모든 패킷을 모니터할 수는 없기 때문이다. 따라서 공격 호스트(20A)는 다양한 경로상에서 탈취한 부분적인 정보를 재조립하여 공격에 사용한다. 또한 공격 호스트(20A)는 필터링 라우터(10) 자체를 감염시키거나 가짜 필터링 라우터를 만들 수 없다. 공격 호스트(20A)가 가짜 필터링 라우터(10)를 만들더라도 네트워크 관리자가 이를 쉽게 적발할 수 있다고 가정한다.

[0034] 한편, 희생 호스트(20V)는 트래픽 패턴을 모니터하여 공격 트래픽을 식별할 수 있다고 가정한다. 많은 서버가

이러한 기능을 포함하고 있다. 또한, 희생 호스트(20V)를 마비시키기 위해서는, 적법한 트래픽보다 눈에 띄게 높은 비율의 공격 흐름이 필요하다고 가정한다. 즉, 공격 트래픽의 pps 또는 bps는 적법한 트래픽 흐름의 pps 또는 bps보다 높다고 가정한다.

[0035] 이제, 도 2 및 도 3을 통해, 본 발명의 일실시예에 따른 필터링 라우터(10) 및 필터링 라우터(10)와 연계하여 동작하는 호스트(예: 적법 호스트(20L) 또는 희생 호스트(20V). 이하 호스트(20)로 통칭)의 구조를 간략하게 살펴본다. 자세한 내용은 후술한다.

[0036] 도 2는 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 필터링 라우터의 구조를 도시하고 있다.

[0037] 본 발명의 일실시예에 따른 필터링 라우터(10)는 필터 저장소(100), 마킹 확률 결정부(102), 패킷 마킹부(104), 필터 관리부(106), 및 필터 전파부(108)를 포함한다.

[0038] 필터 저장소(100)는 하나 이상의 필터를 저장한다. 필터 관리부(106)는 전술한 바와 같이 필터 스케줄링 정책을 사용하여 필터 저장소(100)에 저장되어 있는 필터의 사용 여부 또는 우선 순위 및 폐기 여부를 결정하며, 필터 전파부(108)는 사용되고 있는 필터를 다른 필터링 라우터(10)로 전파한다.

[0039] 패킷 마킹부(104)는 필터링 라우터(10)가 수신한 패킷에 마킹 정보를 삽입한다. 마킹 정보는 필터링 라우터(10)의 주소를 사용하여 생성될 수 있으며, 여러 가지 유형(type)이 있을 수 있다.

[0040] 마킹 정보는 마킹된, 즉, 마킹 정보가 삽입된 패킷을 수신한 장치나 라우터에 의해 패킷에 마킹한 필터링 라우터(10)의 주소를 도출할 수 있다. 즉, 마킹 정보는 해당 패킷의 전송 경로 상에 위치한 필터링 라우터(10)를 식별하는 데 사용될 수 있으며, 마킹 정보로부터 도출된 필터링 라우터(10)의 주소는 필터 또는 필터 요청의 목적지 주소로 사용될 수 있다.

[0041] 패킷 마킹부(104)가 패킷에 마킹하는 확률은 전술한 바와 같이 동적으로 설정되는데, 마킹 확률 결정부(102)가 필터링 라우터(10)의 필터링 효율성에 근거하여 패킷 마킹 확률을 결정한다. 전술한 바와 같이, 필터링 효율성은 패킷의 송신지(예: 공격 호스트(20A) 또는 적법 호스트(20L))와의 거리, 필터링 라우터(10)의 가용 자원(예: 필터 저장소(100) 크기), 및 필터링 라우터(10)의 링크 수에 기초하여 산출될 수 있다.

[0042] 도 3은 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 필터링 라우터와 연계하여 동작하는 호스트의 구조를 도시하고 있다.

[0043] 본 발명의 일실시예에 따른 호스트(20)는 마킹 조립부(202) 및 필터 발송부(204)를 포함한다.

[0044] 마킹 조립부(202)는 수신한 패킷에 포함되어 있는 여러 가지 유형의 마킹 정보를 조립한다. 마킹 정보는 필터링 라우터(10)의 주소를 사용하여 생성되므로, 호스트(20)는 조립된 마킹 정보를 사용하여 필터링 라우터(10)를 식별할 수 있다.

[0045] 따라서 수신한 패킷이 공격 패킷으로 판단되는 경우, 필터 발송부(204)가 필터 또는 필터 요청을 생성하여 해당 필터링 라우터(10)로 발송하는 것이 가능하다.

[0046] 이제, 도 4 내지 도 6을 통해, 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 마킹에 대해 설명한다. 이들 도면에서 레거시 라우터는 생략되었다. 따라서 도시되어 있지 않으나 필터 전파는 다른 레거시 라우터를 거쳐 이루어질 수 있다.

[0047] 도 4는 본 발명의 일실시예에 따른 확률 기반 패킷 마킹의 개념을 도시하고 있다.

[0048] 도면은 필터링 라우터(10)의 패킷 마킹 확률이 40%(mp=40%)일 때를 도시하고 있다. 40%라는 것은 100개의 패킷을 수신하였을 때, 그중 40개의 패킷에 마킹 정보를 삽입한다는 뜻이다. 이에 따라, 패킷 p1, p2, p3, p4, p5이 수신되었을 때, 패킷 p1 및 p4에 마킹 정보가 삽입된 후, p1, p2, p3, p4, p5이 전달(forwarding)되는 모습이 도시되어 있다.

[0049] 패킷 마킹 확률이 100%이라면(mp=100%), 필터링 라우터(10)는 수신한 모든 패킷에 마킹 정보를 삽입하여 전달할 것이다. 대부분의 패킷이 적법 패킷이라면 이는 매우 비효율적일 것이다. 필터링 라우터(10)의 자원은 한정되어 있으며, 마킹 정보 삽입에 따라 패킷 전달에 지연이 발생할 것이기 때문이다.

[0050] 따라서 본 발명의 일실시예에 따른 필터링 라우터(10)는 확률적으로 패킷에 마킹한다. 이러한 패킷 마킹 확률은 고정적일 수도 있고, 가변적일 수도 있을 것이다. 도 5 및 도 6을 통해 고정적일 때의 필터 전파 속도와 필터링 효율성에 기초하여 적응적으로 변할 때의 필터 전파 속도를 비교한다.

[0051] 도 5는 종래의 고정 확률 기반 패킷 마킹의 예를 도시하고 있다.

[0052] 각 필터링 라우터(10-1, 10-2, 10-3, 및 10-4)의 패킷 마킹 확률이 모두 30%(mp=30%)로 고정적인 경우, 희생 호스트(20V)가 공격을 감지하여 필터를 자신과 가장 가까운 곳에 있는 필터링 라우터(10-4)로 발송하면(sf-1), 해당 필터링 라우터(10-4)는 마킹 정보에 의해 식별된 공격 경로 상의 다음 라우터(10-3)로 필터를 전파한다(sf-2). 이러한 과정이 한번 더 이루어져야(sf-3), 공격 호스트(20A)와 가장 가까운 곳에 있는 필터링 라우터(10-1)에 필터가 도달한다.

