



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0009813
(43) 공개일자 2011년01월31일

(51) Int. Cl.

H04L 12/22 (2006.01) H04L 12/24 (2006.01)

(21) 출원번호 10-2009-0067208

(22) 출원일자 2009년07월23일

심사청구일자 2009년07월23일

(71) 출원인

충남대학교산학협력단

대전광역시 유성구 공동 220번지 충남대학교

이형우

경기도 용인시 기흥구 중동 성산마을서해그랑블 3101동 501호

한신대학교 산학협력단

경기 오산시 양산동 한신대학교내

(72) 발명자

이형우

경기도 용인시 기흥구 중동 성산마을서해그랑블 3101동 501호

김태수

경기도 가평군 가평읍 읍내9리 445-2번지

(뒷면에 계속)

(74) 대리인

특허법인태동

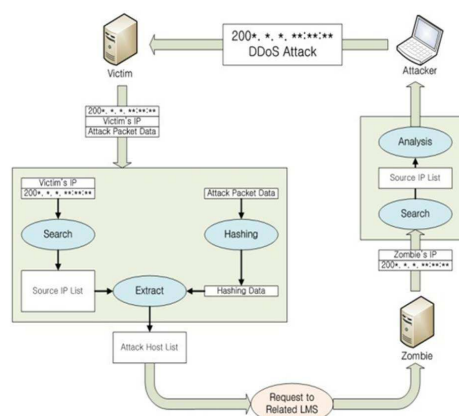
전체 청구항 수 : 총 19 항

(54) 올아이피네트워크 환경의 공격 탐지 및 추적 시스템 및 방법

(57) 요약

본 발명은 올아이피네트워크 환경의 공격 탐지 및 추적 방법에 관한 것으로, 복수개의 소스 및 목적지 단말기, 싱크홀라우터(시스템)를 포함한 복수개의 라우터(router)(시스템), 매니저(서버컴퓨터시스템)(이하, 매니저 시스템이라 함)가 서로 유무선 통신망으로 연결된 올아이피네트워크 환경의 공격 탐지 및 추적 시스템을 이용한 올아이피네트워크 환경의 공격 탐지 및 추적 방법에 있어서, 매니저 시스템, 라우터간에 정보 설정을 초기화하는 제1단계와, 매니저 시스템에서 각각 라우터로 싱크홀 라우터 결정사항을 통보하는 제2단계와, 피해시스템으로부터 공격 발생에 관한 통보를 받을 경우 매니저 시스템은 공격 패킷의 해쉬 정보를 각 라우터에 전송하여 공격리스트에 등록/업데이트 하도록 하는 제3 단계와, 일반 사용자에게 의해 공격패킷이 발생하여 전송될 경우 라우터에서는 자신의 공격 리스트에 기록된 값과 일치하는 해쉬 값을 갖고 있는지 판단하는 제4단계를 포함하여 이루어진 것을 특징으로 한다.

대표도 - 도5



(72) 발명자

김득용

경기도 수원시 권선구 평동 14-5

윤하나

경기도 오산시 양산동 286-2 한신오피스텔 C동 20
5호

특허청구의 범위

청구항 1

복수개의 소스 및 목적지 단말기, 싱크홀라우터(시스템)를 포함한 복수개의 라우터(router)(시스템), 매니저(서버컴퓨터시스템)(이하, 매니저 시스템이라 함)가 서로 유무선 통신망으로 연결된 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에 있어서,

상기 매니저 시스템은

라우터를 관리하고 공격 트래픽에 대한 역추적을 위해서 여러가지 정보를 저장, 관리하는 매니저 데이터부와,

매니저 시스템이 관리하는 라우터의 정보를 관리하는 라우터 관리부와,

공격 트래픽의 역추적을 위한 관리하는 공격패킷 관리부와,

트래픽의 송수신처리를 위한 프로토콜처리부를 포함하여 이루어지고,

상기 라우터 시스템은

공격 패킷의 역추적을 위한 정보 기록하는 라우터 데이터부와

라우터를 지나가는 패킷의 추출 및 해쉬 적용을 위한 패킷 처리부

블룸 필터를 이용하여 패킷의 경로를 확인하는 블룸 필터 처리부와

현재 패킷이 공격 패킷인지 판단하는 공격 패킷 처리부

싱크홀 라우터로 전송되는 원본 공격 패킷들을 관리하는 싱크홀 라우터 데이터부,

공격패킷의 목록을 관리하는 공격패킷 처리부,

패킷 데이터의 송수신처리를 위한 프로토콜 처리부를 포함하여 이루어진 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템.

청구항 2

제 1항에 있어서, 상기 매니저 데이터부는

관리되는 라우터의 ID와 프로토콜 통신을 위한 통신 정보, 해쉬 함수의 목록들을 포함하는 라우터 정보 목록 및 해쉬함수 목록부,

실제 공격이 이루어진 패킷들의 공격 패킷 목록부,

각 라우터에 적용된 공격 패킷에 대해서 싱크홀 라우터가 받은 공격 패킷들을 보낸 라우터들의 ID로서, 공격자의 근원지 혹은 공격 경로를 분석하기 위한 정보인 공격 경로 목록부를 포함하여 이루어진 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템.

청구항 3

제 1 항에 있어서, 상기 라우터 관리부는

라우터의 목록을 생성하는 라우터 목록 생성부,

라우터의 해쉬 정보를 획득하는 작업을 수행하는 해쉬함수 정보관리부,

매니저 시스템에 의해서 관리되어 싱크홀 라우터의 기능으로 전환할 수 있도록 하는 싱크홀 라우터 설정부를 포함하여 이루어진 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템.

청구항 4

제 1 항에 있어서, 상기 공격 패킷 관리부는

모든 라우터를 대상으로 공격 패킷의 해쉬 값을 전송하여 공격 패킷을 등록하는 공격 패킷 등록부,

패킷 경로 정보를 수집하는 패킷 경로정보 수집부,

공격 트래픽을 역추적 하기 위한 역추적부를 포함하여 이루어진 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템.

청구항 5

제 1 항에 있어서, 상기 라우터 시스템은 자신을 지나가는 패킷에 대해 해쉬 함수를 적용하여 두 개의 해쉬 값을 추출하고, 추출된 해쉬 값은 블록 필터에 적용 함으로써 패킷이 지나갔는지의 유무를 판단할 수 있는 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템.

청구항 6

제 1 항에 있어서, 상기 일반 라우터의 경우는 역추적을 위한 블록 필터와 싱크홀 라우터로 보내기 위한 공격 패킷의 해쉬 정보를 가지고 있으며, 싱크홀 라우터는 추가로 원본 공격 패킷의 목록을 가지고 있는 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템.

청구항 7

제 1 항에 있어서, 라우터의 경우 해쉬된 값을 이용해서 자신이 가지고 있는 공격 패킷의 리스트를 통해 싱크홀 라우터로 전송할지의 여부를 판단하는 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템.

청구항 8

제 1 항에 있어서, 싱크홀 라우터는 스스로 처리를 하며, 자신이 처리하거나 다른 라우터로 받은 공격 패킷을 기록하고 어느 라우터로부터 왔는지 매니저 시스템에 알리는 기능을 수행하는 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템.

청구항 9

제 1 항에 있어서, 상기 라우터 데이터부는 대상 단말과 프로토콜 통신을 위한 네트워크 정보를 가지는 매니저 시스템의 네트워크 정보부 및 싱크홀 라우터의 네트워크 정보부와,

블록 필터 적용과 공격 패킷 판단을 위해서 공격 패킷에 대해 두 개의 해쉬 함수를 이용하여 각기 다른 두개의 해쉬 값을 추출하기 위한 해쉬 함수부,

패킷이 자신을 지나갔는지를 효과적이고 효율적인 검색하기 위해 사용되는 상기 블록 필터부,

매니저 시스템으로부터 알려진 공격 패킷에 대해 자신이 수행하는 해쉬 함수를 이용한 해쉬 값 두 개를 하나의 원소로 하여 공격 패킷의 해쉬 정보 목록으로 가지고 있는 공격 패킷의 해쉬 정보 목록부를 포함하여 이루어지며, 이 목록의 비교를 통해서 패킷에 대해 공격 패킷인지를 판단하며, 공격 패킷으로 판단될 경우 싱크홀 라우터로 보내게 되는 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템.

청구항 10

제 1 항에 있어서, 상기 패킷 처리부는

역추적에 필요한 작업을 수행하기 위해 라우터는 자신을 지나가는 IP 패킷을 추출하고, 추출된 패킷의 IP 헤더의 정보 등의 값들을 분석함으로써 이후 역추적을 위한 작업이 진행되도록 하는 패킷 추출부,

패킷 정보를 해쉬하기 전에 IP 헤더의 특정 정보와 페이로드(Payload)의 일부분을 추출하기 위한 패킷 정보 추출부와,

상기 24바이트의 추출된 정보를 두 개의 해쉬 함수를 이용하여 32비트의 두 해쉬 값을 추출하는 해쉬 함수 적용부를 포함하여 이루어진 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템.

청구항 11

제 1 항에 있어서, 상기 블록 필터 처리부는 추출된 두 해쉬 값은 먼저 패킷이 지나갔음을 기록하기 위해 블록 필터를 적용하는 블록 필터 기록부와,

블록 필터를 이용하여 공격 패킷이 자신을 지나갔음을 확인하고 그 결과를 매니저 시스템에 다시 전송함으로써 매니저 시스템이 공격 경로를 확인하도록 하는 블록 필터 검사부를 포함하여 이루어지고,

이후에 bloom 필터를 이용하여 패킷이 지나갔음을 판단함으로써 상기 매니저 시스템이 공격 트래픽의 역추적을 하도록 하는 것을 특징으로 하는 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템.

청구항 12

제 1 항에 있어서,

상기 공격패킷 처리부는 패킷을 라우팅 하기 전에 추출된 두 해쉬 값이 공격 패킷의 해쉬 목록에 유무를 확인 하며, 공격 패킷의 해쉬 목록은 매니저 시스템으로부터 전송받은 공격 패킷의 해쉬 정보이므로, 해쉬 목록에 두 해쉬 값이 존재하게 되면 공격 패킷으로 판단하고 라우팅을 승인하지 않으며, 해당 공격 패킷을 싱크홀 라우터로 전송하는 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템.

청구항 13

복수개의 소스 및 목적지 단말기, 싱크홀라우터(시스템)를 포함한 복수개의 라우터(router)(시스템), 매니저(서버컴퓨터시스템)(이하, 매니저 시스템이라 함)가 서로 유무선 통신망으로 연결된 제 1 항의 올아이피네트워크 환경의 공격 탐지 및 추적 시스템을 이용한 올아이피네트워크 환경의 공격 탐지 및 추적 방법에 있어서,

매니저 시스템, 라우터간에 정보 설정을 초기화하는 제 1단계와,

매니저 시스템에서 각각 라우터로 싱크홀 라우터 결정사항을 통보하는 제 2단계와,

피해시스템으로부터 공격 발생에 관한 통보를 받을 경우 매니저 시스템은 공격 패킷의 해쉬 정보를 각 라우터에 전송하여 공격리스트에 등록/업데이트 하도록 하는 제3 단계와,

일반 사용자에게 의해 공격패킷이 발생하여 전송될 경우 라우터에서는 자신의 공격 리스트에 기록된 값과 일치하는 해쉬 값을 갖고 있는지 판단하는 제4단계를 포함하여 이루어진 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 방법.

청구항 14

제 13 항에 있어서, 상기 제4단계에서 공격리스트에 기록된 값과 일치하는 해쉬값을 갖고 있지 않은 경우 일반 패킷으로 분류하여 bloom필터에 기록하고 목적지로 전송하는 것을 특징으로 하는 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 방법.

청구항 15

제 13 항에 있어서, 상기 제4단계에서 공격리스트에 기록된 값과 일치하는 해쉬 값이 라우터내 bloom필터에 기록된 값과 동일한 형태일 경우, 싱크홀 라우터로 전송하고 싱크홀 라우터는 매니저 시스템에 통보하고, 각 라우터는 자신이 설정한 해쉬 함수를 이용하여 계속적으로 bloom필터 값을 생성/갱신하는 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 방법.

청구항 16

제 13 항에 있어서,

상기 제 1 단계는 매니저에서 주변에 있는 라우터와 통신하면서 해쉬함수 선택을 요청하고, 각 라우터는 함수 인덱스 값을 회신하는 단계인 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 방법.

청구항 17

제 13 항에 있어서, 상기 매니저에서 관리하는 데이터 구조는 라우터 아이디, 싱크홀 라우터 아이디, 해쉬 함수 인덱스, 해쉬 함수 리스트, 공격패킷 리스트, 추적 리스트를 포함하는 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 방법.

청구항 18

제 13 항에 있어서, 상기 라우터에서 관리하는 데이터 구조는 매니저 어드레스, 싱크홀 라우터 어드레스, 해쉬 함수1, 해쉬 함수2, 사용싱크홀 라우터의 라우터 아이디 및 공격 패킷 리스트, 공격 해쉬 값 리스트, bloom 필터(Bloom filter)인 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 방법.

청구항 19

제 13 항에 있어서, 상기 송수신되는 프로토콜 메시지 구조는 1바이트 스타트 코드, 8바이트 메시지 헤더, 2~n 바이트 메시지 바디로 이루어지고, 8바이트 메시지 헤더는 2바이트 소스 아이디, 2바이트 목적지 아이디, 2바이트 길이, 2바이트 CRC를 포함하는 것을 특징으로 하는 올아이피네트워크 환경의 공격 탐지 및 추적 방법.

명세서

발명의 상세한 설명

기술 분야

[0001] 본 발명은 올아이피네트워크 환경의 공격 탐지 및 추적 시스템 및 방법에 관한 것으로, 더욱 상세하게는, All-IP 네트워크 환경을 중심으로 DDoS 공격 등이 발생하였을 경우 공격 근원지 정보를 역추적(Traceback)할 수 있는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템 및 방법에 관한 것이다.

배경 기술

[0002] 최근 All-IP 네트워크 환경이 구축되면서 다양한 형태의 트래픽이 송수신되고 있으며, 이와 더불어 다양한 형태의 공격이 급증하고 있어 이에 대한 능동적 대응 방안이 제시되어야 하는 실정이다.

[0003] 이 분야의 종래의 기술로는 SPIE 시스템 기반 해쉬 함수와 Bloom Filter 방식을 적용하여 각각의 라우터에서 특정 패킷이 거쳐 갔는지를 검사하는 방법이 있었다. 그리고 라우터에 대한 공격이 발생하였을 경우, BGP 프로토콜 등을 사용하여 패킷의 전송 경로를 특정 라우터 쪽으로 수정/전달하는 Sinkhole 라우터 기법이 있었다. 따라서 기존 방식에 대한 분석을 통해 All-IP 네트워크 환경에 적합한 공격 추적 방법을 제시할 필요가 있다.

[0004] 도 1은 종래기술에 따른 원격구동 블랙홀 라우팅 기술을 설명하기 위한 개념도이고, 도 2는 종래기술에 따른 목적지 기반 원격구동 블랙 라우팅 기술을 개략적으로 설명하기 위한 시스템 구성도이고, 도 3은 종래기술에 따른 싱크홀(sinkhole) 기술기반 블랙 스캐터(black scatter)현상을 이용한 공격경로 추적기술을 설명하는 시스템 구성도이다.

[0005] <All-IP 네트워크>

[0006] All-IP 네트워크란 인터넷 프로토콜인 IP를 기반으로 서로 다른 네트워크가 통합된 구조를 갖는 차세대 네트워크를 의미한다. All-IP 네트워크에서는 PSTN과 같은 유선 전화망과 IMT-2000 망, 무선 망, 패킷 데이터 망과 같은 기존의 통신망이 모두 IP 기반의 하나의 망으로 통합되므로 음성, 데이터, 멀티미디어 등을 패킷을 기반으로 처리하는 것이 가능해진다. 즉, 패킷 네트워크와, IP Telephony를 기반으로 하는 망구조를 갖게 되는 것이다.

[0007] <기존의 전향적 역추적 기법/문제점>

[0008] 가)링크 검사법

[0009] 이 방법은 Hop-to-hop 추적방식에 해당하는 것으로, 각 라우터에서는 연결된 링크에 대해 검사하면서 DoS 공격의 여부를 검사하게 된다. 하지만 이 방법은 자동화된 역추적 방법을 제공하지 못하고, 직접적으로 패킷 전송 경로로 조합/판별하는 방법에 해당한다. 따라서 네트워크 관리 측면에서 오버헤드가 발생한다는 단점이 있다.

[0010] 나)로깅 기법

[0011] 라우터에서 전송된 패킷에 대한 특성 등을 기록해 놓은 후에 데이터 마이닝 등의 추론 시스템을 적용하여 공격 근원지를 검출하는 기법으로, 많은 양의 정보를 저장/관리해야 하기 때문에 효율성이 떨어진다는 단점이 있다.

[0012] 다)PPM 기법

[0013] 라우터에서 IP 패킷에 라우터 자신을 거쳐서 전달된 정보에 대해 삽입하는 방식으로, IP 헤더에서 변형 가능한 필드에 대해서 라우터에 해당하는 주소 정보를 마킹하여 다음 라우터로 전달하는 기법이다.

[0014] 라)iTrace 기법

[0015] ICMP와 유사하게 전 단계 라우터 정보와 다음 단계 라우터 정보를 메시지에 포함시키고 패킷의 payload정보 등

을 포함하여 전달하는 방식이다. PPM 기법과 마찬가지로 DDoS공격에 대응하기 위해 많은 정보가 필요하기 때문에 개선된 기법이 제시되어야 한다.

[0016] <대응적 역추적 기법>

[0017] 가)오버레이 네트워크 역추적 기법

[0018] 역추적 라우터 모델을 네트워크에 별도로 설치하고 해킹공격이 발생하였을 경우 네트워크상에서의 종단시스템과 연결된 라우터에 전달된 정보를 역추적 라우터로 전송하는 구조이다. 즉, 기존의 ingress 필터링 기법과 유사하게 종단 라우터에서 보내진 트래픽 정보는 터널링 방식으로 역추적 라우터에 전달하게 된다. 단일 ISP 네트워크상에서 구현가능하며, 소단위 네트워크에 적합한 기법이다.

[0019] 나)해쉬기반 역추적 기법

[0020] SPIE기반 역추적 서버를 구성하고 전체네트워크를 서브그룹으로 나누어 각 그룹별로 에이전트를 두어 망을 관리하는 기법이다. DGA에서 해당 라우터에 전달된 패킷에 대해 패킷의 메시지 해쉬 값에 해당하는 IP헤더 정보와 8 바이트 정보의 payload 정보를 수집/관리, bloom filter 구조로 저장된다. SPIE, SCAR, DGA 기능을 구축해야 하고, 추가적인 모듈로 제공되기 때문에 이기종 환경의 ISP간에도 적용이 가능하다.

[0021] 다)IPSec 기반 역추적 기법

[0022] 오버레이 네트워크 기반 역추적 기법에서 발생하는 터널링 과정에서의 보안상 취약점을 보완하기 위해 제시된 기법이다. 네트워크상에서의 주변 라우터를 선정하여 IPSec 터널을 구성하고 패킷에 대한 전송여부를 판별하여 이를 피해 시스템에 전달하는 기법이다.