[0053] 즉, 종래의 고정 확률 기반 패킷 마킹에서는 공격 호스트(20A)와 희생 호스트(20V) 사이의 경로에 3개의 필터링 라우터(10)가 있을 경우, 공격에 대해 희생 호스트(20V)에서 생성된 필터가 공격 호스트(20A)와 가장 가까운 곳에 있는 필터링 라우터(10-1)까지 도달하기 위해서는 3번의 필터 발송 또는 전파가 이루어져야 한다.

[0054] 도 6은 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 마킹의 예를 도시하고 있다.

[0055] 각 필터링 라우터(10-1, 10-2, 10-3, 및 10-4)의 패킷 마킹 확률이 각각 mp1=30%, mp2=30%, mp3=50%, mp4=10%로 필터링 효율에 따라 적응적으로 설정되어 있다. 희생 호스트(20V)가 공격을 감지하여 필터를 전송하는 필터링 라우터는 자신과 가장 가까운 곳에 있는 필터링 라우터(10-4)가 아니라, 마킹 정보에 의해 식별된 공격 경로 상의 필터링 효율이 높은 라우터(10-3)이다(sa-1). 필터 전파를 한번만 더 하면(sa-2), 공격 호스트(20A)와 가장 가까운 곳에 있는 필터링 라우터(10-1)에 필터가 도달한다.

[0056] 즉, 본발명의 일실시예에 따른 적응적 확률 기반 패킷 마킹에서는 공격 호스트(20A)와 희생 호스트(20V) 사이의 경로에 3개의 필터링 라우터(10)가 있을 경우, 공격에 대해 희생 호스트(20V)에서 생성된 필터가 공격 호스트(20A)와 가장 가까운 곳에 있는 필터링 라우터(10-1)까지 도달하기 위한 필터 발송 또는 전파 횟수가 종래보다 적다. 따라서 공격 호스트(20A)와 가장 가까운 곳에 있는 필터링 라우터(10-1)가 공격 호스트(20A)에 더 이상 공격 패킷을 발송하지 말 것을 요청하거나 공격 호스트(20A)로부터의 패킷을 차단한다고 했을 때, 본발명의 일실시예에 따른 적응적 확률 기반 패킷 마킹 방법이 종래의 방법보다 공격을 좀더 빠르게 차단할 수 있을 것이다.

[0057] 이는 각 필터링 라우터(10)의 패킷 마킹 확률이 각 필터링 라우터(10)의 필터링 효율에 기초하여 설정되기 때문이다. 예를 들어, 필터링 라우터(10-3)는 필터링 라우터(10-4)보다 공격 호스트(20A)에 더 가까이 있고, 더 많은 링크를 가지고 있기 때문에, 필터링 라우터(10-3)의 마킹 확률 결정부(102)가 설정한 패킷 마킹 확률(mp3=50%)이 필터링 라우터(10-4)의 마킹 확률 결정부(102)가 설정한 패킷 마킹 확률(mp4=10%)보다 높은 것이다.

[0058] 도 7은 본 발명의 일실시예에 따른 패킷 마킹 정보의 실시예를 도시하고 있다.

[0059] 전술한 바와 같이, 본 발명의 일실시예에 따른 필터링 라우터(10)는 자신의 주소에 기초한 마킹 정보를 패킷의 미사용 IP 헤더(header) 필드에 삽입한다. 이에 따라 본 발명은 기존의 프로토콜(protocol)을 수정하지 않아도 된다는 장점을 가진다. 예를 들어, 마킹 정보를 삽입하기 위하여 IP의 페이로드(payload) 데이터를 수정할 필요가 없으므로, 레거시 라우터가 해당 패킷을 처리하지 않고 버리거나 조각내는 데 따른 부작용이 없다.

[0060] 단, 미사용 IP 헤더 필드의 공간은 한정되어 있다는 문제가 있다. 예를 들어, IPv4 패킷은 25 비트를 사용하지 않는데, 도시된 실시예에서 본 발명의 일실시예에 따른 필터링 라우터(10)는 자신의 주소를 마킹하기 위해 32 비트를 필요로 한다. 따라서 필터링 라우터(10)의 패킷 마킹부(104)는 필터링 라우터(10)의 주소를 상위 16 비트(FR(add)0-15)와 하위 16 비트(FR(add)16-31)로 분할하여, 각각을 사용한 두가지 유형의 마킹 정보를 생성한다(각각 S1, S2). 호스트(20)는 수신한 이 두가지 마킹 정보를 재조립하여 마킹 정보를 삽입한 필터링 라우터(10)의 주소를 도출할 수 있다.

[0061] 이때 호스트(20)가 마킹 정보를 잘못 재조립하지 않도록 해야 한다. 예를 들어, 호스트(20)는 필터링 라우터(10-3)으로부터의 S1과 필터링 라우터(10-4)로부터의 S2를 조립하지 않아야 한다.

[0062] 이를 방지하기 위해 필터링 라우터(10)의 패킷 마킹부(104)는 필터링 라우터(10)의 주소에 기초하여 산출된 해시(hash) 값인 체크섬(CHK)과 메시지 인증 코드(MAC: Message Authentication Code)를 사용한다. 패킷 마킹부(104)는 수신지 주소, 즉, 목적지 IP 주소에 대해 필터링 라우터(10)의 비밀키(secret key)를 사용하여, S1 및 S2를 위해 각각 6 비트 메시지 인증 코드를 생성한다(각각 MAC1, MAC2).

[0063] 체크섬은 MAC에 따라 변하며, S3이라는 세번째 유형의 마킹 정보를 구성한다. 도시되어 있는 바와 같이, 체크섬은 S1, S2의 분할된 필터링 라우터(10) 주소 및 각각에 대한 메시지 인증 코드를 사용하여 생성될 수 있다. 여

기에서 H()는 암호화 해시 함수를 의미하며, 체크섬은 플래그에서 사용하지 않아도 되는 1비트를 하나 더 사용할 수 있으므로(다음 문단 참조), 23비트로 생성된다.

[0064] 결론적으로, 패킷 마킹부(104)는 도시된 바와 같이, 세가지 유형의 마킹 정보를 생성한다. S1 유형은 필터링 라우터(10)의 IP 주소의 상위 16 비트와 S1을 위한 메시지 인증 코드 6비트, S2 유형은 필터링 라우터(10)의 IP 주소의 하위 16 비트와 S2를 위한 메시지 인증 코드 6비트, S3 유형은 상기 정보들에 따라 산출된 체크섬을 나타낸다. 각각의 마킹 정보는 패킷 마킹 정보임을 나타내는 마킹 비트 1비트와 유형을 나타내는 플래그 2비트 등의 기타 정보를 포함한다. 이러한 방식으로 세가지 유형의 마킹 정보 모두 총 25비트의 미사용 IP 헤더 필드에 수용될 수 있다.

[0065] 체크섬은 호스트(20)가 재조립한 마킹 정보를 검증하는 데 사용될 수 있다. 호스트(20)는 수신한 S1과 S2로부터 필터링 라우터(10)의 패킷 마킹부(104)가 사용한 것과 동일한 방식으로 제 2 체크섬(CHK')를 생성할 수 있으며, 이를 수신한 S3이 포함하고 있는 체크섬(CHK)과 비교하여, 재조립이 성공적으로 수행되었는지 확인할 수 있다. 즉, CHK=CHK'이면 재조립이 성공하여, 수신한 패킷의 전송 경로상에 위치한 필터링 라우터(10)의 주소가 도출된 것이고, 그렇지 않으면 재조립이 실패한 것이다.

[0066] 본 발명은 다음과 같은 이유로 메시지 인증 코드를 사용한다. 공격 호스트(20A)가 해시 함수 H()를 알고 있을 경우, 공격 호스트(20A)가 희생 호스트(20V)로 올바른 S3를 보낼 수 있게 된다. 특히 필터링 라우터(10) 수가 적고 패킷 마킹 확률도 낮은 경우, 공격 호스트(20A)가 보낸 패킷은 마킹되지 않은 채로 희생 호스트(20V)에 도달할 수 있기 때문에, 공격 호스트(20A)는 스푸핑된 마킹을 사용하여 마킹 재조립을 방해할 수 있다.

[0067] 이를 막기 위해, 메시지 인증 코드는 목적지 IP 주소 및 필터링 라우터(10)의 비밀키를 사용하여 산출된다. 메시지 인증 코드 자체가 목적지 IP 주소에 종속적이기 때문에, 공격 호스트(20A)는 패킷을 필터링 라우터(10)를 경유하여 자신에게로 오게 하는 기법으로 메시지 인증 코드를 알아낼 수 없다.

[0068] 그러나, 메시지 인증 코드의 길이가 각각 6비트에 불과하므로, 공격 호스트(20A)가 무차별 대입 공격(brute force attack)을 사용하여 다양한 메시지 인증 코드를 보내어 희생 호스트(20V)의 마킹 재조립을 방해하는 경우를 대비해야 한다. 이를 위해 본 발명의 일실시예에 따른 호스트(20)는 빈도 분석(frequency analysis)를 사용한다.

[0069] 빈도 분석은 본 발명의 일실시예에 따른 필터링 라우터(10)는 적응적 확률 기반으로 패킷에 마킹 정보를 삽입하므로, 올바른 S1, S2, 및 S3 조각의 빈도가 높을 것이라는 가정에 기반한다. 호스트(20)는 수신한 S1, S2, 및 S3를 빈도에 기초하여 정렬한 후, 빈도가 비슷한 S1, S2, 및 S3 조각을 사용하여 재조립한다. 동일한 필터링 라우터(10)로부터의 S1, S2, S3의 수는 공격 호스트(20A)와 희생 호스트(20V) 사이에 얼마나 많은 필터링 라우터(10)가 존재하는지와 해당 필터링 라우터(10)의 패킷 마킹 확률에 상관없이 유사할 것이기 때문이다.

[0070] 메시지 인증 코드가 주기적으로 변경되더라도 호스트(20)는 새로운 메시지 인증 코드를 알아낼 수 있다. 결국에는 새로운 메시지 인증 코드가 오래된 메시지 인증 코드보다 많아질 것이기 때문이다.

[0071] 가장 높은 빈도를 갖는 S1, S2, 및 S3의 재조립이 실패하면, 호스트(20)는 해당 S1, S2, 및 S3의 카운트를 0으로 재설정한다. 이는 다음 재조립 시도시에 동일한 S1, S2, 및 S3를 선택하는 것을 막기 위함이다.

[0072] 이상의 모든 패킷 마킹 정보 재조립 및 검증 방법은 필터링 라우터(10)에서도 필터를 전파할 다른 필터링 라우터(10)의 주소를 산출하기 위해 사용될 수 있다. 예를 들어, 필터링 라우터(10)는 공격 트래픽의 전송 경로상에 위치해 있으면서 공격 호스트(20A)에 좀더 가까운 필터링 라우터(10)의 주소를 패킷 마킹 정보 재조립을 통해 도출할 수 있다.

[0073] 즉, 마킹 정보는 분할된 필터링 라우터(10)의 주소에 기초로 여러 가지 유형으로 생성되어, 각 패킷별로 다른 유형의 마킹 정보가 삽입되며, 마킹 정보가 포함되어 있는 일련의 패킷을 수신한 호스트(20) 또는 다른 필터링 라우터(10)에 의해 재조립되어 사용된다.

[0074] 희생 호스트(20V)는 공격이라 의심되는 트래픽 흐름과 관련된 세가지 유형의 마킹 정보(S1, S2, 및 S3)를 수신하였을 때, 전술한 방법을 사용하여 마킹 정보를 재조립하고 검증한 후, 그 결과로 도출된 필터링 라우터(10)의 주소를 사용하여 해당 필터링 라우터(10)로 필터 요청을 발송한다. 필터 요청은 Req{A, V, CHK}의 형태를 가질 수 있다. 즉, 필터 요청은 공격 호스트(20A) 정보, 희생 호스트(20V) 정보, 및 체크섬(CHK)을 포함할 수 있다.

[0075] 도 8은 본 발명의 일실시예에 따른 패킷 마킹 확률을 산출하는 실시예를 도시하고 있다.

[0076] 전술한 바와 같이, 패킷 마킹 확률은 필터링 라우터(10)의 필터링 효율에 따라 적응적으로 설정될 수 있다. 즉, 특정 네트워크 공격을 막기에 최적인 필터링 라우터(10)가 다른 필터링 라우터(10)보다 높은 패킷 마킹 확률로 자신이 수신하고 전달하는 패킷에 마킹할 수 있다.

[0077] 필터링 효율은 전술한 바와 같이, 필터링 라우터(10)가 패킷의 송신자로부터 얼마나 가까이 있는가에 따라, 가까울수록 높은 확률이 설정된다. 또한 필터링 라우터(10)의 가용 리소스가 얼마나 남아 있는가에 따라, 가용 리소스가 많을수록 높은 확률이 설정된다. 또한 필터링 라우터(10)가 얼마나 많은 링크를 가지고 있는가에 따라, 링크 수가 많을수록 높은 확률이 설정된다.

[0078] 즉, 필터링 라우터(10)는 자신이 공격 호스트(20A)에 가까이 있고, 필터를 저장할 수 있는 공간이 많이 남아 있으며, 연결되어 있는 다른 라우터 수가 많을수록, 높은 확률로 자신의 정보를 패킷에 마킹하게 된다. 이는 해당 필터링 라우터(10)가 서비스 거부 공격 트래픽 등의 악성 트래픽을 차단할 경우 그 효과가 높음을 의미한다.

[0079] 이들 기준은 도시된 수식들에서 각각 HOP(Hop count from attacker), RES(Resource Availability), 및 DEG(Link Degree)로 표현되어 있다.

[0080] HOP 산출 수식(e1)은 어떻게 IP 패킷의 TTL 값에 기초하여 패킷의 송신지로부터의 홉 수(hop count)를 산출할 수 있는지를 보여준다. HOP 산출에 TTL을 사용할 수 있는 이유는 TTL 값이 라우터를 통과할 때마다 감소하기 때문이다. 패킷이 얼마나 많은 라우터를 통과했는지를 나타내는 홉 수 h는 현재 TTL과 초기 TTL의 감산을 통해 산출될 수 있다. hmax는 최대 홉 수를 의미하는데, 일반적으로 인터넷에서 패킷 송신지와 패킷 수신지 사이의 최대 홉 수는 대략 30인 것으로 밝혀졌다.