[0023] 현재 다양한 접근 방법이 시도되고 있으나, 기존의 보안제품 및 기법은 다음과 같은 취약점을 보이고 있다. 우선 로깅 기법인 경우 많은 양의 정보를 저장/관리하고, 데이터 처리량도 방대하기 때문에 비효율적이며, 방대한 패킷에 대한 판별 과정에서의 오류 수정과정이 보완되어야 한다는 단점이 있다. iTrace(ICMP Traceback) 기법인 경우 패킷의 payload 정보 등을 포함하여 전달하기 때문에 공격경로 재구성 사용될 수 있으며, DDoS공격에 대응하기 위해서는 상대적으로 많은 정보가 필요한 실정이다.

[0024] 또한 오버레이 네트워크 역추적 기법인 경우 네트워크 구성상 단일 역추적 라우터로 전체 네트워크를 관리할 수 없으며, 단일 ISP 네트워크상에서 구현 가능한 기법이며 이기종의 네트워크 경우 적용할 수 없다. 따라서 공격자에 의한 터널링 된 패킷이 위조될 수 있기 때문에 문제가 될 수 있다.

[0025] < 기존 라우터를 활용한 네트워크 보안>

[0026] 가.ingress filtering 설정

[0027] ingress 필터링은 standard 또는 extended access-list를 활용하여 라우터 내부로 즉 사내 네트워크로 유입되는 패킷의 소스 IP 나 목적지 포트 등을 체크하여 허용하거나 거부하도록 필터링한다.

[0028] 나. egress filtering 설정

[0029] egress filtering 이란 ingress filtering와는 반대로 내부에서 라우터 외부로 나가는 패킷의 소스 IP를 체크하여 필터링한다.

[0030] 다. Null routing을 활용한 필터링

[0031] access-list 와 함께 유용하게 사용할 수 있는 필터링 기법으로는 blackhole 필터링이 있다.

[0032] 라. Unicast RPF를 이용한 필터링

[0033] Unicast RPF(Unicast Reverse-Path Forwarding) 이용하면 앞에서 살펴본 access-list 나 blackhole 필터링을 이용하여 일일이 IP 나 IP 대역을 지정하지 않고도 비정상 트래픽을 효율적으로 필터링 할 수 있는 방법이다.

[0034] < 기존 방어기술의 한계 >

[0035] 가. ACL(Access Control List)

[0036] 가장 일반적인 유해 트래픽 차단 기술로써 IP주소, 서비스 포트 그리고 콘텐츠를 기반으로 한 차단이 가능하지만 이 방법은 접근통제를 위한 별도의 ASIC화된 모듈이 없을 경우 네트워크 장비에 많은 부담을 주어 성능저하의 원인이 될 수 있다. 또한 ISP와 같이 많은 네트워크 장비를 보유하고 있는 기관의 경우, 이들 장비들에 접

근통제 정책을 업데이트하기 위해서 별도의 스크립트를 작성하거나, 그렇지 않은 경우 개별적으로 로그인하여 설정을 변경하여야 하는 어려움이 있다.

[0037] 나. Null0 라우팅

[0038] 특정한 목적지로 향하는 패킷들을 Null0라는 가상 인터페이스에 포워딩함으로써 drop 시킬 수 있는 기술이다. 이 기술은 네트워크 장비의 기본 기능인 포워딩 기능을 이용하므로 ACL 기술에 비해 장비의 과부하가 거의 없으나, IP 기반(L3)의 필터링만 제공할 수 있고, 서비스 포트(L4)나 콘텐츠(L7)에 의한 필터링은 불가능한 단점을 가지고 있다.

[0039] 다.urPF(unicast Reverse Path Forwarding)

[0040] 출발지 IP주소를 위장(IP Spoofing)한 공격을 차단해 줄 수 있는 기술로써, 라우터가 패킷을 받으면 출발지 IP 주소를 확인하여 해당 IP로 갈 수 있는 역 경로(Reverse Path)가 존재하는지 확인함으로써 출발지 IP 주소의 신뢰한다.

[0041] 대부분의 DoS 또는 DDoS 공격이 자신의 출발지 주소를 위장하므로 urPF는 상당히 효과적인 서비스거부공격 차단 수단이 될 수 있지만, 이 기술 역시 다수의 라우팅 경로가 존재하는 비대칭 망구조를 가지고 있을 경우 적용의 한계(strict 모드 사용 못함)가 있으며, Spoofing을 방지하는 것 이외에 다양한 서비스거부공격에 대한 대응 기능이 존재 하지 않는다.

[0042] 라.Rate-Limit 기술

[0043] 출발지 IP주소를 위장(IP Spoofing)한 공격을 차단해 줄 수 있는 기술로써, 라우터가 패킷을 받으면 출발지 IP 주소를 확인하여 해당 IP로 갈 수 있는 역 경로(Reverse Path)가 존재하는지 확인함으로써 출발지 IP 주소의 신뢰한다. 대부분의 DoS 또는 DDoS 공격이 자신의 출발지 주소를 위장하므로 urPF는 상당히 효과적인 서비스거부공격 차단 수단이 될 수 있지만, 이 기술 역시 다수의 라우팅 경로가 존재하는 비대칭 망구조를 가지고 있을 경우 적용의 한계(strict 모드 사용 못함)가 있으며, Spoofing을 방지하는 것 이외에 다양한 서비스거부공격에 대한 대응 기능이 존재 하지 않는다.

[0044] 마.Netflow

[0045] 트래픽 흐름 분석(Traffic Flow Analysis)을 통해 소스 및 대상 주소, 각 flow의 바이트 수 및 패킷 수, 트래픽 유입 인터페이스 및 업스트림 피어 정보 등을 모니터링 할 수 있다. Cisco에서 개발한 NetFlow는 트래픽 flow를 측정할 수 있는 대표적인 것으로써 이를 이용하여 Spoofing된 유해 트래픽이 어떤 인터페이스에서 유입되고 있는지 확인할 수 있다. 하지만, 이 기능을 이용한 공격자 추적은 공격로 상의 모든 네트워크 장비에 대한 접근권한이 주어져야 하고, 공격이 이루어지고 있을 동안 분석이 완료되어야 된다는 단점이 있다. Netflow는 공격자를 추적하는 것 이외에 실시간으로 네트워크를 모니터링 하여 이상징후를 탐지하는 용도로도 사용될 수 있다.

[0046] <기존 원격구동 블랙홀 라우팅 기술>

[0047] 블랙홀 라우팅 기술 개요

[0048] 가.iBGP

[0049] 도 1을 참조하면, 원격구동 블랙홀 라우팅 기술의 핵심은 iBGP를 이용해 라우팅 경로를 AS(Autonomous System) 내의 라우터들에게 알려주는 기술과 특정 트래픽을 null0 라우팅하여 drop 시키는 기술이다. 원격구동 블랙홀 라우팅 기술에서는 이 두 기술을 조합하여 효과적으로 DDoS 공격을 차단할 수 있도록 한다. iBGP를 이용한 라우팅 경로 광고(Advertise)는 iBGP 프로토콜을 공유하는 AS 내부의 다수 라우터들에게 라우팅 정보를 원격에서 전달할 수 있다. 또한, 각 edge 라우터에 설정된 특정 IP를 가상 인터페이스인 Null0로 포워딩하는 것은 공격 트래픽을 Null0로 라우팅 함으로써 공격 트래픽을 drop시키는 효과를 가진다.

[0050] 목적지 기반 원격구동 블랙홀 라우팅 기술

[0051] 목적지 기반 원격구동 블랙홀 라우팅 기술은 특정한 목적지로 향하는 모든 트래픽을 edge 라우터들에서 차단할 수 있는 방법을 제공한다. 이 기술은 iBGP 네트워크를 통해 공격 목표 시스템의 next hop 주소를 블랙홀로 빠지도록 지정된 특정 IP 주소로 바꾸는 기술에 착안한다.

[0052] 가.블랙홀 라우팅 시나리오

- [0053] DDoS 공격 발생 시 목적지 기반 원격구동 블랙홀 라우팅 기술을 이용한 효과적인 차단 시나리오 도2 에 도시된 바와 같다.
- [0054] ISP의 블랙홀 라우터 서버에서 iBGP 광고를 위한 준비와 각 edge 라우터들에 null0 라우팅을 설정해 놓고, 공격이 발생되면 공격 대상 사이트에서 DNS 정보를 변경하고, ISP에서는 각 edge 라우터들에게 공격 대상 IP로 향하는 패킷들을 drop할 수 있도록 명령을 보내는 과정을 보여주고 있다.
- [0055] **출발지 기반 원격구동 블랙홀 라우팅 기술**
- [0056] 인터넷 웹에 감염되어 웹을 전파시키는 시스템이나 DoS 또는 DDoS 공격에 이용되는 시스템을 네트워크에서 신속하게 분리시킬 수 있는 방법을 찾을 필요가 있다. 이러한 요구사항에 대한 고민으로 등장한 것이 출발지 기반의 원격구동 블랙홀 라우팅 기술이다. 이 기술은 수십개의 IP 주소로부터 웹이나 DoS 공격이 발생되었을 경우 이들 공격지로부터의 패킷을 전체 edge 라우터들에서 단시간에 차단할 수 있으며, 공격지 IP 주소가 수시로 바뀔 경우 이를 신속하게 업데이트하면서 차단할 수 있는 기능을 제공해 준다. 이 기술은 앞서 살펴본 목적지 기반의 원격 구동 블랙홀 라우팅 기술을 약간 변형한 것으로 각 edge 라우터의 인터페이스들에 uRPF 기능을 추가적으로 설정하여야 한다. 출발지기반의 원격구동 블랙홀 라우팅 기술에서는 uRPF 기술이 기존의 null0 라우팅 기술과 iBGP 광고 기능과 함께 핵심 기술로 사용되고 있다.
- [0057] 가.Sinkhole 기술기반 Back scatter 현상을 이용한 공격경로 추적
- [0058] 대부분의 서비스거부공격에서는 근원지 추적을 피하기 위해 Source IP주소를 Spoofing하는 것이 일반적이어서 이를 추적하는 것은 쉽지 않다. 기존의 추적 기술 중 Cisco사의 Netflow를 이용하여 역추적이 가능하지만, 공격 경로상의 라우터들이 Cisco사의 제품이어야 하고, 라우터에 접근할 수 있는 권한을 가져야 하고, 공격이 진행 중인 동안에만 분석할 수 있다는 단점을 가지고 있다. 따라서 공격 관련된 패킷들을 특정 네트워크로 끌어 들여서 분석하는 기술이 필요하다.
- [0059] 도 3을 참조하면, 목적지 기반 원격구동 블랙홀 라우터에 의해 drop된 패킷들에 대한 ICMP Unreachable 패킷을 수집하여 공격 진입지점을 추적하는 시나리오를 보여주고 있다.
- [0060] 나. Sinkhole tunnel 기술
- [0061] Sinkhole 라우터를 이용한 트래픽 분석은 검사 결과 정상적인 트래픽일지라도 다시 목적지 호스트까지 보낼 수 없어 결국 합법적인 트래픽도 서비스가 거부되는 결과를 가져올 수 있다. 이러한 단점을 극복할 수 있는 Sinkhole tunnel 기술은 트래픽 전환(traffic shunt) 이라고도 불린다. Sinkhole tunnel 기술은 목적지 주소의 next hop 주소를 변경하지 않고 정해진 터널을 지나가게 하고, 이 터널에서 ACL, rate limit, 분석 등의 필요한 작업을 한다. 필요한 작업 후에 정상적인 트래픽일 경우에는 터널을 빠져나가 원래의 목적지로 전송될 수 있도록 내보낼 수도 있다.

발명의 내용

해결 하고자하는 과제

- [0062] 본 발명의 목적은 최소화된 Bloom Filter 값으로 장기간 패킷에 대한 정보를 저장할 수 있으며, 공격 발생 시 단위 네트워크내 라우터에 대한 관리 구조를 제공하기 때문에 보다 효율적인 공격 탐지 및 제어 기능을 수행하도록 하는 올아이피네트워크 환경의 공격 탐지 및 추적 시스템 및 방법을 제공하고자 하는 것이다.

과제 해결수단

- [0063] 상기한 바와 같은 목적을 달성하기 위한 본 발명의 바람직한 실시예에 따르면, 올아이피네트워크 환경의 공격 탐지 및 추적 방법은 복수개의 소스 및 목적지 단말기, 싱크홀라우터(시스템)를 포함한 복수개의 라우터(router)(시스템), 매니저(서버컴퓨터시스템)(이하, 매니저 시스템이라 함)가 서로 유무선 통신망으로 연결된 올아이피네트워크 환경의 공격 탐지 및 추적 시스템을 이용한 올아이피네트워크 환경의 공격 탐지 및 추적 방법에 있어서, 매니저 시스템, 라우터간에 정보 설정을 초기화하는 제 1단계와, 매니저 시스템에서 각각 라우터로 싱크홀 라우터 결정사항을 통보하는 제 2단계와, 피해시스템으로부터 공격 발생에 관한 통보를 받을 경우 매니저 시스템은 공격 패킷의 해쉬 정보를 각 라우터에 전송하여 공격리스트에 등록/업데이트 하도록 하는 제3 단계와, 일반 사용자에게 의해 공격패킷이 발생하여 전송될 경우 라우터에서는 자신의 공격 리스트에 기록된 값과 일치하는 해쉬 값을 갖고 있는지 판단하는 제4단계를 포함하여 이루어진 것을 특징으로 한다.

[0064] 본 발명의 다른 측면에 따르면, 복수개의 소스 및 목적지 단말기, 싱크홀라우터(시스템)를 포함한 복수개의 라우터(router)(시스템), 매니저(서버컴퓨터시스템)(이하, 매니저 시스템이라 함)가 서로 유무선 통신망으로 연결된 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에 있어서, 상기 매니저 시스템은 라우터를 관리하고 공격 트래픽에 대한 역추적을 위해서 여러 가지 정보를 저장, 관리하는 매니저 데이터부와, 매니저 시스템이 관리하는 라우터의 정보를 관리하는 라우터 관리부와, 공격 트래픽의 역추적을 위한 관리하는 공격패킷 관리부와, 트래픽의 송수신처리를 위한 프로토콜처리부를 포함하여 이루어지고, 상기 라우터 시스템은 공격 패킷의 역추적을 위한 정보 기록하는 라우터 데이터부와 라우터를 지나가는 패킷의 추출 및 해쉬 적용을 위한 패킷 처리부 블룸 필터를 이용하여 패킷의 경로를 확인하는 블룸 필터 처리부와, 현재 패킷이 공격 패킷인지 판단하는 공격 패킷 처리부와, 싱크홀 라우터로 전송되는 원본 공격 패킷들을 관리하는 싱크홀 라우터 데이터부, 공격패킷의 목록을 관리하는 공격패킷 처리부와, 패킷 데이터의 송수신처리를 위한 프로토콜 처리부를 포함하여 이루어진 것을 특징으로 한다.

효 과

[0065] 이상 설명한 바와 같은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템 및 방법에 의하면, 최소화된 Bloom Filter 값으로 장기간 패킷에 대한 정보를 저장할 수 있으며, 공격 발생 시 단위 네트워크내 라우터에 대한 관리 구조를 제공하기 때문에 보다 효율적인 공격 탐지 및 제어 기능을 제공되는 효과가 있다.

[0066] 본 발명에서는 유선/무선 네트워크 환경에서의 공격 및 추적 시스템 및 방법 및 MAC/IP/어플리케이션 이용자 공격 및 추적 방법에 대해 조사, 발명함으로써 기존의 SPIE 시스템에서 사용하는 Bloom Filter 기반 역추적 기법에 대해 분석/조사하고 이 기법의 문제점과 해결하고 개선방안을 도출한 효과가 있다.

[0067] 또한 라우터 기반 트래픽 수집 방법인 Sinkhole 라우터 기반 트래픽 분석 기법에 대해 분석하고 이를 통한 개선한 효과가 있다. 본 발명에서는 기존의 SPIE 시스템의 문제점을 해결하면서 Sinkhole 라우터와 연계한 새로운 All-IP 네트워크 환경에서의 효율적 역추적 기법 등에 대해 제시하였다.

발명의 실시를 위한 구체적인 내용

[0068] 이하 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템 및방법에 대하여 첨부도면을 참조로 상세히 설명한다.

[0069] 도 4는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 경로로그 분석과정을 설명하는 도면이고, 도 5는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 패킷 로그중심 역추적 및 공격경로 추출과정을 나타낸 도면이고, 도 6은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 싱크홀 라우터 기반 공격 패킷 역추적 과정을 나타낸 도면이고, 도 7은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 블룸 필터(bloom filter) 기반 라우터를 이용한 공격 패킷 역추적 과정을 나타낸 도면이고, 도 8은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 아이피 패킷내 24바이트 해쉬 적용부분을 나타낸 도면이고, 도 9는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 블룸 필터기반 패킷 전송 경로정보 저장과정을 나타낸 도면이고, 도 10은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 32비트 블룸 필터 생성 매커니즘을 나타내는 도면이고, 도 11은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 프레임구조 및 전송장비별 모니터링 계층의 일예를 나타낸 도면이고, 도 12는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 Hop-by-Hop 패킷 전송과정을 개략적으로 나타내는 도면이고, 도 13은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 패킷에 대한 블룸 필터 생성 및 부가적 정보생성구조를 나타낸 도면이고, 도 14는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 패킷에 대한 블룸 필터 생성관련 세부 단계를 나타낸 도면이고, 도 15는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 공격 발생시 라우터에서 싱크홀로 패킷을 전달하는 과정을 나타내는 도면이고, 도 16은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 매니저 시스템 기반 공격 역추적 과정을 개략적으로 나타내는 도면이고, 도 17은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 매니저 선정 및 라우터 초기화과정을 개략적으로 나타내는 도면이고, 도 18은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 싱크홀 라우터 설정 및 라우터 관리구조를 개략적으로 나타낸 도면이고, 도 19는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 공격 발생 시 각 라우터에서의 작동방식을 개략적으로 나타낸 도면이고, 도 20은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 공격 발생시 피해시스템에서의 작동 방

식 및 매니저 역할을 개략적으로 나타낸 도면이고, 도 21은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 DDos 공격 트래픽에 대한 싱크홀 라우터로의 전송 및 관리구조를 개략적으로 나타낸 도면이고, 도 22는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 매니저 기반시스템 설정 초기화단계를 나타낸 도면이고, 도 23은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 싱크홀 라우터 데이터구조의 일예를 개략적으로 나타낸 도면이고, 도 24는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 개별 라우터의 데이터구조의 일예를 개략적으로 나타낸 도면이고, 도 25는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 싱크홀 라우터정보 설정 단계를 개략적으로 나타낸 도면이고, 도 26은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 라우터 및 싱크홀 정보 설정 단계를 개략적으로 나타낸 도면이고, 도 27은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 일반 트래픽에 대한 처리과정의 일예를 개략적으로 나타낸 도면이고, 도 28은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 공격 트래픽에 대한 처리과정의 일예를 개략적으로 나타낸 도면이고, 도 29는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 매니저 시스템과 라우터 간의 관계를 개략적으로 나타낸 도면이고, 도 30은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 매니저 시스템 구조를 개략적으로 나타낸 도면이고, 도 31은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 라우터 시스템구조를 개략적으로 나타낸 도면이고, 도 32는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 매니저 시스템과 라우터간 통신을 위한 프로토콜 구조를 개략적으로 나타낸 도면이고, 도 33은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 블룸 필터 모듈의 개략적인 구조를 나타내는 도면이고, 도 34는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 블룸 필터를 이용한 라우터의 처리과정의 일예를 개략적으로 나타낸 도면이고, 도 35는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 공격 트래픽 역추적 과정을 개략적으로 나타낸 도면이고, 도 36은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 프로토콜 처리과정을 개략적으로 나타낸 도면이다.

- [0070] 도 4 및 도 5를 참조하면, 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템은 네트워크 환경에서 패킷별 로그 정보를 대상으로 역추적 경로 등을 관리 추출한다.
- [0071] **A11-IP 네트워크 기반 IP Traceback**
- [0072] 역추적 기술은 IP 패킷의 실제 송신 근원지를 찾는 과정이다. 패킷이 전송되는 과정에서 IP 패킷 헤더에는 발신자의 IP 주소 값을 기록하게 되어 있으나, 공격자는 실제 패킷이 전송되는 근원지 IP에 대해 변경(IP Spoofing)하여 전송할 수 있다. 따라서 수신자 측면에서 수신된 IP 패킷의 헤더에 기록된 근원지 IP 값만을 가지고는 실제 패킷의 송신지 주소값을 확인하기 어렵게 되어 있다.
- [0073] 따라서 본 발명에서는 A11-IP 네트워크 환경에서 다양한 형태의 공격이 발생하였을 경우 이를 해결할 수 있는 방법에 대해 발명하고 특히 DDos 공격에 대해 라우터 중심으로 해결할 수 있는 방법에 대해 제시하고자 한다.
- [0074] **DDoS 공격**
- [0075] DoS 공격은 대량의 패킷이 특정 IP 네트워크 주소로 전송되는 과정에서 해당 시스템의 서비스가 정상적으로 제공되지 못하는 경우를 의미한다. 따라서 분산형 서비스 거부 공격 형태로 패킷을 송수신할 경우 전체 네트워크 중심으로 이를 관리/대응할 수 있는 기술이 제시되어야 한다.
- [0076] 하지만 기본적으로 공격자는 자신이 이용하는 시스템에 대한 IP 주소를 변경하여 대량의 패킷을 생성/전송하기 때문에 실제 패킷이 전송되는 경로에 해당하는 라우터를 중심으로 트래픽에 대해 모니터링하지 않고서는 효율적인 공격 대응 기술 등을 개발하기 어려운 실정이다.
- [0077] 지금까지 앞에서 제시한 DDos 공격에 능동적으로 대응하기 위해 다양한 발명이 수행되었다. 우선 근원지 시스템에서 패킷의 회신 주소가 부적합한 경우 수신된 패킷을 폐기하는 등의 필터링 과정을 수행할 수 있다. 이 방식은 기존의 대부분의 라우터 및 방화벽 등에 포함되어 있는 기술이지만 모든 개별 패킷에 대해 회귀 주소에 해당하는 리턴 주소 값의 적합성 여부를 매번 판별해야 하기 때문에 해당 라우터 또는 방화벽 시스템의 성능을 저하시킬 수 있다는 단점이 있다.
- [0078] 앞에서 제시한 방식과 유사하게 백본 라우터(backbone router) 중심으로 필터링 과정을 수행하는 방식이 있다. BGP 프로토콜 중심으로 라우터에서는 근원지 IP 주소 값을 중심으로 라우터에 수신된 패킷에 대해 필터링 과정

을 수행하게 된다.

- [0079] 이 방식은 가장 일반적인 형태라고 볼 수 있으나, 라우터의 성능 및 메모리 부분에 많은 부담을 주게 되며 기존의 라우터에 대한 부담을 높여주게 된다. 따라서 이에 대한 개선 방법에 대한 발명이 계속 진행되고 있으며 Blackhole/Sinkhole 라우터 방식을 통해 이를 개선하고자 하였다.
- [0080] 본 발명에서는 기존의 SPIE 시스템에서 제시한 Bloom Filter 기반의 네트워크 관리 기법에 Sinkhole 라우터 방식을 결합하여 보다 개선된 IP 역추적 기법을 제시하고자 한다. 기존의 역추적 기법인 경우 다음과 같이 정리할 수 있다.
- [0081] **Digested Sinkhole 기반 IP 역추적 구조**
- [0082] 본 발명에서 제시하는 방식은 기존 SPIE 시스템과 Sinkhole 라우터 방식의 장단점을 비교 분석하여 최적의 해결 방안을 제시하는 것이다. 도 6에 도시된 바와 같이 라우터를 중심으로 패킷에 대한 공격 발생시 Sinkhole 라우터로 해당 패킷에 대한 정보를 전송하고 공격 역추적 정보를 생성/관리하는 구조를 설계할 수 있다.
- [0083] 도 6을 참조하면, 주요 작동 방식은 Victim 사이트로 공격 발생 시 해당 네트워크에 소속된 라우터로 통보하여 Sinkhole 라우터에 대한 정보를 전송하고, 이후에 개별 라우터에 수신되는 패킷에 대해서는 Sinkhole 라우터로 전송하는 방식이다. 따라서 이를 위해서는 각 라우터에 기존의 SPIE 시스템과 유사한 형태로 패킷에 대한 요약 정보를 저장하는 구조가 추가로 구현되어야 한다. 도 7을 참조하면, 각각의 라우터에서는 개별적으로 캐쉬 구조를 갖고 있으면서 라우터를 거치는 패킷에 대해 Bloom Filter 방식을 적용해서 패킷에 대한 요약 정보를 구축하게 된다.
- [0084] 각각의 라우터에서 구축하게 되는 Bloom Filter 모듈에서는 도 8에 도시된 바와 같이 IP 패킷의 헤더를 포함하여 처음 24바이트 정보를 취하여 이에 대해 해쉬 함수를 적용하게 된다.
- [0085] 도 9에 도시된 바와 같이 네트워크 구조에서 패킷이 송수신 되는 과정에서 데이터링크 계층에서는 링크 간의 두 노드에 대한 물리주소값을 프레임 헤더정보에 기입하여 전송하게 된다.
- [0086] 도 9에 도시된 바와 같이 각각의 라우터에서는 수신된 패킷의 처음 24바이트 정보에 대해 두가지형태의 해쉬 함수를 이용하여 해쉬 값을 생성하고 이를 Bloom Filter에 저장하고 라우터를 통해 다음 홉으로 패킷을 전송하게 된다.
- [0087] 만일 공격 형태에 해당하는 패킷일 경우 공격 리스트 파일에서 검색하고 만일 공격에 해당한다면 이를 Sinkhole 라우터로도 전송하게 된다.
- [0088] 각각의 라우터에서 적용하는 해쉬 함수의 작동 과정을 좀 더 자세히 살펴보면, 도 10을 참조하면, 다음과 같다. 암호학적으로 안전한 해쉬 함수는 SHA-256 함수를 사용할 수 있다. 이 경우 임의의 비트에 해당하는 패킷이 입력으로 들어오면, 항상 256비트의 출력 값을 갖는 경우이다.
- [0089] Bloom Filter인 경우 전체적인 크기는 해쉬 함수의 출력 비트 크기에 영향을 받기 때문에, 일반적으로 저장용량 및 Bloom Filter의 크기를 생각한다면 일반적으로 32비트 정도가 적절하다. 따라서 본 발명에서는 기존에 암호학적으로 안전하다고 알려진 SHA-256 함수를 이용하면서 도 10에 도시된 바와 같이 Folding 방식을 이용하여 최종적으로 32비트 값의 해쉬 값을 계산하도록 하였다.
- [0090] 따라서 프레임 헤더에 기록되는 송수신자의 물리 주소 값은 네트워크 전송 경로상의 각 홉(hop)을 거치면서 매번 변경되는 정보이기 때문에 이 정보는 역추적 과정에 이용할 수 없다.
- [0091] 도 11은 프레임구조 및 전송장비별 모니터링 계층을 나타내는 도면이다.
- [0092] 한편, 도 12에 도시된 바와 같이 IP 패킷 구조에 있는 정보는 라우터를 거치면서 고정된 값으로 되어 있으며 근원지에서 최종 목적지로 패킷이 전달되는 과정에서 일관적으로 유지되는 값이다. 물론 IP 헤더 구조에서 TTL, Checksum 등과 같은 일부 필드는 변경된다. 따라서 앞에서 제시된 구조와 같이 IP 헤더에서 변경되는 부분을 제외하고 페이로드 부분을 포함하여 앞부분 24바이트에 대해 Bloom Filter 모듈을 적용하면 패킷에 대해 고유한 특성을 요약하여 저장할 수 있으며 개별 라우터에 대한 경로 근거 정보로도 활용할 수 있다.
- [0093] 도 13에 도시된 바와 같이 각각의 라우터에서는 수신된 패킷에 대해 Bloom Filter를 적용하여 각각 저장하게 된다. 본 발명에서는 개별 라우터에서 두 개의 해쉬 함수를 선택하도록 하였으며 이를 이용하여 각 패킷에 대해 해쉬를 적용하고 그 결과를 필터에 저장토록 하였다.

- [0094] 저장된 정보는 특정 피해 시스템에서 DDoS 공격이 발생하였을 경우에 실제 패킷의 전송 경로를 판단하는데 활용된다. 도 14에 도시된 바와 같이 각각의 라우터 Ri 에서는 각기 해쉬 함수를 적용하여 그 결과를 주기적으로 저장하게 된다. 이때 Bloom Filter에 저장되는 파일의 크기는 n 비트 길이의 해쉬 값을 저장할 수 있는 구조이며, 부가적인 위치 태깅 정보에 대해서는 Sinkhole 라우터로 전송되는 구조이다.
- [0095] 도 15에 도시된 바와 같이 전체 네트워크 구조에서 라우터 중심으로 패킷이 송수신되는 구조를 보인다. 위에서 제시한 Bloom Filter 생성 구조를 이용하여 각각의 라우터에서는 개별 패킷에 대해 해쉬 함수를 적용하여 자신의 필터 구조 내에 기록하게 되며, 부가적인 정보에 대해서는 Sinkhole 라우터로 전송하여 공격 경로 등을 판별하게 하는 구조이다.
- [0096] **개선된 Bloom Filter 기반 Sinkhole Traceback 구조**
- [0097] 본 발명에서 제안하는 구조는 도 16에 도시된 바와 같이 개별 라우터에서 패킷에 대한 모니터링 과정을 수행하고 이를 전체적으로 통합 관리하는 구조로 되어 있다. 도 16은 전체적인 구조를 보인다. Manager 시스템을 두어 일정 네트워크 망에 대한 역추적 기능을 담당하도록 하였으며 분산 관리 기능을 제공하게 된다. 시스템 구성 요소 및 전체적인 시스템 구조는 다음과 같다.
- [0098] - 각 사용자 노드 : 네트워크 일반 사용자 및 공격자 등을 포함하는 네트워크상의 end 노드 시스템을 의미한다. 기존의 tcp/ip 프로토콜을 기반으로 네트워크에 접속된 사용자 시스템을 의미한다.
- [0099] - 라우터 : 네트워크 트래픽을 송수신하는 중간 네트워크 장비에 해당한다. BGP 프로토콜을 이용하여 전체적인 패킷의 전송 경로 등을 파악하며, 패킷의 IP 헤더에 기록된 수신자 IP 주소를 보고 RIP, OSPF 등의 경로설정 방식을 이용하여 패킷을 전달하는 기능을 제공한다.
- [0100] - Sinkhole 라우터 : 앞에서 제시한 일반적인 라우터의 기능을 수행하면서도, 별도로 전체 네트워크에 대한 공격이 발생하였을 경우 개별 라우터로부터 sinkhole 라우터로 패킷을 전송토록 하여 DDoS 발생 시 공격 트래픽에 대한 수집 기능을 제공하면서도 이에 대한 분석 및 필터링 및 역추적 등의 부가적 기능을 수행할 수 있는 라우터 시스템이다.
- [0101] - Manager 시스템 : 라우터 및 sinkhole 라우터로 구성된 네트워크에 대한 역추적 및 DDoS 대응 기능을 제공하기 위해 별도로 구성한 관리 시스템을 의미한다. 일정 규모의 네트워크를 대상으로 공격 트래픽에 대한 관리/확인 기능을 제공하며 공격 발생 시 해당 패킷의 실제 전송 경로 등을 판별하는 기능을 제공한다.
- [0102] 이와 같은 시스템 구성요소 및 시스템 구조를 토대로 단계별 작동과정을 제시하면 다음과 같다.
- [0103] 1단계 : Manager 선정 및 라우터 초기화 과정(도 17참조)
- [0104] - 본 작동 과정에서는 Manager 시스템이 해당 네트워크에 속한 라우터에게 Bloom Filter에 사용되는 해쉬 함수의 선택 및 설정 등에 대한 정보 등을 요청하면, 해당 라우터는 자신이 선택한 해쉬 함수 관련 선택 정보 및 파라미터 설정 정보 등을 안전한 채널로 Manager 시스템에 전송하여 초기화하는 과정이다.
- [0105] - 본 과정을 통해 Manager 시스템은 주변에 있는 라우터와 연계하여 DDoS 공격 발생시 패킷에 대한 모니터링 구조를 구축할 수 있게 된다.
- [0106] 2단계 : Sinkhole 라우터 설정 및 라우터에 대한 설정(도 18참조)
- [0107] - 앞의 1단계를 거친 후에 Manager 시스템은 공격 패킷이 저장될 Sinkhole 라우터를 설정하게 된다. 도 18에서와 같이 해당 네트워크내 라우터들 중에서 sinkhole 라우터 기능을 담당할 라우터를 설정한다.
- [0108] - Manager 시스템은 선정된 sinkhole 라우터에 대한 정보를 해당 네트워크에 속한 라우터 등에게 전송하게 된다.
- [0109] - 개별 라우터는 자신의 내부 변수에 sinkhole 라우터 주소 값 등을 설정하게 된다.
- [0110] 3단계 : Victim에 대한 공격 발생 및 DDoS 트래픽 발생
- [0111] - 피해 시스템에 DDoS 공격 등이 발생하였을 경우를 예상하면 도 19와 같이 구성할 수 있다.
- [0112] DDoS 공격 발생 시 공격 패킷은 네트워크를 구성하는 라우터를 거치게 되며 개별 라우터는 모든 패킷에 대해 Bloom Filter를 적용하게 된다.

- [0113] 4단계 : Victim에서 Manager로의 공격 알림 및 Manager에서의 작동과정(도 20참조)
- [0114] - 공격이 발생하게 되면 피해 시스템은 우선 Manager 시스템으로 공격 발생 사실을 통보하게 된다. 피해 시스템은 공격이라고 의심되는 패킷에 대한 해쉬 값을 포함하여 공격 패킷에 대한 정보를 Manager 시스템에 전송하여 공격 발생을 알리게 된다.
- [0115] - Manager 시스템은 피해 시스템으로부터 수신한 공격 패킷에 대해 자체 저장 구조 내에 기록하고, 이를 해당 라우터에 알리게 된다. 개별 라우터는 자신의 Bloom Filter에 트래픽에 대한 전달 정보 등을 기록하고 있기 때문에, Manager로부터 각 라우터에 전달된 공격 패킷에 대해 각각의 라우터는 자신의 Bloom Filter를 검사하게 된다.
- [0116] - 각각의 라우터에 기록된 Bloom Filter 검사 결과 각각의 라우터에서는 공격 패킷이 자신의 라우터를 거쳐 갔을 경우(Packet Passed)와 그렇지 않은 경우로 나눌 수 있다. 그리고 해당 패킷에 대해서는 sinkhole 라우터로 전송된다.
- [0117] 5단계 : 공격 발생 시 패킷의 처리 과정(도 21참조)
- [0118] - 공격이 발생하게 되면 각각의 라우터는 평상시와 마찬가지로 Bloom Filter 과정을 수행하게 된다.
- [0119] - 만일 라우터에 저장 관리되는 Bloom Filter에 기록된 정보와 현재 전송되는 패킷의 형태가 유사한 공격 패킷에 해당한다면 이는 실제 목적지 IP로 전송되는 것이 아니라 라우터에 이미 설정되어 있는 Sinkhole 라우터로 전송된다.
- [0120] - 그리고, Sinkhole 라우터는 Manager 시스템에게 해당 패킷이 수신된 것을 통보하게 되고, 주기적으로 네트워크에 대한 모니터링 과정을 계속적으로 수행하게 된다.
- [0121] **단계별 Bloom Filter 기반 Sinkhole Traceback 메커니즘**
- [0122] 본 절에서는 단계별 작동 메커니즘에 대해 좀 더 구체적으로 설명하고자 한다.
- [0123] 가.초기화 단계 : Manager 기반 시스템 설정 초기화 단계(도 22참조)
- [0124] - 앞에서 제시한 바와 같이 라우터(21,22,23,24...)에서는 주변에 있는 라우터에서 사용할 해쉬 함수에 대한 환경변수 등 동기화 과정을 수행하게 된다.
- [0125] Manager 시스템에서는 주변에 있는 라우터와 통신하면서 해쉬 함수 선택을 요청하면 각 라우터는 함수 인덱스 값을 회신하게 된다.
- [0126] - 초기화 단계에서는 Manager 시스템(10)에서 라우터로 메시지를 송신하는 과정과 수신하는 과정을 수행하게 된다.
- [0127] - Manager 시스템에서는 라우터로 해쉬 함수 등의 설정 등에 관한 요청 메시지를 송신하게 된다.
- [0128] - 라우터에서는 Manager 시스템으로 설정 결과에 대한 인덱스 값을 전송한다.
- [0129] - 이때 송수신되는 메시지 포맷은 다음 구조와 같다. 클라이언트/서버 구조상 일반 노드, 라우터 및 Manager 시스템, 그리고 Sinkhole 라우터 간 송수신되는 메시지 구조를 설정하였다.
- [0130] 미설명부호 31은 (소스)단말을 나타내며, 32는 (목적지) 단말을 나타낸다.
- [0131] Manager 시스템에서 관리하는 데이터 구조는 도 23에 도시된 바와 같다.
- [0132] - 개별 라우터에서는 도 24에 도시된 바와 같은 데이터 구조를 갖는다. 라우터 내부에는 각각의 라우터에서 설정한 두 개의 해쉬 함수에 대한 정보를 저장하고 있으며, Sinkhole 라우터에 대한 정보 등을 관리하면서, 공격 패킷에 해당하는 정보 등을 해쉬 함수에 대한 정보와 함께 리스트를 관리하고 있다. 물론 각 라우터에는 Bloom Filter 정보도 저장/관리하고 있게 된다.
- [0133] - 이들간 메시지 송수신 구조 등을 설계하여 IP 역추적 및 전체 네트워크에 대한 모니터링 구조를 설계하였다.
- [0134] 나.설정단계 : Sinkhole 라우터 정보 설정 단계(도 25참조)
- [0135] - 라우터에 정보를 설정하는 단계로 Sinkhole 라우터를 설정하는 과정을 수행하며, 설정된 sinkhole 라우터에 대한 통보 기능을 수행하게 된다.