[0081] 초기 TTL 값은 패킷 송신지(예: 공격 호스트(20A) 또는 적법 호스트(20L))의 운영 체제에 따라 다르다. 예를 들어, 리눅스 등 유닉스 기반 운영 체제들은 일반적으로 초기 TTL 값이 64이며, 윈도즈 시리즈는 128이다.

[0082] 따라서 예를 들어, 초기 TTL 값이 운영 체제에 따라 64 또는 128이라고 가정했을 때, 필터링 라우터(10)가 수신한 패킷의 TTL 값이 45라면, 해당 패킷의 초기 TTL은 64일 것임을 유추할 수 있다. 최대 홉 수가 30이라면 초기 TTL이 128이 될 수 없을 것이기 때문이다.

[0083] 따라서 본 발명의 일실시예에 따른 필터링 라우터(10)는 자신이 공격 호스트(20A)에 얼마나 가까이 있는지를 나타내는 HOP는 필터링 라우터(10)에서 추출된 현재 TTL 값과 이를 근거로 유추된 초기 TTL 값의 차이인 홉 수 h와 최대 홉 수인 hmax를 사용하여 산출할 수 있다.

[0084] 예를 들어, TTL에 기초하여 산출한 홉 수가 19라면, HOP은 (32-19)/19이므로 약 0.4이다.

[0085] RES 산출 수식(e2)은 필터링 라우터(10)의 필터 저장소(100)의 가용 공간을 나타낸다. 전술한 수식과 비슷하게, qmax는 필터 저장소(100)가 저장할 수 있는 최대 필터 수를, q는 현재 저장된 필터 수를 의미한다.

[0086] 예를 들어, 필터링 라우터(10)에 설치될 수 있는 최대 필터 수가 100이고, 현재 설치되어 있는 필터 수가 30이라면, RES는 (100-30)/100이므로 0.7이다.

[0087] DEG 산출 수식(e3, e4)은 필터링 라우터(10)가 토폴로지(topology) 관점에서 얼마나 중요한가를 측정한다. 즉, 허브 라우터 또는 코어 라우터와 같은, 많은 링크가 연결되어 있어, 트래픽 전달(forwarding)에 있어 중요한 역할을 담당하는 라우터에 필터가 설치되어 있다면, 악성 트래픽을 좀더 효과적으로 차단할 수 있을 것이기 때문에, 이를 나타내는 기준인 DEG 값은 연결되어 있는 링크 수가 많을수록, 즉, 필터링 라우터(10)가 네트워크의 좀더 중요한 허브로 동작할수록 더 높아야 한다.

[0088] 이를 측정하는 방법은 다양할 수 있다. 예를 들어, DEG 산출 수식(e3)은 단순히, 필터링 라우터(10)에 연결된 링크 수를 나타내는 k를 네트워크상의 필터링 라우터 당 평균 링크 연결 수를 나타내는 kavg로 나누어 DEG를 산출한다. 이때 연결 링크 수는 진입 링크 수와 진출 링크 수를 모두 포함할 수 있다.

[0089] 또다른 실시예인 수식(e4)는 패킷의 최단 경로 상에서의 해당 필터링 라우터(10)의 중요성(betweenness centrality)을 산출한다. 수식에서 s는 패킷의 송신지, d는 패킷의 목적지, m은 중간 노드를 의미한다. G(s, d)가 s에서 d까지의 경로의 수를 나타내며, G(m; s, d)는 s에서 d까지의 m을 포함하는 경로의 수를 나타낸다고 했을 때, s에서 d까지의 m을 포함하는 최단 경로의 비율은 P(m; s, d)= G(m; s, d)/G(s, d)로 표현할 수 있다. 따라서 필터링 라우터(10)를 m으로 하여 DEG를 산출할 수 있다.

[0090] 이러한 실시예는 최단 경로를 미리 알고 있어야 하므로 실용적이지는 않다. 그러나 네트워크 관리자가 각 노드

간 최단 경로에 대한 토폴로지 지식이 있을 때에는 수식 e4를 사용하여 DEG를 산출할 수 있을 것이다.

[0091] 최종적으로 적응적 패킹 마킹 확률(pa)는 세가지 기준 HOP, RES, DEG를 각각의 가중치 whop, wres, wdeg와 곱하여 합산한 후 기본 패킹 마킹 확률(pd)에 더해 산출될 수 있다.

[0092] whop, wres, wdeg 및 pd는 네트워크 환경에 따라 설정될 수 있다. 예를 들어, 네트워크에 설치되어 있는 필터링 라우터(10)의 토폴로지상 중요도가 모두 유사한 경우, DEG에 대한 가중치 wdeg는 낮게 설정되는 것이 효율적일 수 있다.

[0093] pd는 0.05%에서 50% 사이의 값으로 설정될 수 있다. 예를 들어, IP 역추적(IP traceback)을 위하여 전체 경로를 재구성하는 경우, pd는 0.05%로 설정될 수 있다. 반면, 서비스 거부 공격을 방지하기 위한 경우에는 전체 경로 재구성의 경우보다, 필터링 라우터(10)의 주소 정보가 더 중요해지므로, pd로 30%에서 50% 사이의 값을 설정할 수 있다.

[0094] pd는 pa를 산출하는 데 있어 중요하므로 적절히 설정하는 것이 바람직하다. 실험 결과, pd=50%일 때 가장 좋은 성능을 나타내는 것으로 나타났다. 예를 들어, 네트워크에 설치된 필터링 라우터(10) 비율이 10%로 낮을 때에도 공격 트래픽을 80% 차단할 수 있었다.

[0095] 도 9는 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 필터링 방법의 흐름을 도시하고 있다.

[0096] 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 필터링 방법은 크게 패킷 마킹(S100), 필터 생성(S200), 필터 전파(S300), 및 필터 관리(S400)라는 네가지 단계를 포함하고 있다.

[0097] 패킷 마킹(S100)은 전술한 바와 같이, 필터링 라우터(10)에서 수신한 패킷에 대해(S100-0), HOP, RES, 및 DEG 등의 기준에 따라 적응적으로 결정된 마킹 확률(S100-2)에 기반하여, 마킹 정보를 삽입한 후(S100-4), 전달하는(S100-5) 단계를 포함한다. 자세한 설명은 전술하였으므로 생략한다.

[0098] 또한 필터 생성(S200)은 전술한 바와 같이, 호스트(20)에서 수신한 패킷에 대해(S200-0), 마킹을 조립하여 패킷의 전송 경로상에 위치한 필터링 라우터(10)의 주소를 도출하고(S200-2), 차단이 필요한 트래픽에 대해(S200-4), 해당 필터링 라우터(10)로 필터 또는 필터 요청을 발송하는(S200-6) 단계를 포함한다. 도면은 설명의 편의상 모든 수신한 패킷에 대해 마킹을 조립하는 것을 도시하고 있으나, 상기 마킹 조립 단계(S200-2)는 차단이 필요한 트래픽이라고 판단되는 경우에 한해(S200-4) 수행될 수 있다. 자세한 설명은 전술하였으므로 생략한다.