- [0136] - 등록 과정 역시 Manager 시스템에서 각각의 라우터로 메시지를 전송하는 과정이며, Sinkhole 라우터 결정 사항에 대해 통보하게 된다.
- [0137] - Sinkhole 라우터에 대한 설정 과정 등을 수행하게 되며, 라우터로 설정하는 과정을 수행하게 된다.
- [0138] 다.등록단계 : 해쉬 함수 정보 설정 및 공격 정보 업데이트/등록(도 26참조)
- [0139] - 피해 시스템으로부터 공격 발생에 대한 통보를 받을 경우 Manager 시스템은 공격 패킷의 해쉬 정보를 각 라우터에 전송하여 공격리스트에 등록/업데이트 하도록 한다. 이와 같은 등록 과정을 통해 해당 지역 네트워크에 속한 라우터에 대해 공격 정보에 대한 업데이트 기능을 제공하게 되며, Manager 시스템을 중심으로 공격 대응 기능을 제공하게 된다.
- [0140] - Manager 시스템은 라우터에게 관련 정보를 전송하면, 각 라우터와 Sinkhole 라우터는 응답메시지를 다시 Manager 시스템에게 회신하게 된다.
- [0141] - Sinkhole 라우터는 메시지를 생성하여 Manager 시스템에 전송하여 초기 등록과정 등을 마무리하게 된다.
- [0142] 라.패킷에 대한 처리 1단계(도 27참조)
- [0143] - 일반 사용자에게 의해 공격 패킷이 발생해서 전송될 경우 라우터는 계속적으로 모든 패킷에 대해 자신의 Bloom Filter 부분에 기록하고 있기 때문에 이 부분을 검색해서 유사한 형태의 해쉬 값을 갖는 경우 공격 패킷으로 분류할 수 있다.
- [0144] - 따라서 아래 처리 단계 1에서와 같이 라우터에서는 자신의 공격 리스트에 기록된 값과 일치하는 해쉬 값을 갖지 않을 경우 일반 패킷이라고 판단하게 된다.
- [0145] - 피해 시스템에서는 공격이 발생하였을 경우 해당 패킷에 대한 정보를 Manager 시스템으로 전송한다. Victim 시스템에서는 Manager 시스템으로 해당 프로토콜 포맷에 맞추어 메시지를 전송하게 된다.
- [0146] 마.패킷에 대한 처리 2단계(도 28참조)
- [0147] - 만일 패킷이 라우터내 Bloom Filter에 기록된 값과 동일한 형태일 경우 공격 패킷에 해당하므로, 이를 Sinkhole 라우터로 전송하게 된다. 라우터는 Manager 시스템으로부터 공격 패킷에 대한 리스트를 사전에 전송 받았기 때문에 이를 토대로 공격 패킷에 대한 판단 과정을 수행하게 된다.
- [0148] - 만일 공격이 발생하게 되면 라우터에서는 공격리스트를 확인하고 리스트에 존재할 경우 이를 Sinkhole 라우터로 전송하게 된다. 물론 각각의 라우터는 자신이 설정한 해쉬 함수를 이용하여 계속적으로 Bloom Filter 값을 생성/갱신하게 된다.
- [0149] 개발 시스템 구조
- [0150] **개발 시스템의 개요**
- [0151] 본 발명에서는 Manager 시스템과 Manager 시스템에 의해서 관리되는 라우터들에 의해서 공격에 대한 역추적이 이루어진다. Manager 시스템은 역추적을 위한 설정 요청, 공격 패킷에 대한 관리, 공격 패킷에 대한 정보 알림, 그리고 각 라우터들의 정보를 수집함으로써 역추적에 대한 전반적인 관리 기능을 수행한다. 라우터의 경우는 Sinkhole 라우터와 일반적인 라우터로 나뉘며, Sinkhole 라우터와 일반 라우터에서 공통으로 수행되는 패킷 처리 기능과 Sinkhole 라우터에서만 수행되는 공격 패킷 관리 기능이 있다(도 29참조).
- [0152] **Manager 시스템 구조(도 30참조)**
- [0153] Manager 시스템(10)은 기본적으로 네트워크 그룹에서의 라우터 관리 기능을 한다. 자신이 관리하는 라우터들 안에서 Sinkhole 라우터를 설정하고 모든 라우터들의 정보를 유지, 갱신, 관리를 한다. Manager 시스템은 라우터 관리를 이용하여 설정된 Sinkhole 라우터를 통해 공격 패킷에 대한 정보를 획득하며, 획득된 공격 패킷을 이용하여 Bloom Filter를 사용하는 라우터들을 이용하여 공격 트래픽을 확인하고 역추적을 수행한다.
- [0154] 가. 매니저 데이터부(11): 라우터 및 역추적을 위한 정보 기록
- [0155] - Manager 시스템은 라우터를 관리하고 공격 트래픽에 대한 역추적을 위해서 여러가지 정보를 저장, 관리하고 있다.
- [0156] - 라우터 정보 목록에는 관리되는 라우터의 ID와 프로토콜 통신을 위한 통신 정보, 해쉬 함수의 정보를 가지고

있다. ID는 라우터 관리를 위한 고유번호이며, 통신 정보는 메시지를 주고받기 위한 네트워크 정보로써 네트워크 상황에 따라 달라질 수 있다. 해쉬 함수 정보는 라우터가 수행하는 해쉬의 정보로써 라우터와 같은 해쉬 값을 추출하기 위해 가지고 있다.

- [0157] - 해쉬 함수 목록에는 관리되는 해쉬 함수의 목록들이 있다. 라우터 정보에는 해쉬 함수의 인덱스만 보유하고 있으면 실제 해쉬 함수 목록에 해쉬 함수들이 존재한다.
- [0158] - 공격 패킷 목록은 실제 공격이 이루어진 패킷들의 목록이다. 이 목록은 보안 관리자에 의해서, 혹은 Victim의 요청으로 얻게 되는 실제 공격 패킷이다. 보안 관리자는 이 목록에서 Sinkhole 라우터로 보내는 패킷을 선택할 수 있다. 단지 패킷들의 정보이며, 각 라우터에 적용되지 않은 패킷들의 목록이다.
- [0159] - 공격 경로 목록은 각 라우터에 적용된 공격 패킷에 대해서 Sinkhole 라우터가 받은 공격 패킷들을 보낸 라우터들의 ID이다. 이 부분은 공격자의 근원지 혹은 공격 경로를 분석하기 위한 정보이다.
- [0160] 나.라우터 관리부(13) : Manager 시스템이 관리하는 라우터의 정보를 관리
- [0161] - Manger 시스템이 처음 구동 시에, 선행되어 수행하는 작업이다. 라우터의 정보를 획득하고 관리하는 기능을 한다.
- [0162] - Manager 시스템은 공격 패킷에 대해 해쉬 된 값을 라우터에 전송하여 라우터가 공격 패킷에 대한 처리를 하도록 한다. 그러기 위해서 각 라우터의 해쉬 정보를 획득하는 작업을 수행한다.
- [0163] - Manager 시스템에 의해서 관리되는 라우터들은 일반 라우터의 기능을 수행할 수도 있으며 Sinkhole 라우터의 기능으로 전환할 수 있다. 이 부분을 지정해주는 작업을 Manager 시스템이 수행한다. Sinkhole 라우터로 지정된 라우터는 그 순간부터 싱크홀의 기능을 수행하며, Manager 시스템은 다른 라우터에게 싱크홀 라우터의 정보를 알린다.
- [0164] 다.공격 패킷 관리부(15) : 공격 트래픽의 역추적을 위한 관리
- [0165] - 공격 트래픽에 관련된 역추적을 위한 핵심적인 기능을 담당한다.
- [0166] - 공격 패킷에 대한 등록을 통해 각 라우터에서 공격 패킷에 대해 Sinkhole 라우터로 보내도록 한다. Manager 시스템은 모든 라우터를 대상으로 공격 패킷의 해쉬 값을 전송한다. 전송되는 해쉬 값은 각 라우터의 해쉬 함수의 맞는 해쉬 값이다.
- [0167] - 각 라우터들은 Bloom Filter를 사용하기 때문에 공격 패킷 등록을 통해 전송받은 해쉬 값을 이용해서 해당되는 공격 패킷이 자신을 지나갔는지 판단할 수 있으며, 이로 인해 Manager 시스템은 공격 패킷에 대해 공격 경로를 판단할 수 있다.
- [0168] 미설명부호 17은 프로토콜을 가진 프로토콜처리부를 나타낸다.

[0169] 라우터 시스템 구조(도 31참조)

- [0170] 라우터 시스템(21 혹은 22, 23 등이 될 수 있음)은 크게 두가지로 분류할 수 있다. 하나는 일반적인 라우터 기능을 수행하며 Bloom Filter를 적용하는 매커니즘을 가지는 라우터와 다른 하나는 그 기능과 더불어 Sinkhole 기능을 수행하는 Sinkhole 라우터이다. 두 라우터는 모두 자신을 지나가는 패킷에 대해 해쉬 함수를 적용하여 두 개의 해쉬 값을 추출한다. 추출된 해쉬 값은 Bloom Filter에 적용함으로써 패킷이 지나갔는지의 유무를 판단할 수 있다.
- [0171] 일반 라우터의 경우 해쉬된 값을 이용해서 자신이 가지고 있는 공격 패킷의 리스트를 통해 Sinkhole 라우터로 전송할지의 여부를 판단한다. Sinkhole 라우터는 스스로 처리를 하며, 자신이 처리하거나 다른 라우터로 받은 공격 패킷을 기록하고 어느 라우터로부터 왔는지 Manager 시스템에 알리는 기능을 한다.
- [0172] 가. 라우터 데이터부(210): 역추적을 위한 정보 기록
- [0173] - 라우터의 데이터는 일반 라우터에서 사용하는 데이터 구조와 Sinkhole 라우터에서만 쓰이는 데이터 구조가 있다. 일반 라우터의 경우는 역추적을 위한 Bloom Fliter와 Sinkhole 라우터로 보내기 위한 공격 패킷의 해쉬 정보를 가지고 있으며, Sinkhole 라우터는 추가로 원본 공격 패킷의 목록을 가지고 있다.
- [0174] - Manager 시스템과 Sinkhole 라우터의 네트워크 정보는 대상 단말과 프로토콜 통신을 위한 네트워크

정보이다.

- [0175] - 각 라우터는 Bloom Filter 적용과 공격 패킷 판단을 위해서 공격 패킷에 대해 두 개의 해쉬 함수를 이용하여 각기 다른 두개의 해쉬 값을 추출한다.
- [0176] - Bloom Filter는 앞서 설명한 것과 같이 패킷이 자신을 지나갔는지를 효과적이고 효율적인 검색하기 위해 사용된다.
- [0177] - Manager 시스템으로부터 알려진 공격 패킷에 대해 자신이 수행하는 해쉬 함수를 이용한 해쉬 값 두 개를 하나의 원소로 하여 공격 패킷의 해쉬 정보 목록으로 가지고 있다. 이 목록의 비교를 통해서 패킷에 대해 공격 패킷인지를 판단할 수 있으며, 공격 패킷으로 판단될 경우 싱크홀 라우터로 보내게 된다.
- [0178] 나.패킷 처리부(230) : 라우터를 지나가는 패킷의 추출 및 해쉬 적용
- [0179] - 역추적에 필요한 작업을 수행하기 위해 라우터는 자신을 지나가는 IP 패킷을 추출한다. 추출된 패킷의 IP 헤더의 정보 등의 값들을 분석함으로써 이후 역추적을 위한 작업이 진행된다.
- [0180] - 앞서 설명한 바와 같이 패킷 정보를 해쉬하기 전에 IP 헤더의 특정 정보와 Payload의 일부분을 추출한다. 이렇게 추출된 정보는 24바이트의 정보이며, 이 정보를 두 개의 해쉬 함수를 이용하여 32비트의 두 해쉬 값을 추출한다.
- [0181] 다.Bloom Filter 처리부(250) : Bloom Filter를 이용하여 패킷의 경로를 확인
- [0182] - 추출된 두 해쉬 값은 먼저 패킷이 지나갔음을 기록하기 위해 Bloom Filter를 적용한다. 이후에 Bloom Filter를 이용하여 패킷이 지나갔음을 판단함으로써 공격 트래픽의 역추적을 한다.
- [0183] - 프로토콜 처리부(260)의 프로토콜을 이용하여 Manager 시스템으로부터 전송받은 두 해쉬 값은 자신의 해쉬 함수로부터 해쉬된 공격 패킷의 해쉬 값이다. 이 값이 자신을 지나갔다면 Bloom Filter에 기록이 되어 있을 것이며, 빠르게 확인을 할 수 있다. 해당 패킷이 자신을 지나갔음을 확인하고 그 결과를 Manager 시스템에 다시 전송함으로써 Manager 시스템이 공격 경로를 확인할 수 있도록 도와주며, 이 작업을 위해 Bloom Filter를 사용한다.
- [0184] 라.공격 패킷 처리부(290) : 현재 패킷이 공격 패킷인지 판단
- [0185] - 패킷을 라우팅 하기 전에 추출된 두 해쉬 값이 공격 패킷의 해쉬 목록에 유무를 확인한다. 공격 패킷의 해쉬 목록은 Manager 시스템으로부터 전송받은 공격 패킷의 해쉬 정보이므로, 해쉬 목록에 두 해쉬 값이 존재하게 되면 공격 패킷으로 판단하고 라우팅을 승인하지 않으며, 해당 공격 패킷을 Sinkhole 라우터로 전송한다.
- [0186] 마.Sinkhole 라우터 데이터부(280)의 처리 : 공격 패킷들을 흡수하며,Manager 시스템과의 연동
- [0187] - Sinkhole 라우터로 전송되는 공격 패킷들은 Sinkhole 라우터가 관리하게 된다. 관리되는 패킷들은 Manager 시스템의 요청으로 열람이 가능하며, 보안 관리자에 의해서 분석이 될 수 있다.
- [0188] - Sinkhole 라우터(라우터 들 중 어느 하나가 지정됨)는 다른 라우터로부터 패킷을 흡수할 때, 공격 패킷에 대해 Manager 시스템에게 공격 패킷에 대해 알린다. Manager 시스템은 실시간으로 공격의 유무의 확인과 역추적을 수행할 수 있다.
- [0189] - 모든 라우터는 Sinkhole 라우터의 기능을 수행할 수 있으며, 그 기능을 수행하기 위한 정보를 소유하고 있다. Sinkhole 라우터와 일반 라우터의 구분이 이루어지는 것은 Manager 시스템에 의해서 Sinkhole 라우터로 지정되는 것에 따른다. Sinkhole 라우터 지정 작업과 함께 자신의 수행을 결정한다.
- [0190] **Manager 시스템과 라우터 간 프로토콜(도 32참조)**
- [0191] 라우터는 패킷이 지나감과 함께 Bloom Filter에 기록하며, 공격 패킷을 판단하여 Sinkhole 라우터로 공격 패킷을 전송하며, Manager 시스템은 모든 라우터를 관리하면서 공격에 대한 역추적을 위한 분석을 주도하게 된다. 이런 과정을 위해 Manager 시스템과 라우터, 라우터와 Sinkhole 라우터, 그리고 Sinkhole 라우터와 Manager 시스템간의 통신이 필요하며, 이를 위한 프로토콜을 설계하였다.
- [0192] 프로토콜은 Manager 시스템이 라우터들에게 보내는 설정, 명령, 알람 등의 메시지와 라우터가 Manager 시스템으로 보내는 패킷의 이동 경로가 포함되어 있다.
- [0193] 'Start Code'는 프로토콜을 구분하기 위한 값이다. 1 바이트 크기의 고정된 값을 가지며, 다른 프로토콜과의

구분을 위한 값으로 사용된다.

- [0194] 'Message Code'는 보내는 단말의 ID와 목적지 ID, 전체 메시지의 길이, 그리고 메시지의 CRC 코드를 포함한다. ID는 라우터의 경우 '1'부터 시작되는 고유 번호이며, Manager 시스템은 '0'의 ID를 가진다. 메시지 길이는 'Start Code'부터 시작되는 전체 메시지의 바이트 크기이다. CRC코드는 'Message Header'의 시작 부분부터 'Message Body' 끝까지 CRC코드 부분을 제외한 값의 CRC를 구한 값이다.
- [0195] 'Message Body'는 실제 메시지 정보를 담고 있다. 2바이트 크기의 요청 ID를 포함하며, 메시지에 따라 크기가 가변적이다.
- [0196] 세부 모듈
- [0197] 본 발명에서의 개발 시스템의 주요 구성은 각 라우터에서의 Bloom Filter를 이용한 패킷 통과 유무를 확인하는 모듈 Manager 시스템에서 처리하는 공격에 대한 역추적을 수행하는 모듈이다. 또한 Manager 시스템과 라우터간의 메시지 통신을 위한 프로토콜 모듈도 포함되어 있다.
- [0198] **본 발명에서 개발한 Bloom Filter 모듈(도 33참조)**
- [0199] Bloom Filter 모듈은 라우터에 존재하며, Bloom filter를 생성하고, 불러드리고, 해쉬 값을 Bloom Filter에 적용하며, Bloom Filter에 값이 기록이 되어 있는지 확인하는 작업을 수행한다.
- [0200] Bloom Filter 생성에 의해서 생성되는 Bloom Filter의 크기는 512 메가바이트이다. 이는 32비트의 값을 기록하기 위한 크기이며, 이 공간을 생성하기 위해 파일시스템을 이용한다. 한번 생성된 Bloom Filter는 이후에 라우터에 의해서 불러지며, 라우터에서 기능을 수행하면서 지속적으로 사용된다. 추후 필요에 의해서 Bloom Filter는 삭제될 수 있으며, 기록된 모든 정보를 초기화 할 수도 있다.
- [0201] 라우터는 패킷의 정보를 추출하고 그 정보를 이용해서 두 개의 해쉬 값을 구한다. 해쉬 값들은 Bloom Filter의 적용되는 값이며, Bloom Filter에 기록된 값을 이용해서 패킷이 지나갔는지를 판단한다(도 34참조).
- [0202] **공격 트래픽 역추적 모듈**
- [0203] 공격 트래픽의 역추적 모듈은 실시간으로 이루어지는 경우와 사후 공격 경로 재구성으로, 두 가지의 방법을 제공한다(도 35참조).
- [0204] 실시간 역추적은 각각의 라우터들이 공격으로 판단한 트래픽을 Sinkhole 라우터로 전송하며, 트래픽을 받은 Sinkhole 라우터는 Manager 시스템에 패킷의 정보를 알람으로써 이루어진다. 그리고 사후 공격 경로 재구성은 Manager 시스템이 각 라우터에게 공격 패킷에 대한 등록을 요청할 때, 각 라우터들이 그 공격 패킷이 자신을 지나갔는지 알려면서 이루어진다.
- [0205] 실제 공격이 이루어진 상태에서 Manager 시스템은 공격패킷에 대한 각 라우터의 해쉬 함수를 적용하여 해쉬 값을 추출하고 라우터에게 전송한다. 해쉬 값을 받은 라우터들은 그 패킷이 자신을 지나갔는지를 Bloom Filter를 통해 확인하여 Manager 시스템에 알린다. 그 정보를 토대로 역추적 모듈은 공격 트래픽의 경로를 구성한다.
- [0206] Manager 시스템이 공격 패킷에 대한 해쉬 값을 라우터에게 전송할 때, 각 라우터들은 그 해쉬 값을 목록화 해서 저장하고 있다. 이 공격 해쉬 값의 목록은 같은 패킷이 라우터에 도착했을 때, 라우터는 트래픽을 Sinkhole 라우터로 돌리게 되고, 트래픽을 받은 Sinkhole 라우터는 패킷들을 흡수하면서 Manager 시스템에게 알린다. 이로써 실시간으로 Manager 시스템이 관리하는 네트워크 단위에서 공격에 대한 추적이 가능하다.
- [0207] **프로토콜 처리 모듈**
- [0208] 프로토콜 처리 모듈은 프로토콜 메시지를 송수신하기 위한 전송 모듈과 프로토콜을 해석하기 위한 해석 모듈로 나눌 수 있다.
- [0209] 전송 모듈은 메시지를 보내는 처리를 하는 부분과 메시지를 받는 처리를 하는 부분이 있다. Manager 시스템이나 라우터 모두 공통된 전송 모듈을 사용하며, 서로간의 ID를 이용한 통신 기능을 담당한다. 해석 모듈은 요청을 위한 메시지 생성과 수신된 메시지를 요청에 따라 해석하는 기능을 한다. 프로토콜 구조와 관련된 기능이며, Manager 시스템과 라우터 각각의 다른 작업을 수행한다.
- [0210] Manager 시스템이나 라우터에서 어떤 이벤트가 발생했고, 이를 처리하기 위해 요청메시지를 보내야 하는 상황이면, 프로토콜 모듈은 메시지를 생성하고 전송 모듈을 통해 목적지에 메시지를 전송한다. 마찬가지로 전송받은 메시지에 대해 프로토콜 모듈은 메시지를 해석하여 메시지의 신뢰성을 판단한 후 메시지가 요청한 작업을

수행하게 된다(도 36참조).

도면의 간단한 설명

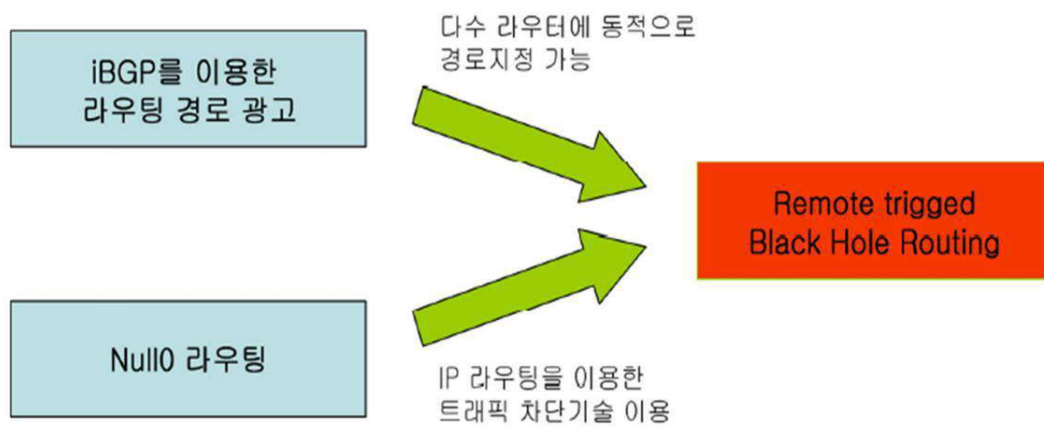
- [0211] 도 1은 종래기술에 따른 원격구동 블랙홀 라우팅 기술을 설명하기 위한 개념도이다.
- [0212] 도 2는 종래기술에 따른 목적지 기반 원격구동 블랙 라우팅 기술을 개략적으로 설명하기 위한 시스템 구성도이다.
- [0213] 도 3은 종래기술에 따른 싱크홀(sinkhole) 기술기반 블랙 스캐터(black scatter)현상을 이용한 공격경로 추적 기술을 설명하는 시스템 구성도이다.
- [0214] 도 4는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 경로로그 분석과정을 설명하는 도면이다.
- [0215] 도 5는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 패킷 로그중심 역추적 및 공격경로 추출과정을 나타낸 도면이다.
- [0216] 도 6은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 싱크홀 라우터 기반 공격 패킷 역추적 과정을 나타낸 도면이다.
- [0217] 도 7은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 bloom 필터(bloom filter) 기반 라우터를 이용한 공격 패킷 역추적 과정을 나타낸 도면이다.
- [0218] 도 8은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 아이피 패킷내 24바이트 해쉬 적용부분을 나타낸 도면이다.
- [0219] 도 9는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 bloom 필터기반 패킷 전송 경로정보 저장과정을 나타낸 도면이다.
- [0220] 도 10은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 32비트 bloom 필터 생성 매커니즘을 나타내는 도면이다.
- [0221] 도 11은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 프레임구조 및 전송장비별 모니터링 계층의 일예를 나타낸 도면이다.
- [0222] 도 12는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 Hop-by-Hop 패킷 전송과정을 개략적으로 나타내는 도면이다.
- [0223] 도 13은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 패킷에 대한 bloom 필터 생성 및 부가적 정보생성구조를 나타낸 도면이다.
- [0224] 도 14는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 패킷에 대한 bloom 필터 생성관련 세부 단계를 나타낸 도면이다.
- [0225] 도 15는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 공격 발생 시 라우터에서 싱크홀로 패킷을 전달하는 과정을 나타내는 도면이다.
- [0226] 도 16은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 매니저 시스템 기반 공격 역추적 과정을 개략적으로 나타내는 도면이다.
- [0227] 도 17은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 매니저 선정 및 라우터 초기화과정을 개략적으로 나타내는 도면이다.
- [0228] 도 18은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 싱크홀 라우터 설정 및 라우터 관리구조를 개략적으로 나타낸 도면이다.
- [0229] 도 19는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 공격 발생 시 각 라우터에서의 작동방식을 개략적으로 나타낸 도면이다.
- [0230] 도 20은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 공격 발생 시 피해시스템에서의 작동 방식 및 매니저 역할을 개략적으로 나타낸 도면이다.

- [0231] 도 21은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 DDos 공격 트래픽에 대한 싱크홀 라우터로의 전송 및 관리구조를 개략적으로 나타낸 도면이다.
- [0232] 도 22는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 매니저 기반시스템 설정 초기화단계를 나타낸 도면이다.
- [0233] 도 23은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 싱크홀 라우터 데이터구조의 일예를 개략적으로 나타낸 도면이다.
- [0234] 도 24는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 개별 라우터의 데이터구조의 일예를 개략적으로 나타낸 도면이다.
- [0235] 도 25는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 싱크홀 라우터정보 설정 단계를 개략적으로 나타낸 도면이다.
- [0236] 도 26은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 라우터 및 싱크홀 정보 설정 단계를 개략적으로 나타낸 도면이다.
- [0237] 도 27은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 일반 트래픽에 대한 처리과정의 일예를 개략적으로 나타낸 도면이다.
- [0238] 도 28은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 공격 트래픽에 대한 처리과정의 일예를 개략적으로 나타낸 도면이다.
- [0239] 도 29는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 매니저 시스템과 라우터 간의 관계를 개략적으로 나타낸 도면이다.
- [0240] 도 30은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 매니저 시스템 구조를 개략적으로 나타낸 도면이다.
- [0241] 도 31은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 라우터 시스템구조를 개략적으로 나타낸 도면이다.
- [0242] 도 32는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 매니저 시스템과 라우터간 통신을 위한 프로토콜 구조를 개략적으로 나타낸 도면이다.
- [0243] 도 33은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 블룸 필터 모듈의 개략적인 구조를 나타내는 도면이다.
- [0244] 도 34는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 블룸 필터를 이용한 라우터의 처리과정의 일예를 개략적으로 나타낸 도면이다.
- [0245] 도 35는 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 공격 트래픽 역추적 과정을 개략적으로 나타낸 도면이다.
- [0246] 도 36은 본 발명에 따른 올아이피네트워크 환경의 공격 탐지 및 추적 시스템에서의 프로토콜 처리과정을 개략적으로 나타낸 도면이다.
- [0247] * 도면의 주요부분에 대한 부호의 설명 *
- [0248] 10: 매니저(시스템)
- [0249] 11: 매니저 데이터부
- [0250] 13: 라우터 관리부
- [0251] 15: 공격패킷 관리부
- [0252] 17: 프로토콜부
- [0253] 21,22,23,24...: 라우터(시스템), 싱크홀 라우터(시스템)
- [0254] 210: 라우터 데이터부

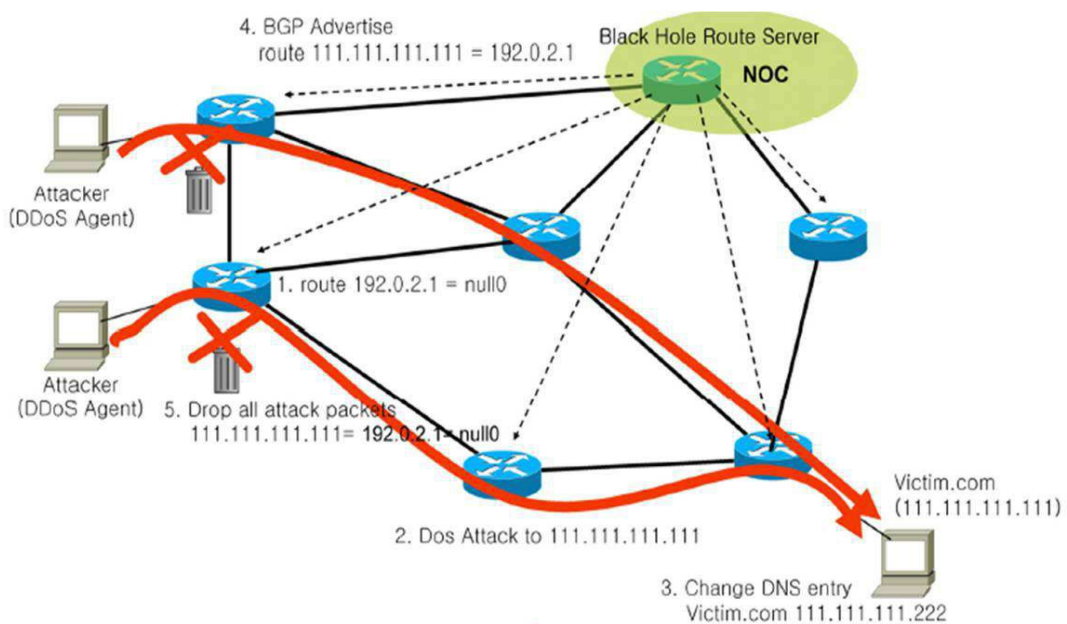
- [0255] 230: 패킷처리부
- [0256] 250: 블룸필터 처리부
- [0257] 260: 프로토콜 처리부
- [0258] 270: 공격패킷 처리부
- [0259] 280: 싱크홀 라우터데이터부
- [0260] 290: 공격패킷 처리부
- [0261] 31,32: (소스)단말, (목적지)단말