[0099] 필터 전파(S300)는 전술한 바와 같이, 필터링 라우터(10)가 수신한 필터에 대해(S300-0), 호스트(20)에서와 마찬가지 방법으로 마킹을 조립하여 공격 패킷의 경로 상에 위치한 다음 필터링 라우터(10)의 주소를 도출하고(S300-2), 패킷 전파가 필요한 경우(S300-4) 필터를 전파하는(S300-6) 단계를 포함한다. 도면은 설명의 편의상 수신한 필터에 대해 바로 마킹을 조립하는 것으로 도시하고 있으나, 수신한 필터는 후술할 필터 관리 단계(S400)와 연계하여 필터 저장소(100)에 저장된 후, 유용한 필터라고 판단되는 경우에 한해(S300-4) 마킹 조립 단계(S300-2)를 수행할 수 있다. 자세한 설명은 호스트(20)에서 수행하는 상기 단계(S200)와 유사하므로 생략한다.

[0100] 필터 관리(S400)는 전술한 바와 같이, 필터 스케줄링 정책을 사용하여, 가장 효과적인 필터만이 유지되도록 필터의 수를 관리하는 단계이다.

[0101] 단순하게 설명하면, 유용 필터라고 판단되면(S400-0) 해당 필터의 우선 순위를 높이고(S400-2), 무용 필터라고 판단되면(S400-4) 해당 필터를 폐기, 즉, 필터 저장소(100)에서 해당 필터를 제거하는(S400-6) 단계이다.

[0102] 필터 스케줄링 정책은 운영 체제의 가장 효과적인 페이지만이 캐시 메모리 내에 유지되록 하는 캐시 페이지 교체 정책과 유사할 수 있다. 가장 널리 사용되는 캐시 페이지 교체 정책에는 LRU(least recently used)와 ARC(adaptive replacement cache)가 있는데, ARC 쪽의 성능이 더 좋으므로, 본 발명의 일실시예에 따른 필터링 라우터(10)는 ARC에 기반한 필터 스케줄링 정책을 사용하되, 네트워크 환경은 악성 코드 및 공격 호스트(20A)가 존재할 수 있는 환경이므로, 이에 맞게 수정하여 사용한다.

[0103] 본 발명의 일실시예에 따른 필터링 라우터(10)의 필터 저장소(100)는 고스트 리스트(ghost list)와 필터 리스트(filter list)라는 두가지 필터 목록을 유지할 수 있다. 고스트 리스트는 의심 필터를 저장하며, 필터링 라우터(10)는 수신한 필터를 일단 고스트 리스트에 저장한다. 편의상 이를 고스트 필터(ghost filter)라고 부르도록 한다. 필터링 라우터(10)는 필터 리스트에 저장되어 있는 필터만을 실제로 트래픽을 차단하는 데 사용한다.

[0104] 필터링 라우터(10)는 주기적으로 고스트 리스트 및 필터 리스트에 저장되어 있는 각 필터의 빈도(frequency)와

최신 정도(recency)를 함께 고려하여 필터 점수(filter score)를 산출하여, 이를 필터 관리의 근거로 사용한다.

[0105] 필터 점수가 기지정된 임계값, 이른바 승격 임계값(promotion threshold)를 넘어서는 고스트 필터는 필터 리스트로 승격된다. 필터 리스트가 꽉 차 있는 경우에는 고스트 필터의 필터 점수가 필터 리스트에 저장되어 있는 필터들의 필터 점수 중에서 가장 낮은 필터 점수보다 높은 경우에만 승격된다.

[0106] 즉, 필터링 라우터(10)는 수신한 필터를 바로 설치하는 대신에, 먼저 고스트 리스트에 저장한 후, 빈도 및 최신 정도를 고려하였을 때 유용하다고 판단되는 고스트 필터만을 선별하여 필터 리스트에 저장하여 설치한다. 이러한 방법으로 최적의 필터를 유지할 수 있다.

[0107] 필터 I에 대한 t 시점에서의 빈도 점수를 F, 최신 정도 점수를 R라고 하면, F는 I가 사용된 횟수로 구할 수 있으며, R은 tc를 I와 관련된 현재 패킷의 도착 시점, tp를 이전 패킷의 도착 시점이라고 할 때, R= (tc-tp)로 산출될 수 있다. 따라서, 이들에 대한 가중치를 각각 wF, wR이라 하면, t 시점에서의 필터 I의 필터 점수 P(t)는 "P(t)= wF x F(t) + wR x R(t)= wF x F(t) + wR x (tc-tp)"를 이용하여 산출될 수 있다. 단, P(0)=0이다.

[0108] 필터 점수는 이동 평균(movitg average) 기법을 사용하여 추적될 수 있다. 이동 평균을 계산할 윈도우(witdow) 크기를 n, S(t)를 해당 윈도우 동안의 필터 I에 대한 필터 점수의 이동 평균이라고 하면, S(t)는 최근 n개의 S(t)를 사용하여 산출된다. 따라서, 일실시예에서 이동 평균은 "S(t)= S(t-1) - (P(t-n)/t) + (P(t)/t) - r"를 이용하여 산출될 수 있다. 이동 평균은 공지 기술이므로, 자세한 설명은 생략한다.

[0109] 단, 여기서 r은 필터 점수를 감소시킬 수 있는 벌칙 점수로, 필터 리스트에서 쫓아낼 무용 필터를 선별하기 위해 사용된다. r에 의해 S(t)가 승격 임계값보다 낮아진 필터는 고스트 리스트로 쫓겨나고, 결국 폐기된다.

[0110] 이는 필터링 라우터(10)에서 수행되는 암묵적 필터 폐기 방식이다. 희생 호스트(20V)가 필터링 라우터(10)로 필터 폐기 요청을 보내는 명시적 필터 폐기 방식을 사용할 수도 있으나, 이는 해당 필터 폐기 요청 인증을 위해 키(key)가 설정된 안전한 채널이 필요하다는 문제가 있다. 따라서 본 발명의 일실시예에 따른 필터링 라우터(10)는 명시적인 필터 폐기 요청 없이, 필터 점수가 낮아 무용 필터로 판단된 필터를 자동 폐기한다.

[0111] 도 10 및 도 11은 각각 종래의 고정된 패킷 마킹 확률을 사용했을 때와 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 필터링의 성능을 분석한 그래프를 도시하고 있다.

[0112] 희생 호스트(20V)가 마킹을 수신할 확률이 희생 호스트(20V)로부터의 홉(hop) 수에 따라 어떻게 달라지는지를 보면, 본 발명의 일실시예에 따른 적응적 확률 기반 패킷 필터링의 성능이 더 좋음을 알 수 있다.

[0113] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0114] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0115] 10: 적응적 확률 기반 패킷 필터링 라우터

100: 필터 저장소

102: 마킹 확률 결정부

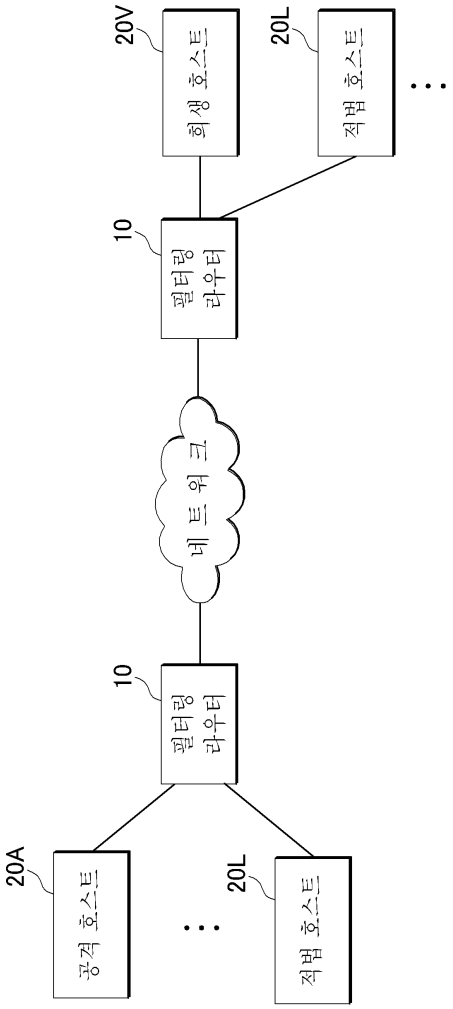
104: 패킷 마킹부

106: 필터 관리부

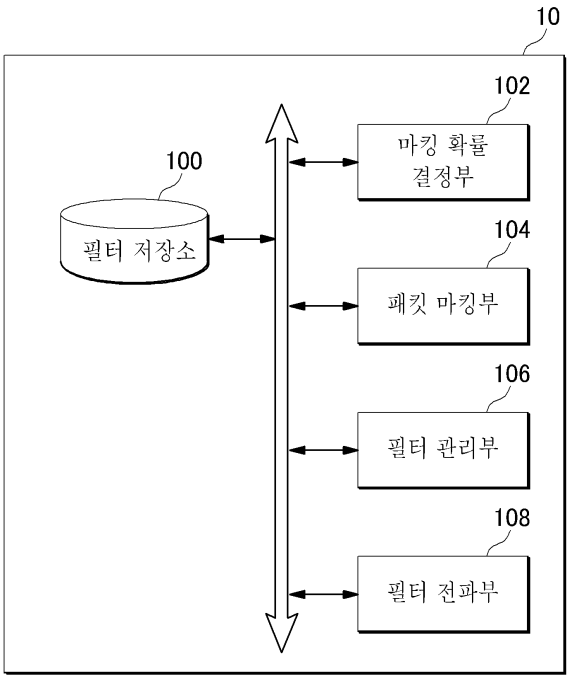
108: 필터 전파부

도면

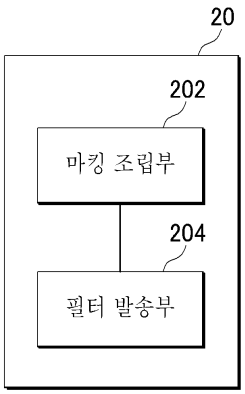
도면1


20V
희생 호스트
20L
적법 호스트
...
10
필터링 라우터
네트워크
10
필터링 라우터
20A
공격 호스트
...
20L
적법 호스트

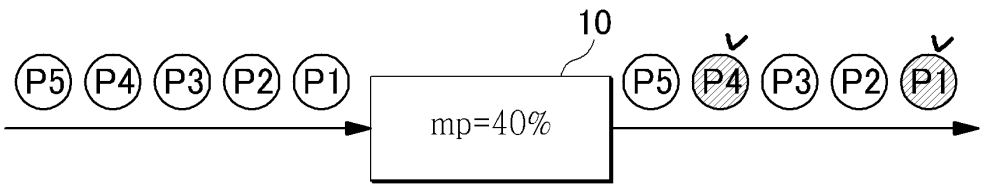
도면2


10
102
마킹 확률 결정부
100
필터 저장소
104
패킷 마킹부
106
필터 관리부
108
필터 전파부

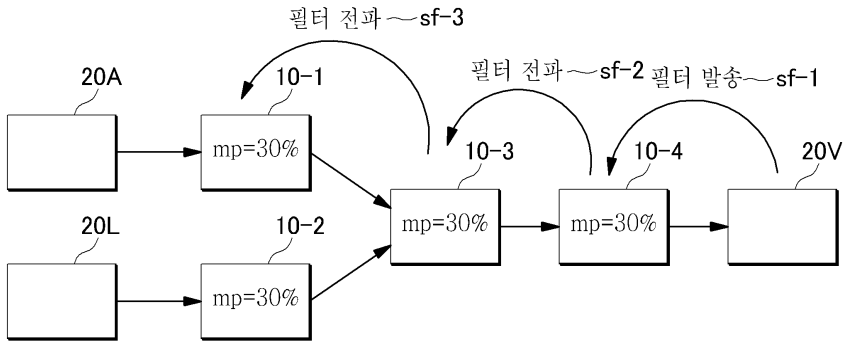
도면3


20
202
마킹 조립부
204
필터 발송부

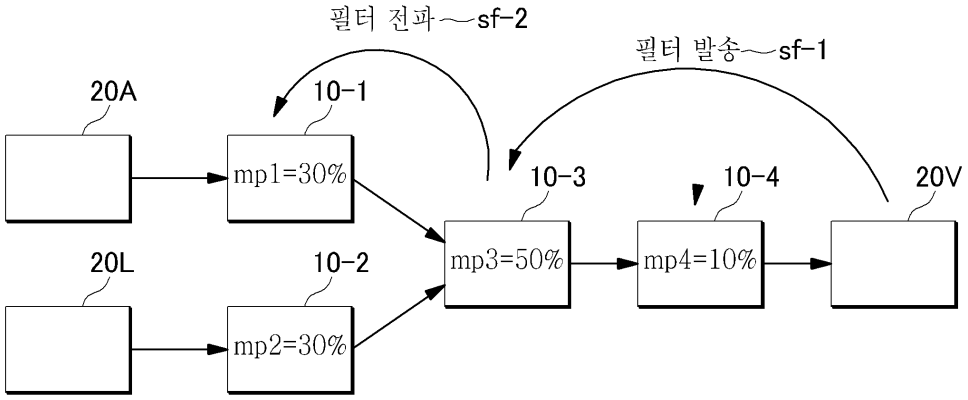