도면

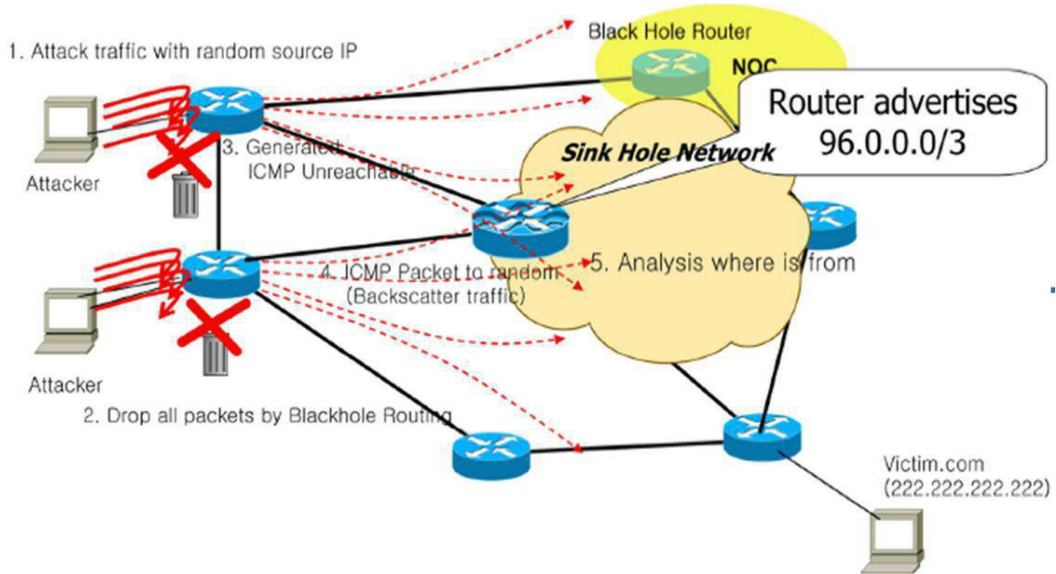
도면1



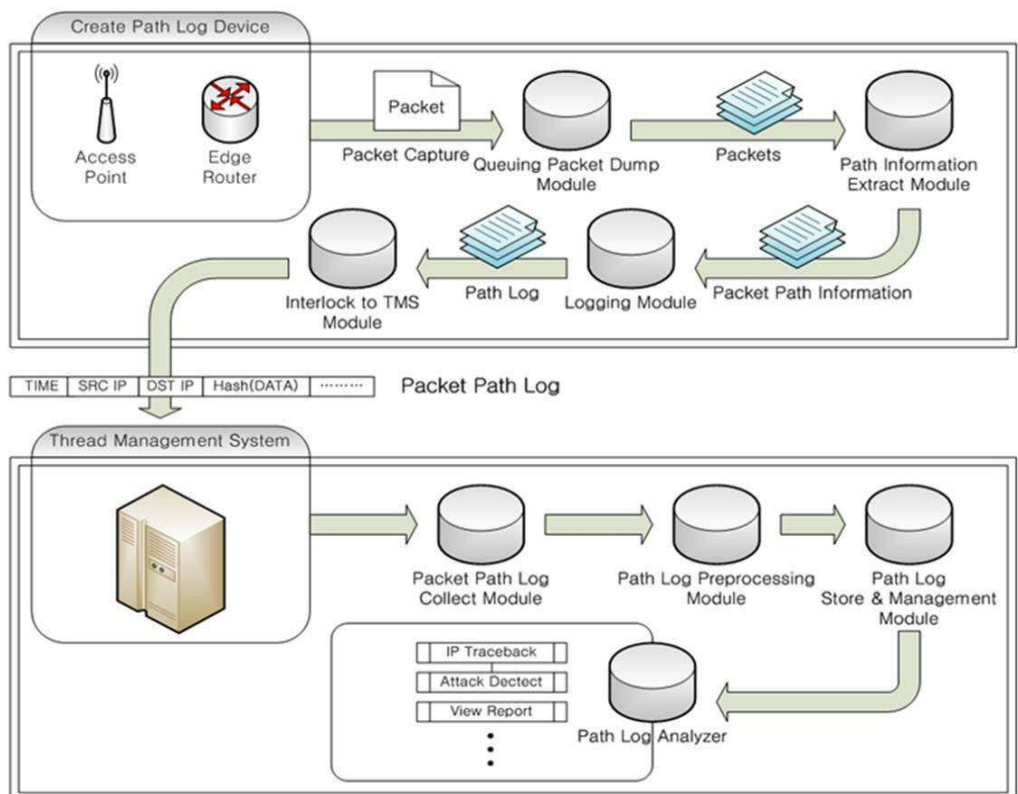
도면2



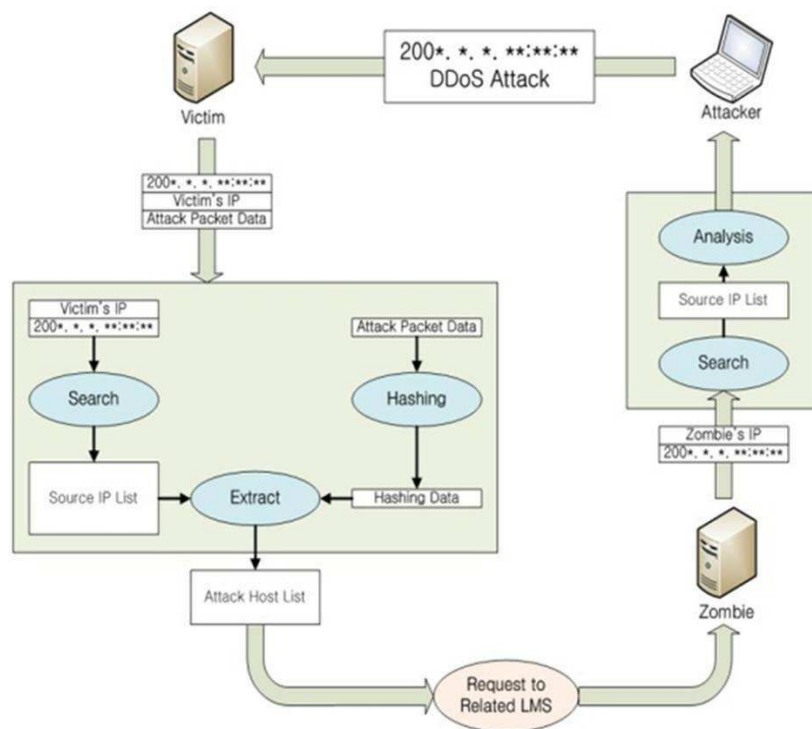
도면3



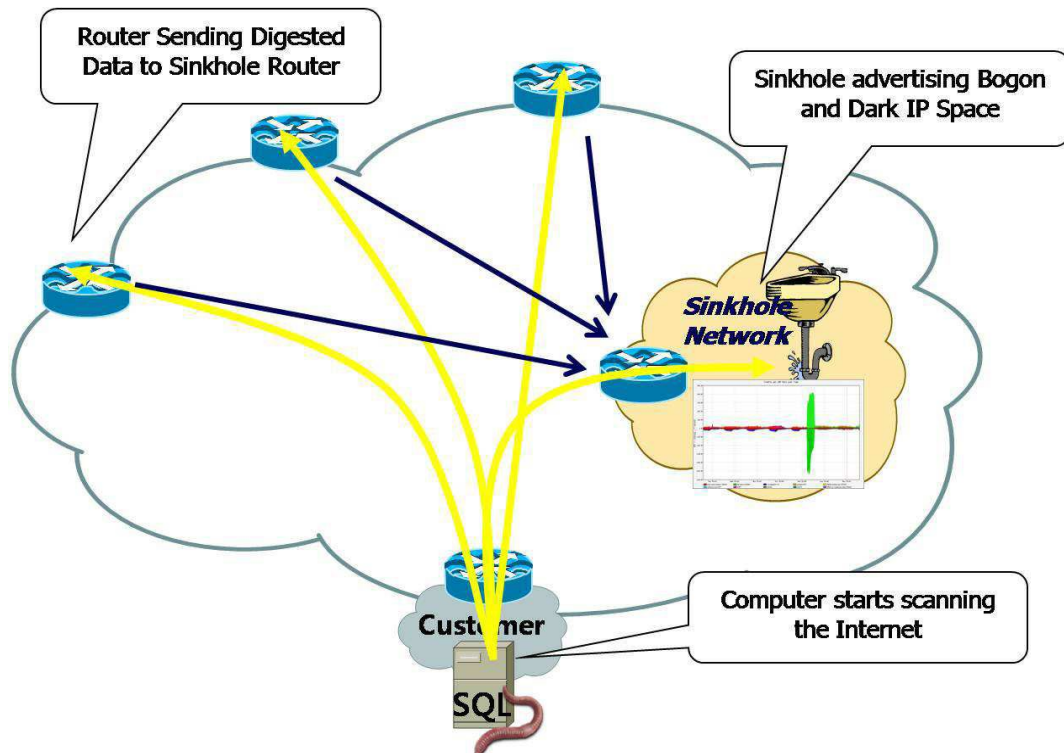
도면4



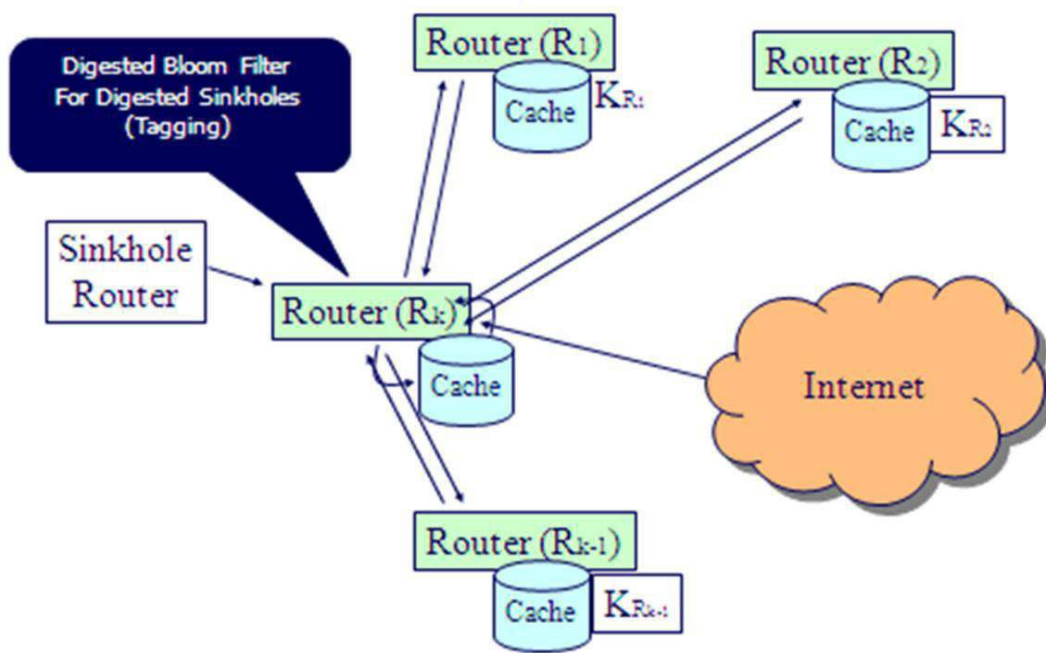
도면5



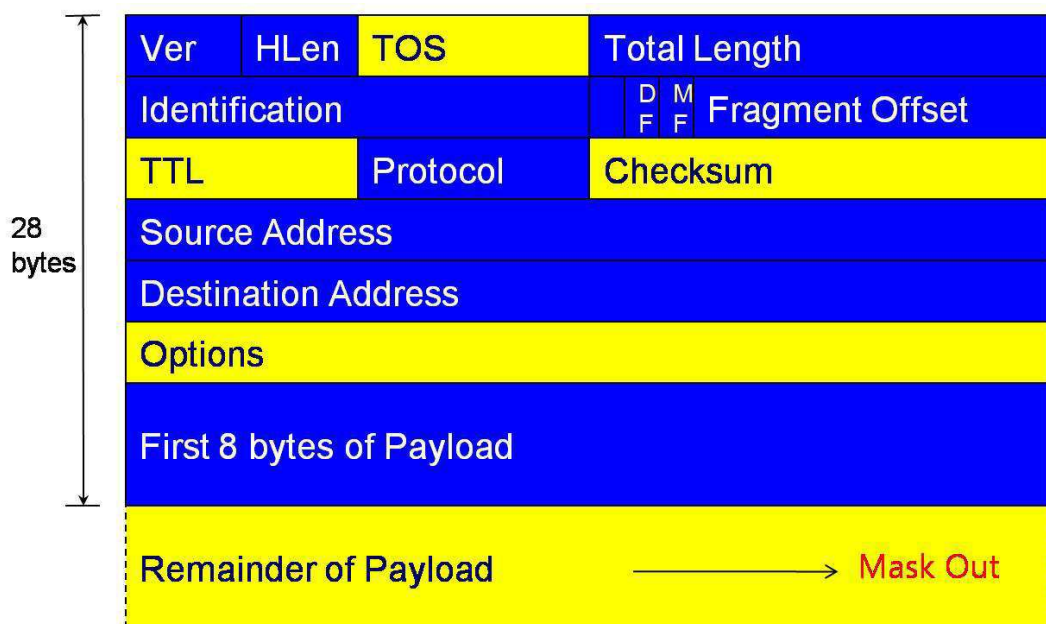
도면6



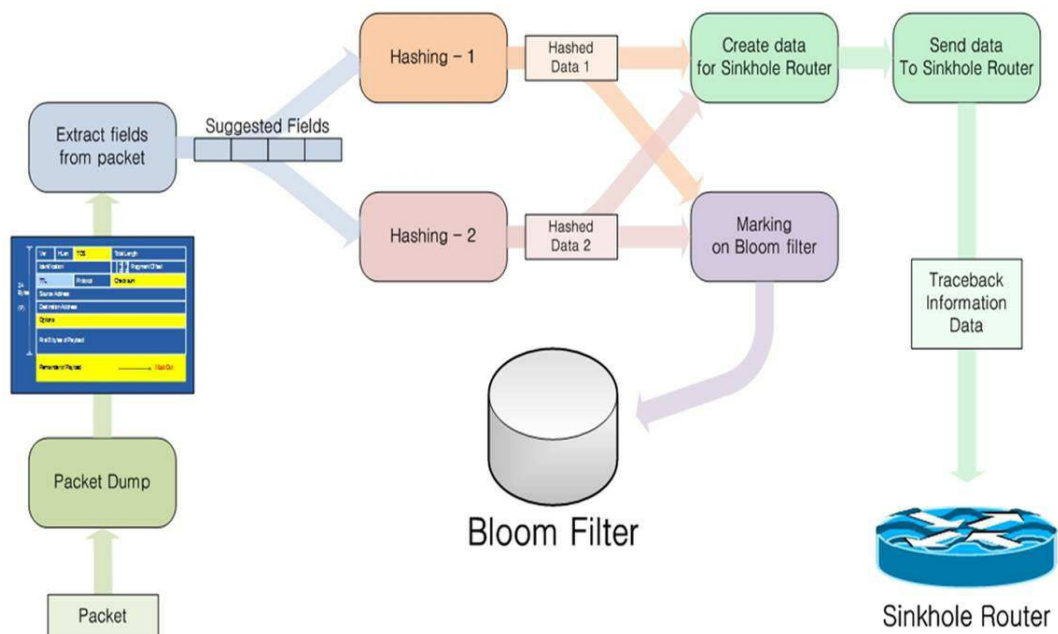
도면7



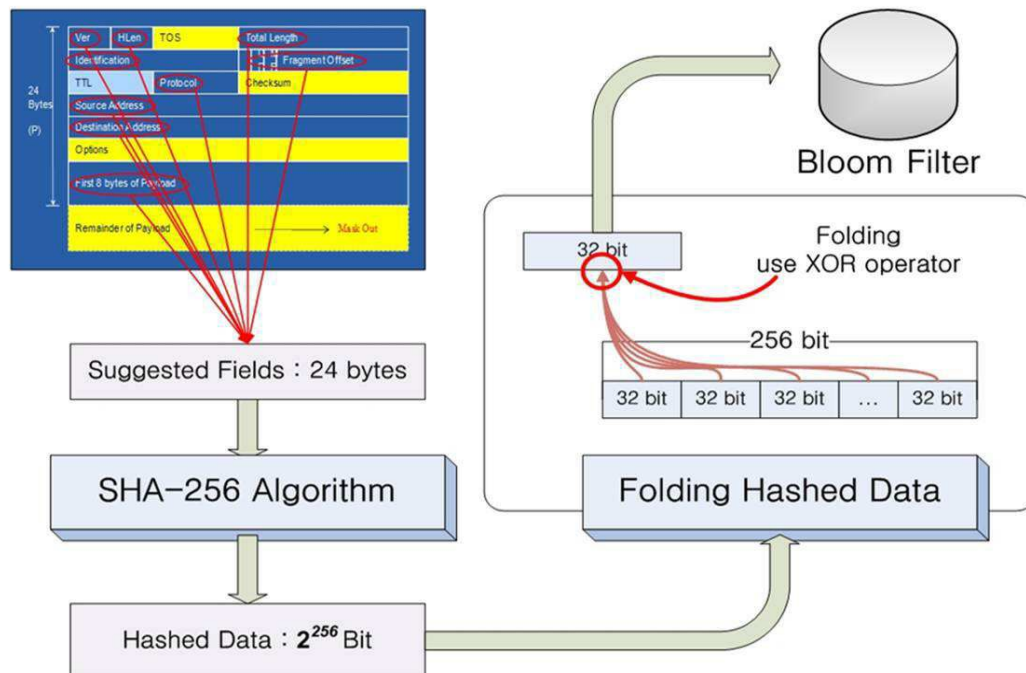
도면8



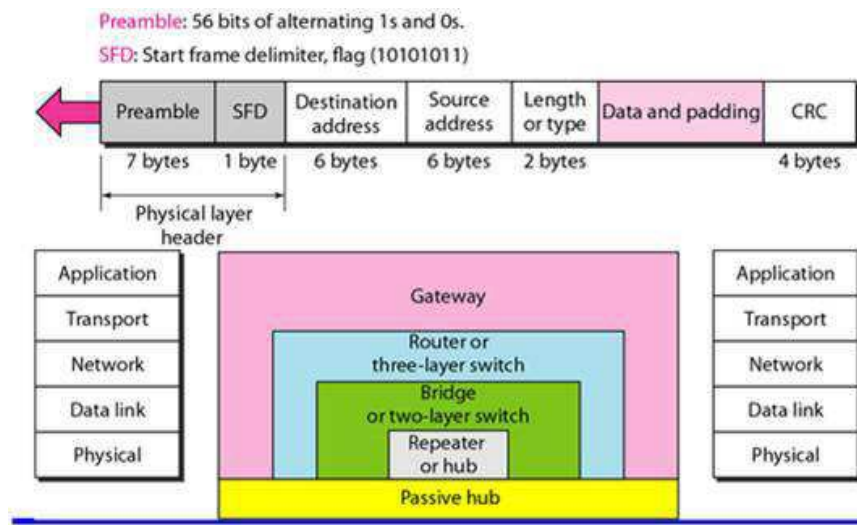
도면9



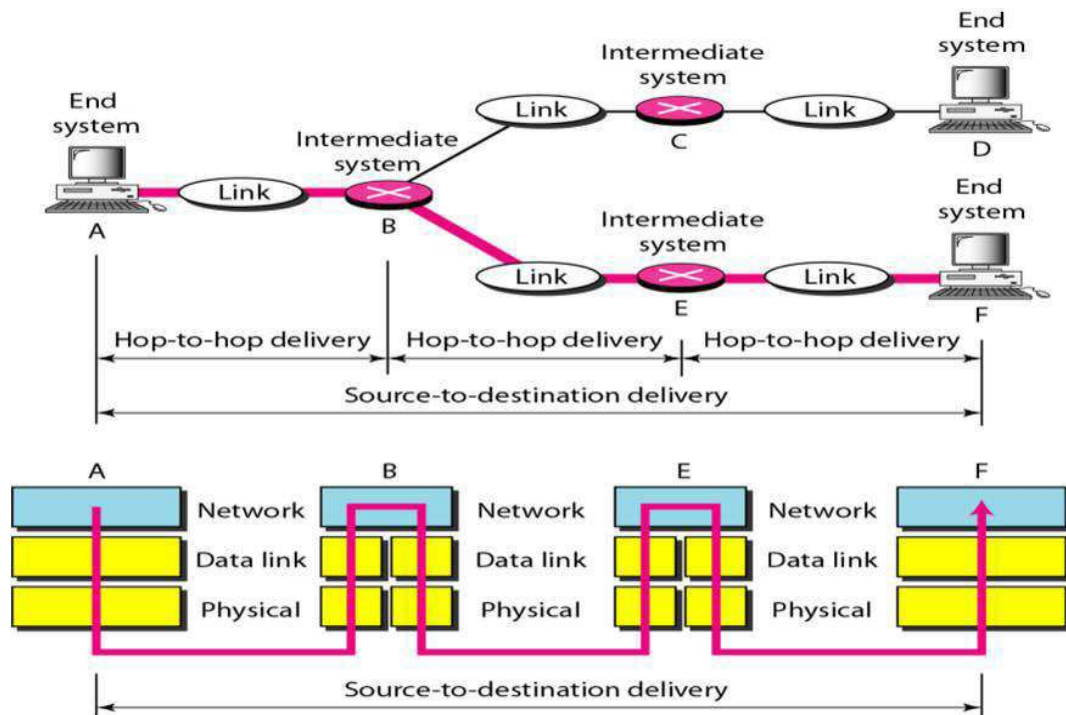
도면10



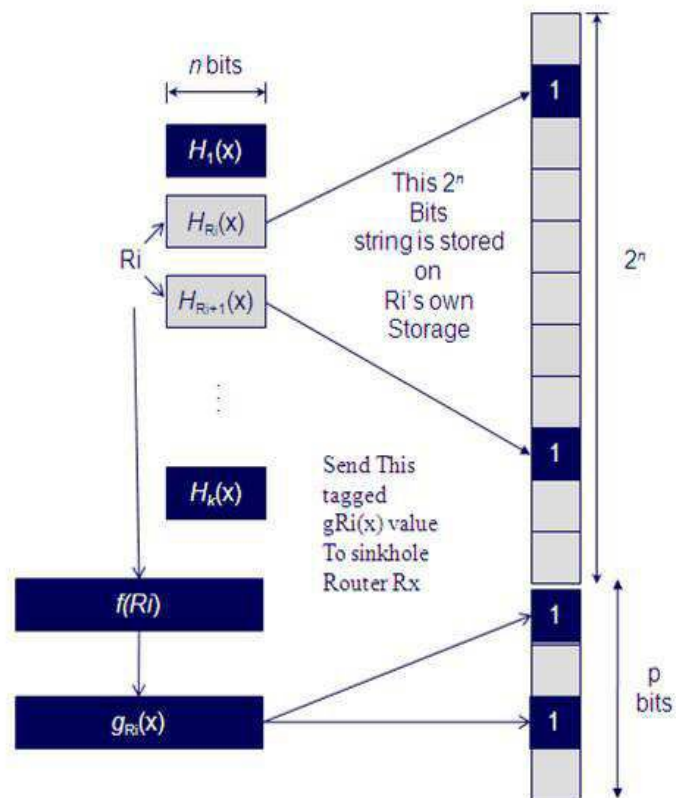
도면11



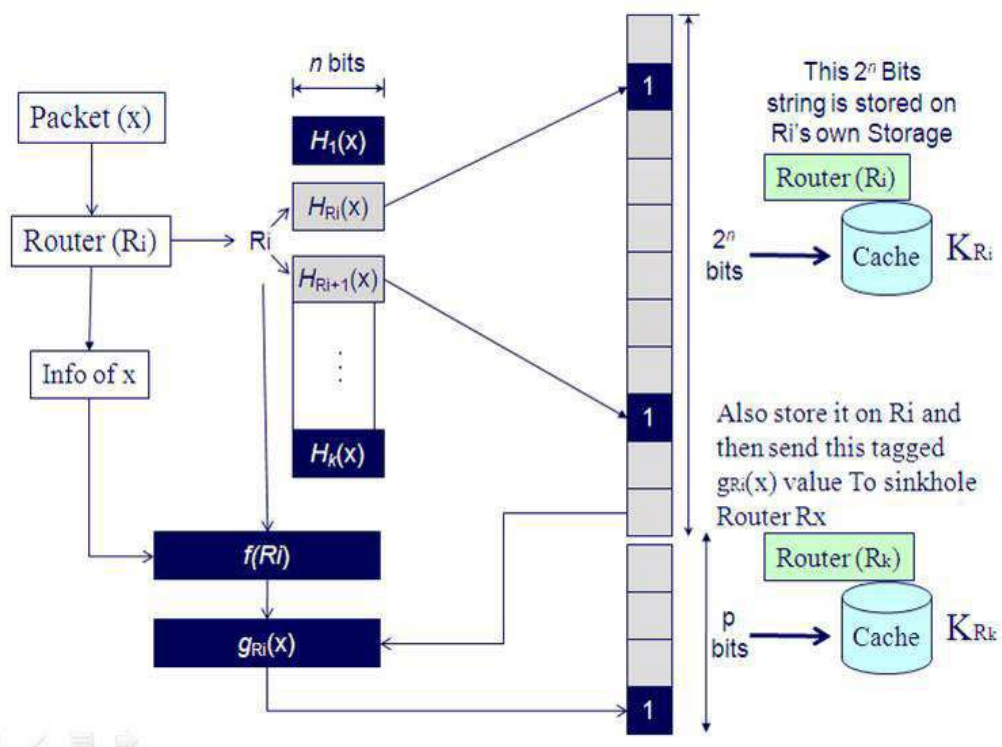
도면12



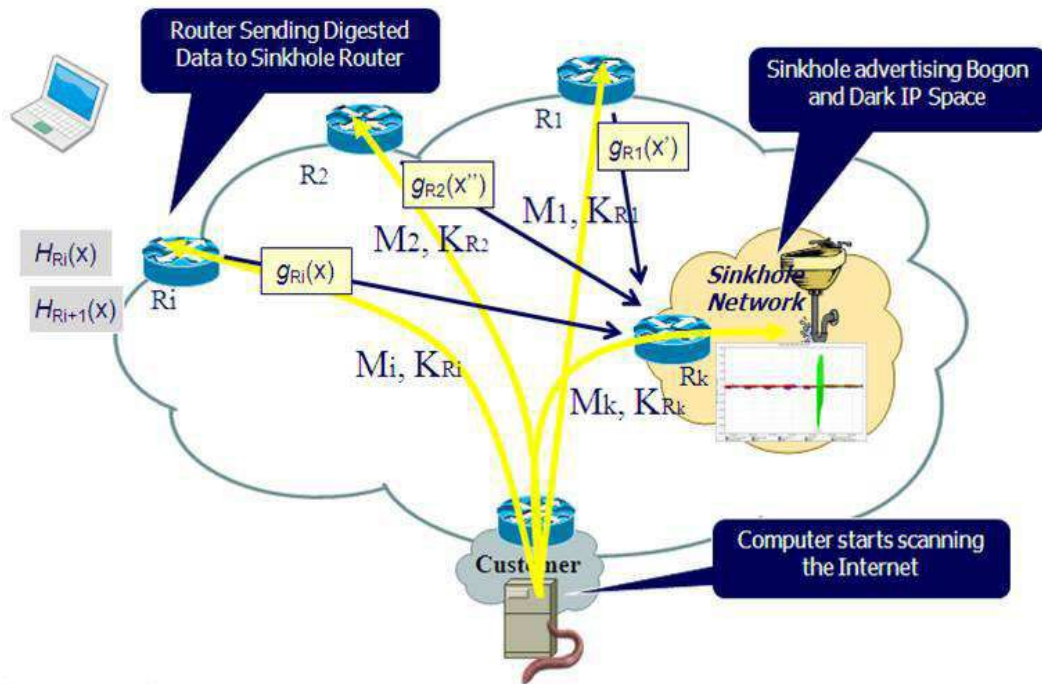
도면13



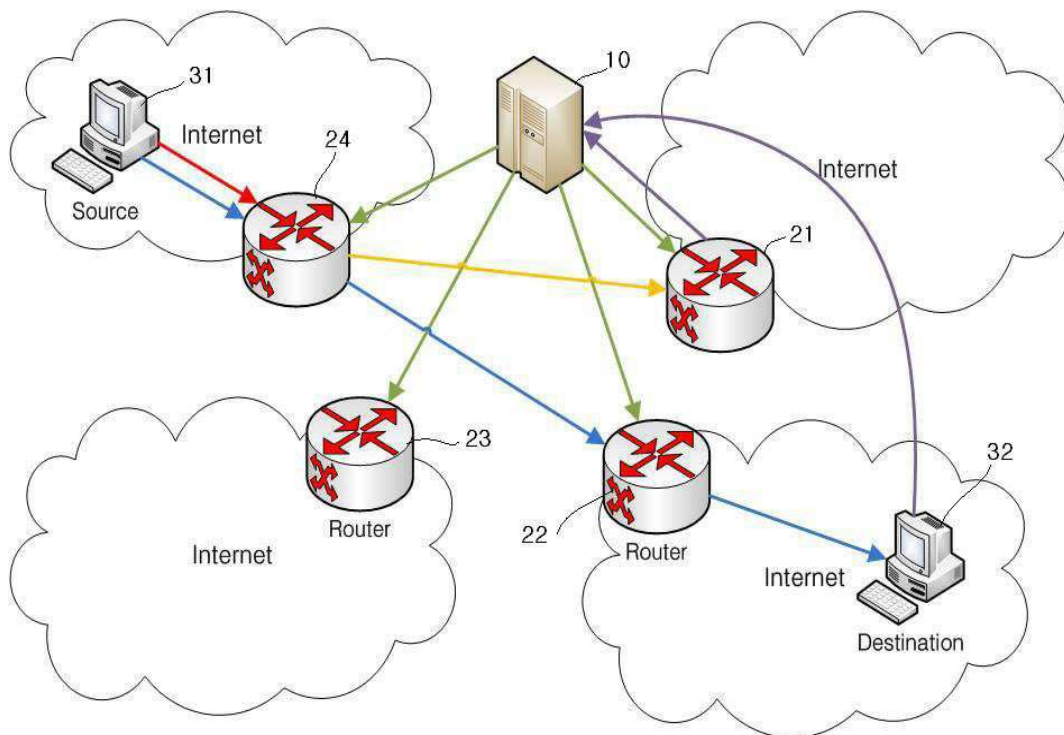
도면14



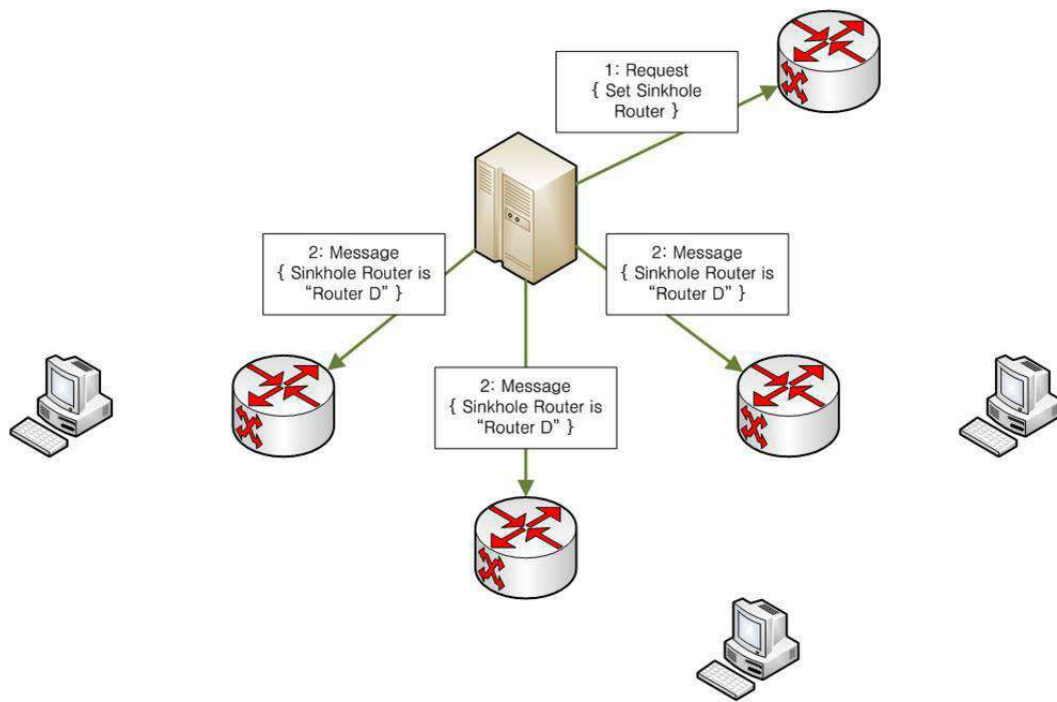
도면15



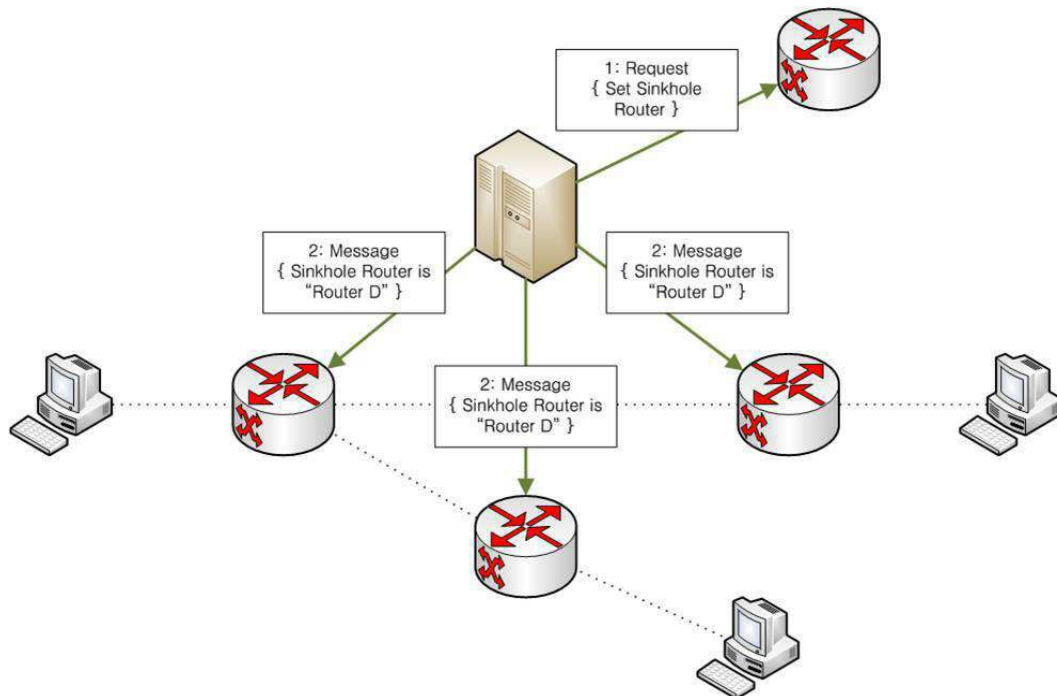
도면16



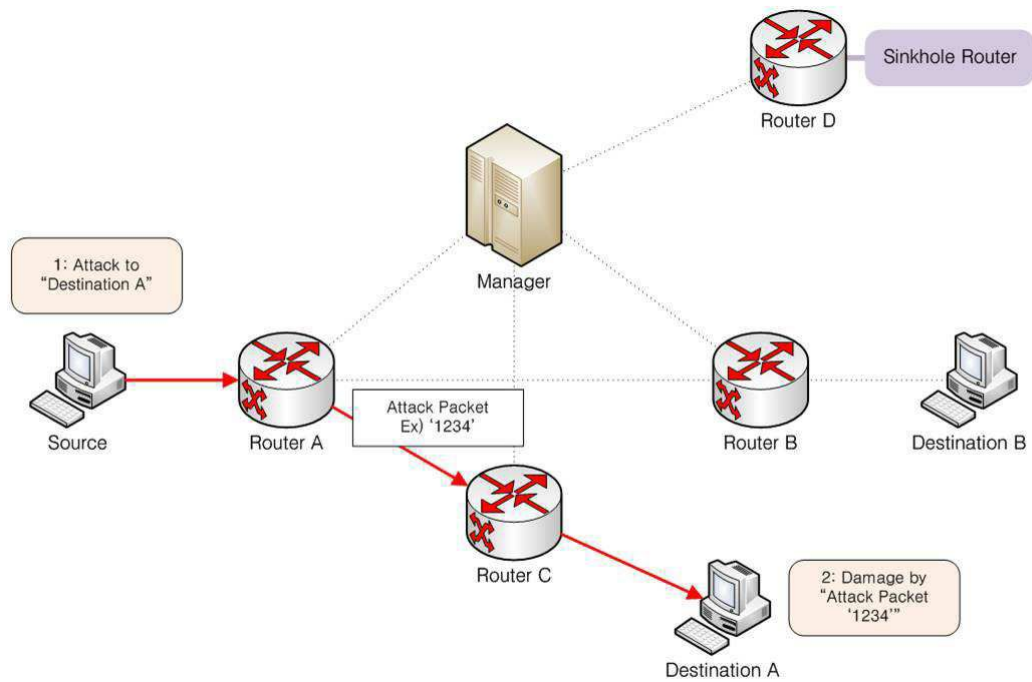
도면17



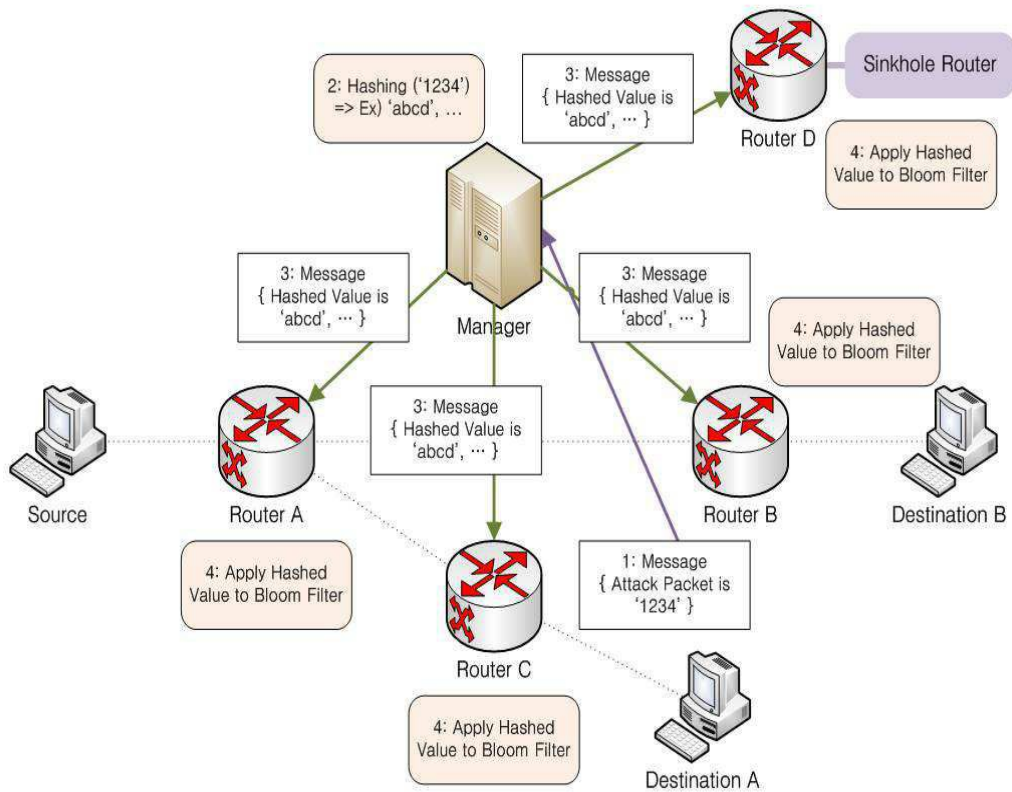
도면18



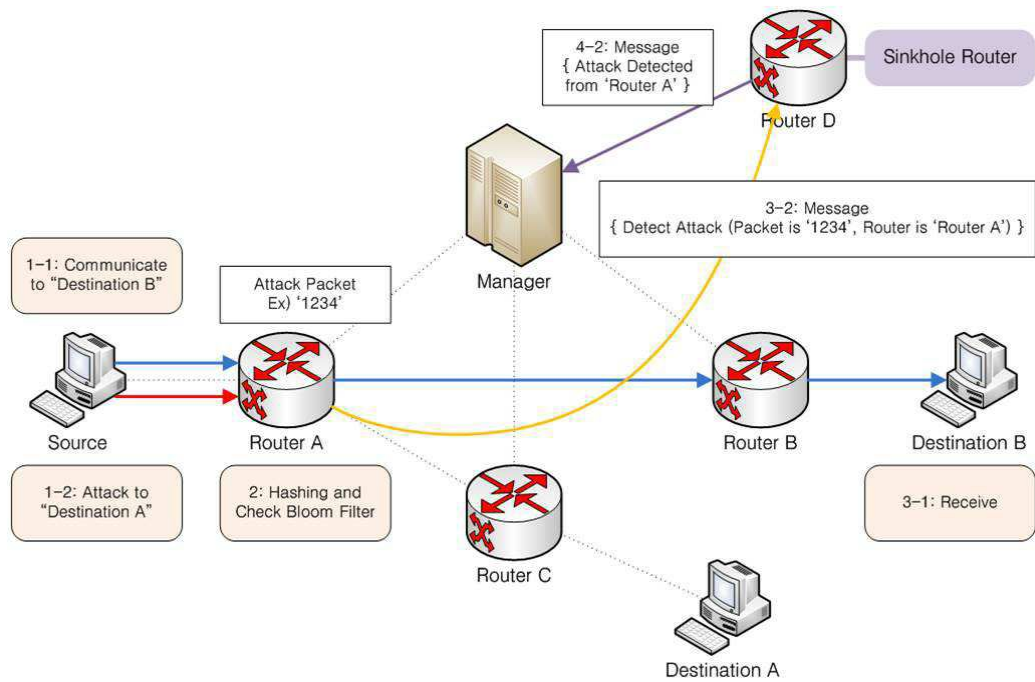
도면19



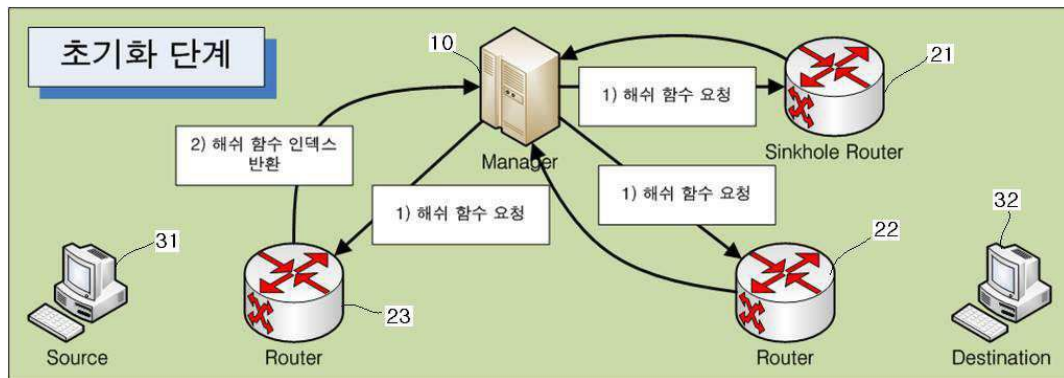
도면20



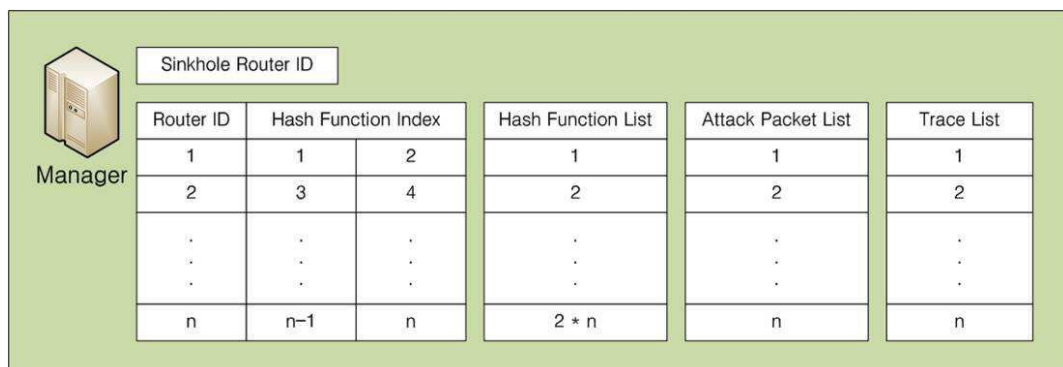
도면21



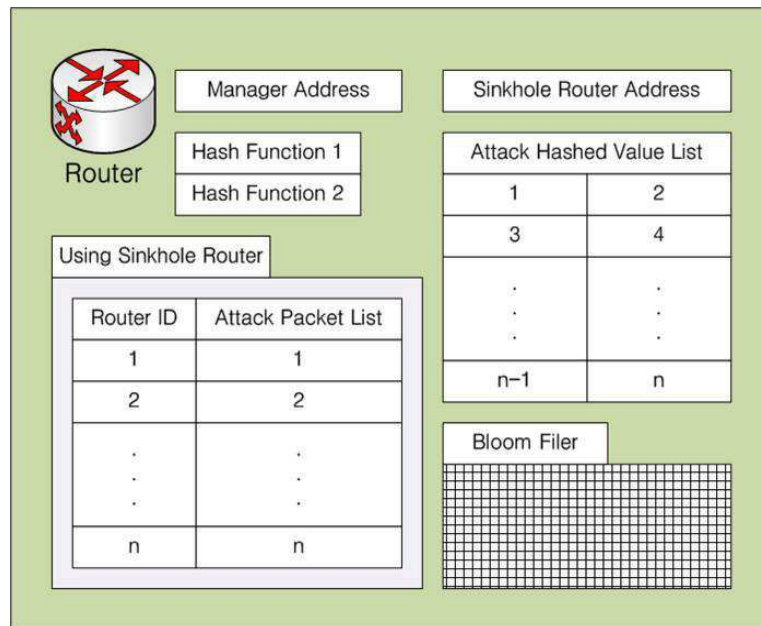
도면22