도면4


10
P5
P4
P3
P2
P1
mp=40%
P5
P4
P3
P2
P1

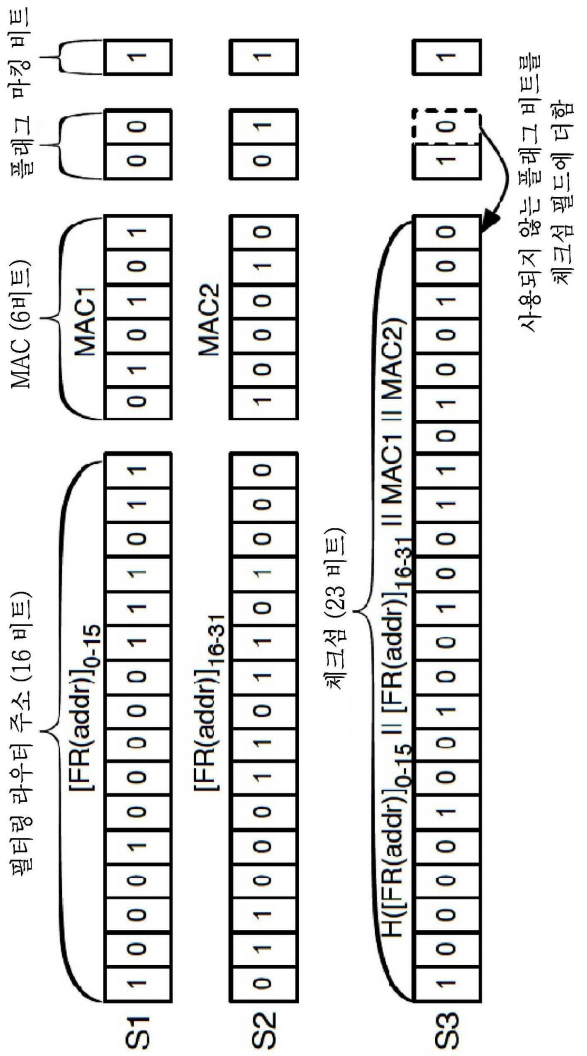
도면5


필터 전파 ~ sf-3
20A
10-1
필터 전파 ~ sf-2
필터 발송 ~ sf-1
mp=30%
10-3
10-4
20V
20L
10-2
mp=30%
mp=30%
mp=30%

도면6


필터 전파 ~ sf-2
필터 발송 ~ sf-1
20A
10-1
mp1=30%
10-3
10-4
20V
20L
10-2
mp3=50%
mp4=10%
mp2=30%

도면7


필터링 라우터 주소 (16 비트)
MAC (6비트)
플래그
마킹 비트
[FR(addr)]0-15
MAC1
[FR(addr)]16-31
MAC2
체크섬 (23 비트)
H([FR(addr)]0-15 || [FR(addr)]16-31 || MAC1 || MAC2)
사용되지 않는 플래그 비트를
체크섬 필드에 더함
S1
S2
S3

도면8

$$HOP = \frac{h_{max} - h}{h_{max}}, \quad \sim e1$$

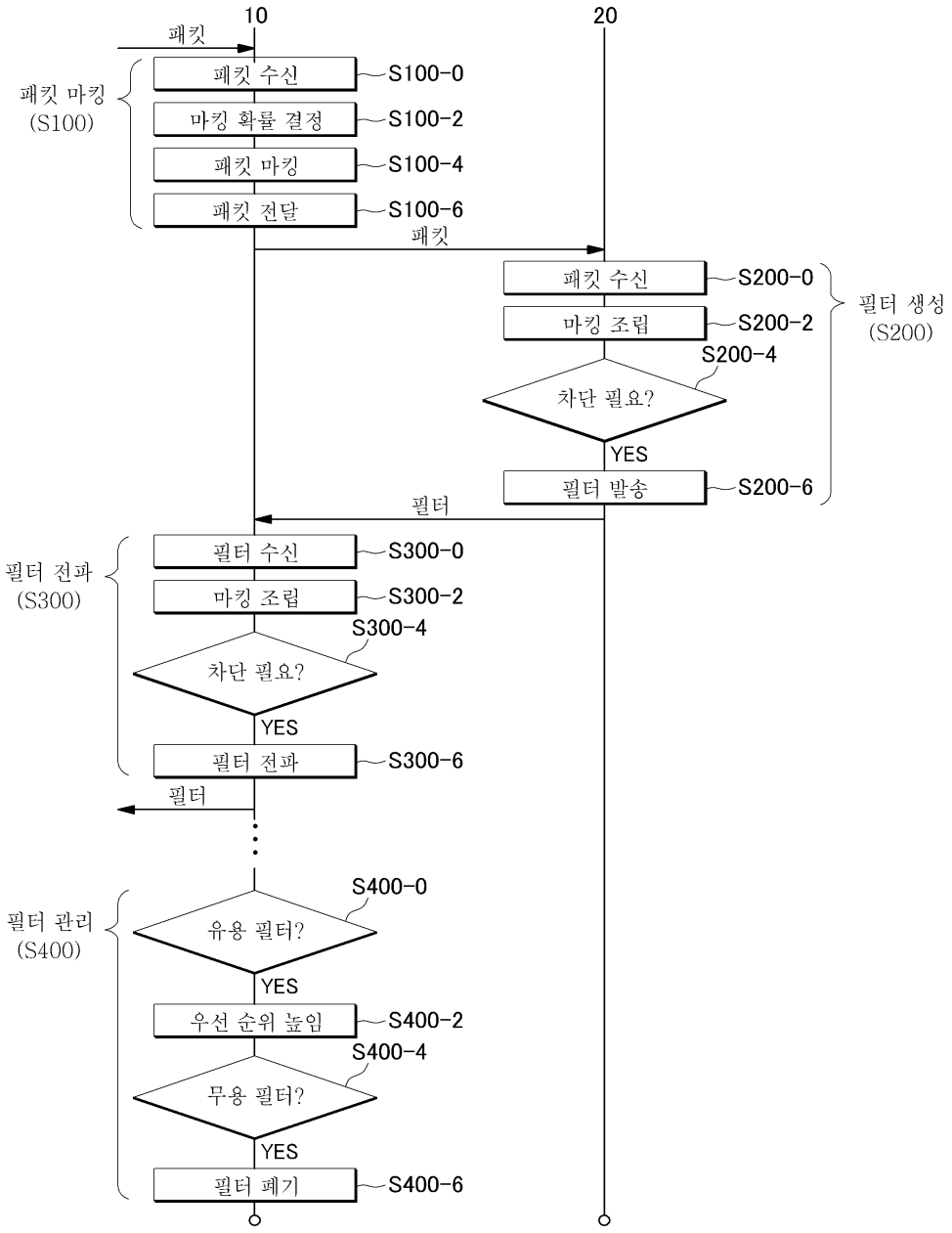
$$RES = \frac{q_{max} - q}{q_{max}} \sim e2$$