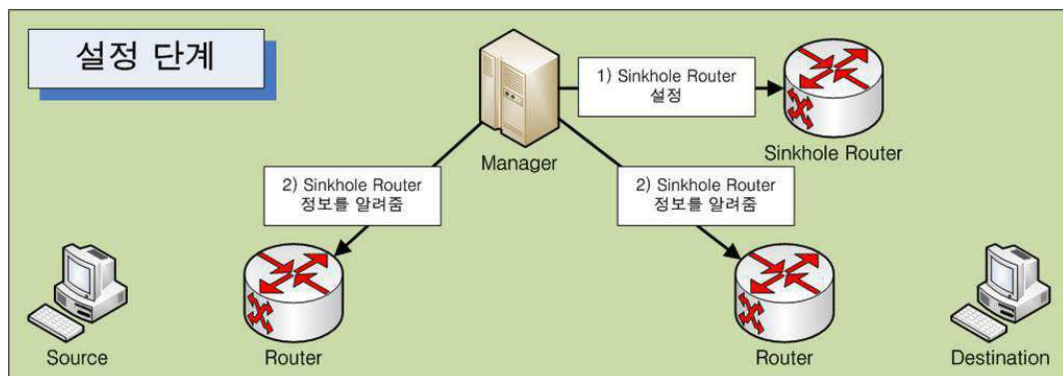
도면23



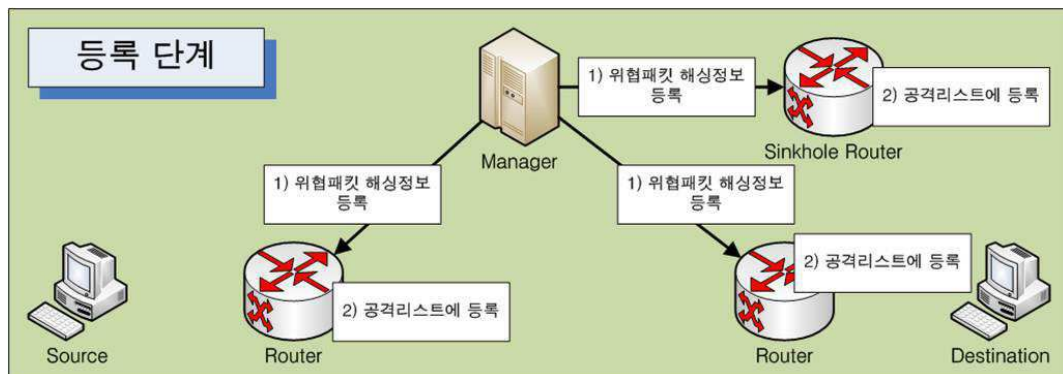
도면24



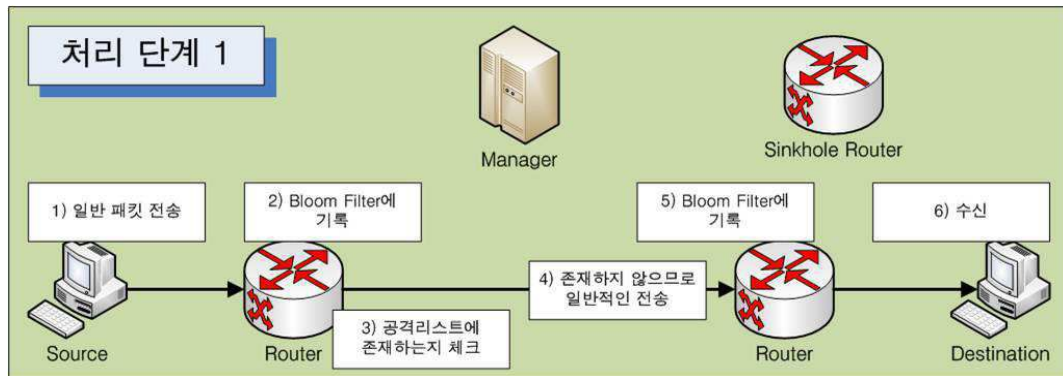
도면25



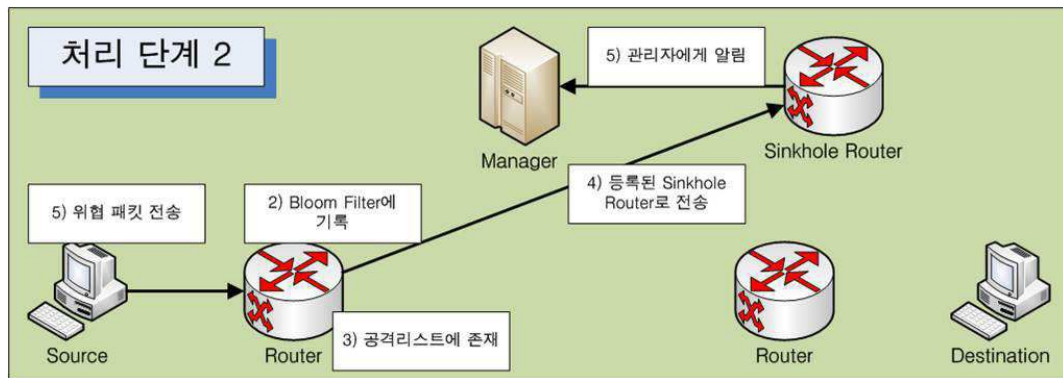
도면26



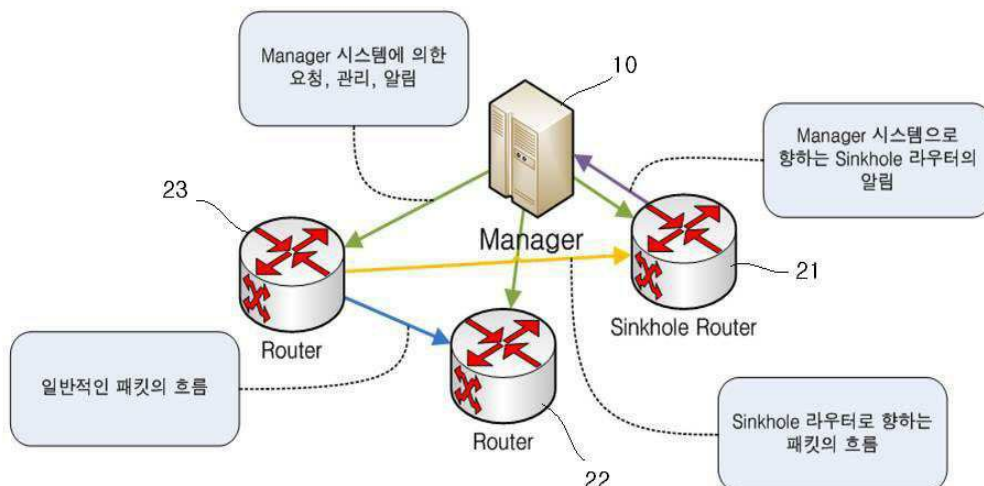
도면27



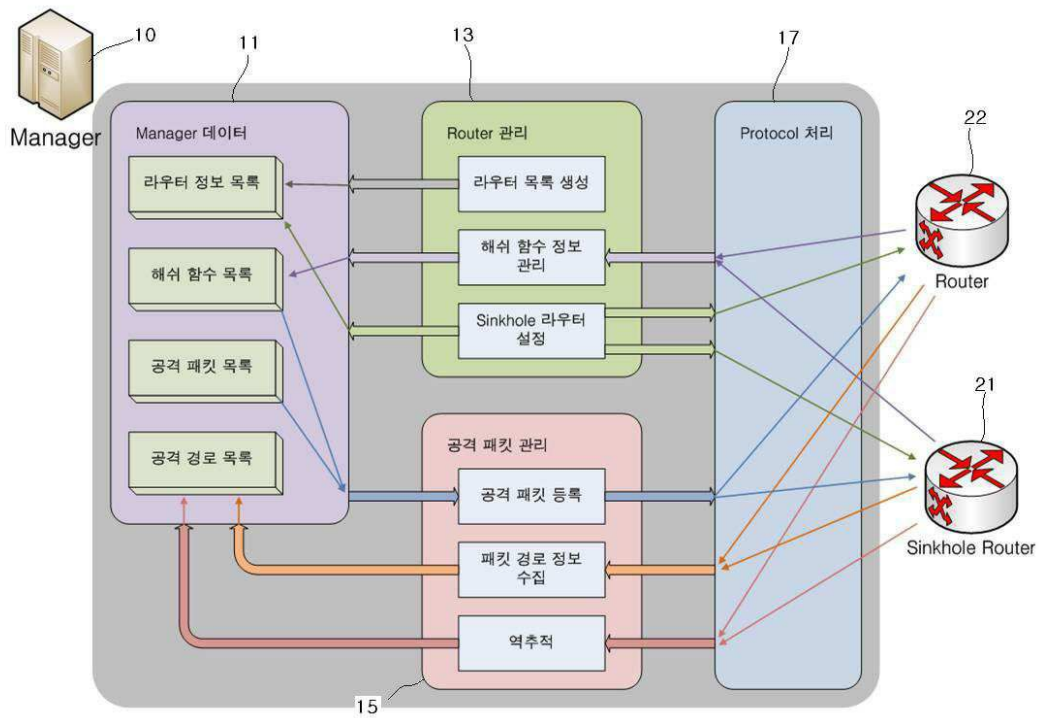
도면28



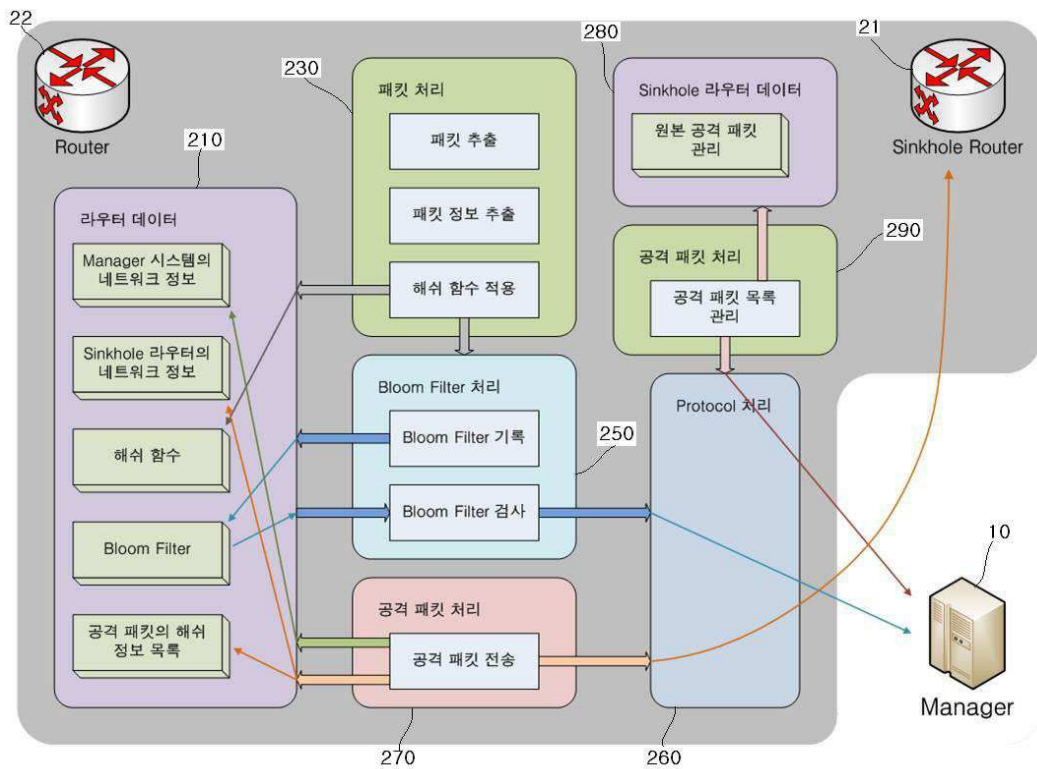
도면29



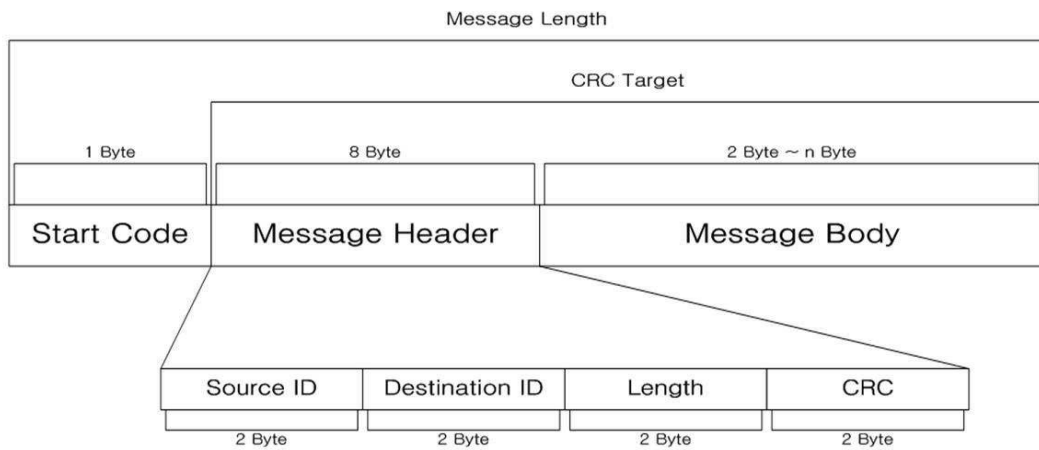
도면30



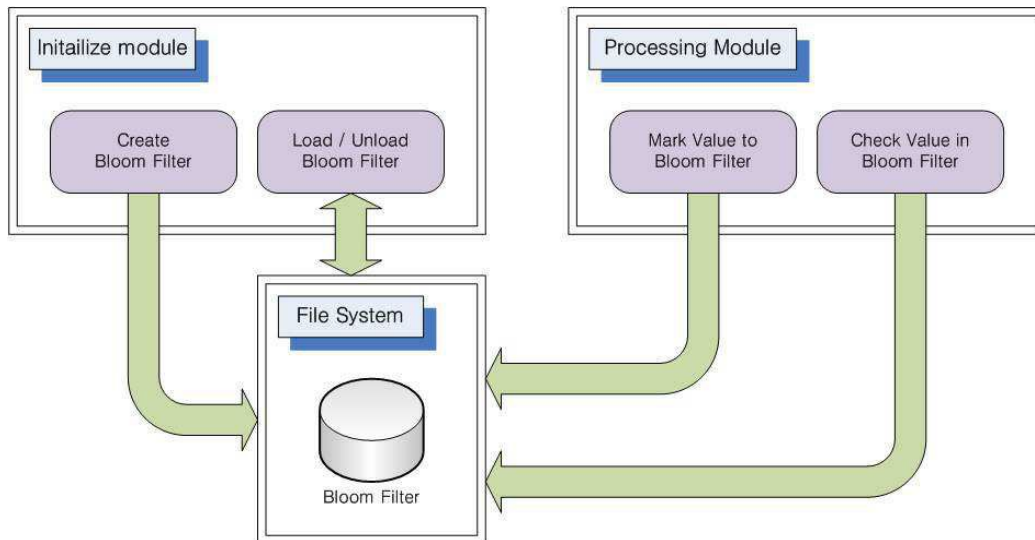
도면31



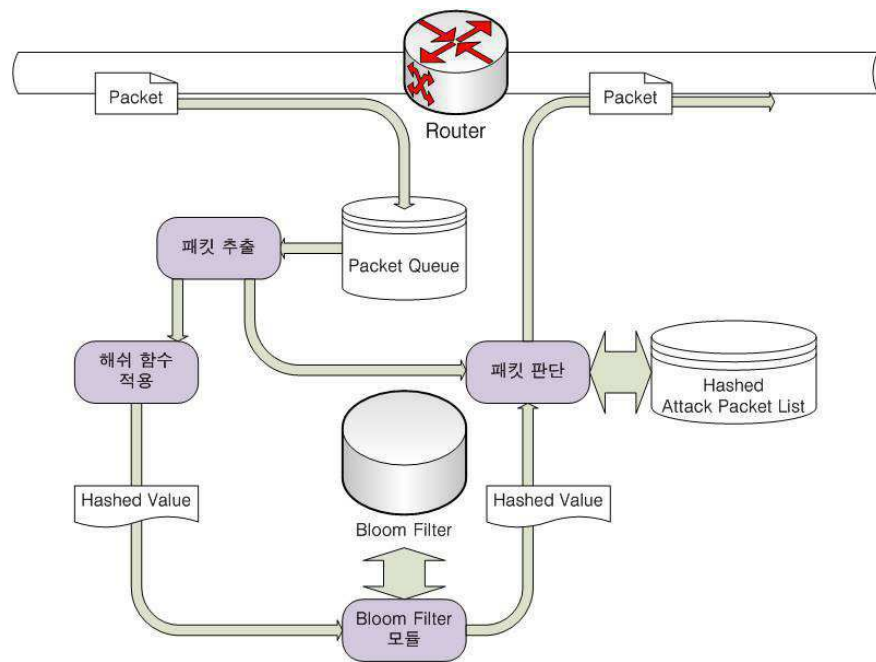
도면32



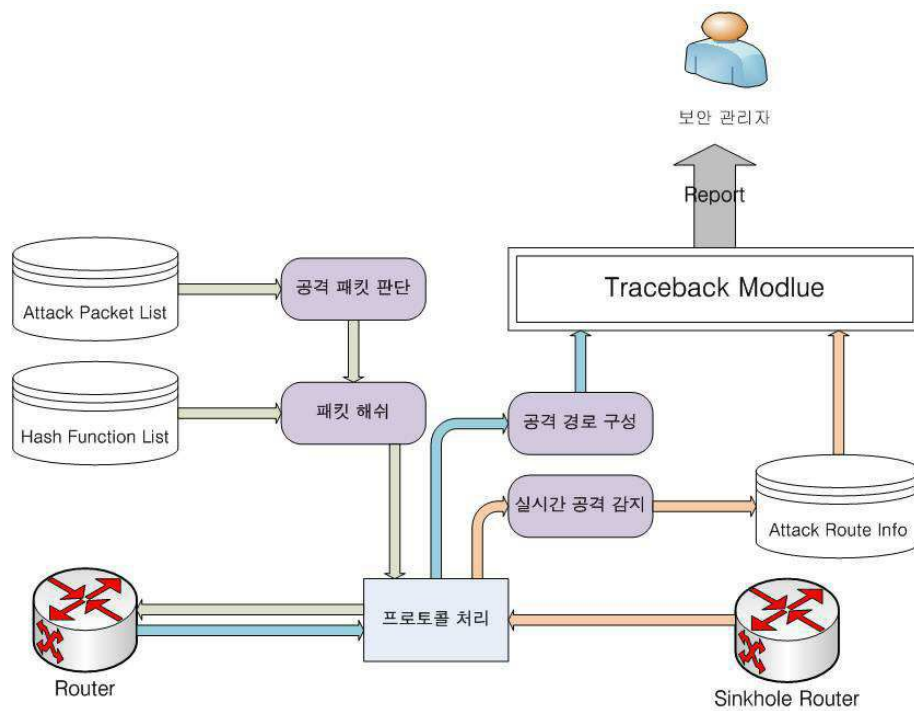
도면33



도면34



도면35



도면36