$$DEG = \frac{k}{k_{avg}} \sim e3$$

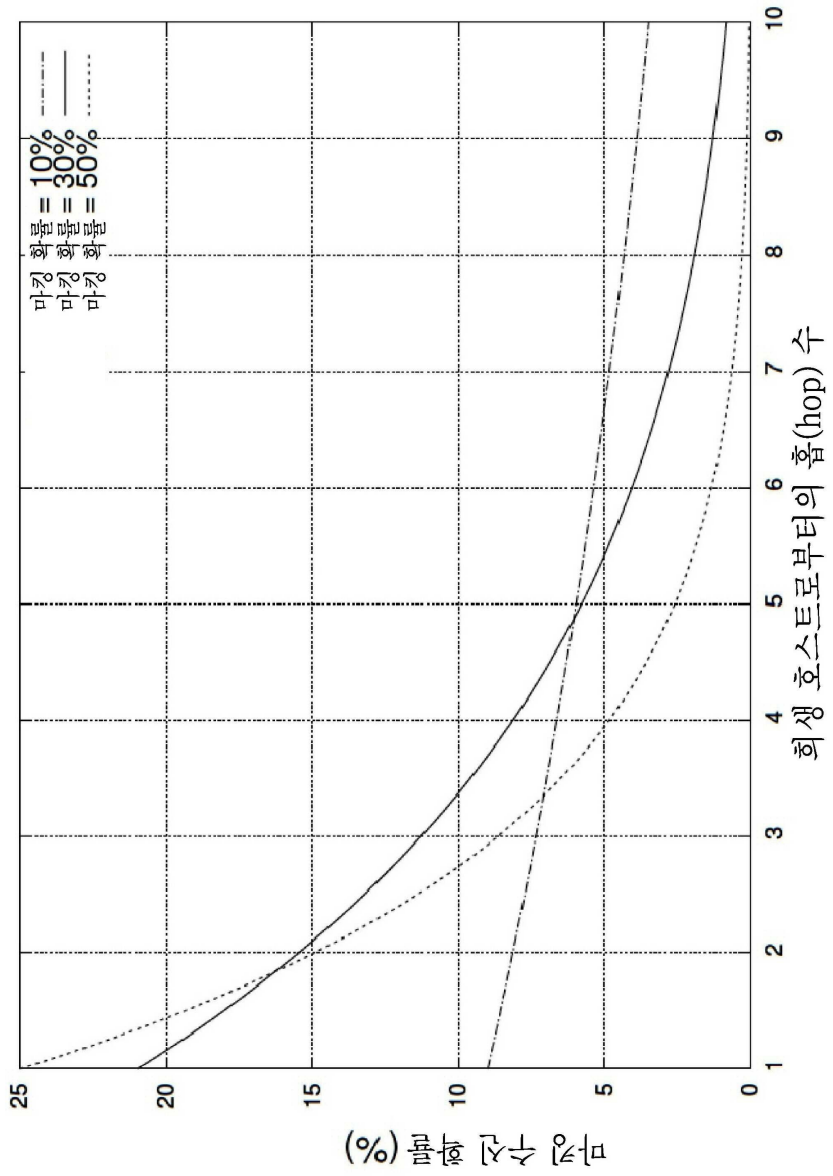
$$DEG = \sum_{s} \sum_{s \neq d} P(m; s, d) \sim e4$$

$$mp = p_d + (w_{hop} \cdot HOP) + (w_{res} \cdot RES) + (w_{deg} \cdot DEG) \sim e5$$

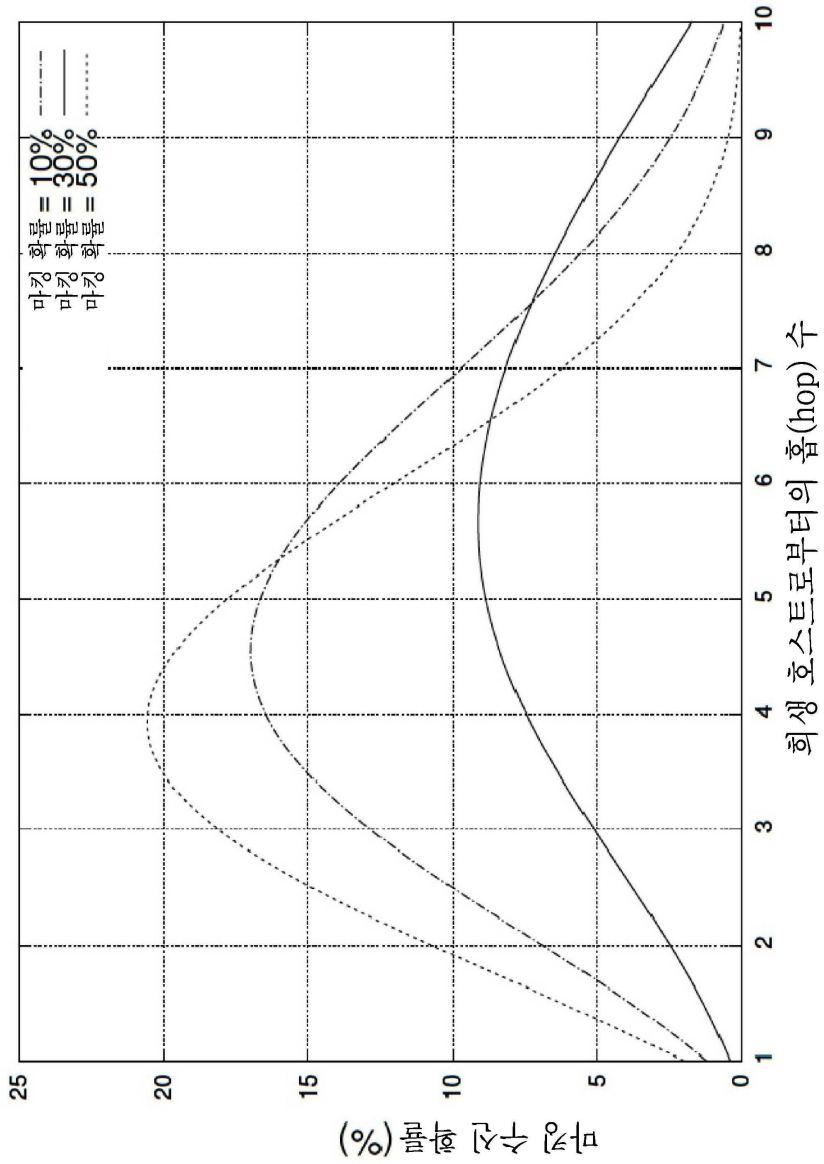
도면9


10
20
패킷
패킷 수신
S100-0
패킷 마킹
(S100)
마킹 확률 결정
S100-2
패킷 마킹
S100-4
패킷 전달
S100-6
패킷
패킷 수신
S200-0
필터 생성
(S200)
마킹 조립
S200-2
S200-4
차단 필요?
YES
필터 발송
S200-6
필터
필터 수신
S300-0
필터 전파
(S300)
마킹 조립
S300-2
S300-4
차단 필요?
YES
필터 전파
S300-6
필터
S400-0
필터 관리
(S400)
유용 필터?
YES
우선 순위 높임
S400-2
S400-4
무용 필터?
YES
필터 폐기
S400-6

도면10


마킹 확률 = 10%
마킹 확률 = 30%
마킹 확률 = 50%
마킹 수신 확률 (%)
0
5
10
15
20
25
1
2
3
4
5
6
7
8
9
10
희생 호스트로부터의 홉(hop) 수

도면11


마킹 확률 = 10%
마킹 확률 = 30%
마킹 확률 = 50%
마킹 수신 확률(%)
0
5
10
15
20
25
1
2
3
4
5
6
7
8
9
10
희생 호스트로부터의 홉(hop) 수