(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0040631
(43) 공개일자 2024년03월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *G06F 16/901* (2019.01)
(52) CPC특허분류
H04L 63/1458 (2013.01)
G06F 16/9014 (2019.01)
(21) 출원번호 10-2023-0120679
(22) 출원일자 2023년09월11일
심사청구일자 2023년09월11일
(30) 우선권주장
1020220119420 2022년09월21일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
백상헌
서울특별시 서초구 고무래로 35, 109동 1004호
오서율
서울특별시 성북구 숭인로 50, 112동 3001호
한솔
서울특별시 노원구 동일로197길 85, A동 1504호
(74) 대리인
김등용

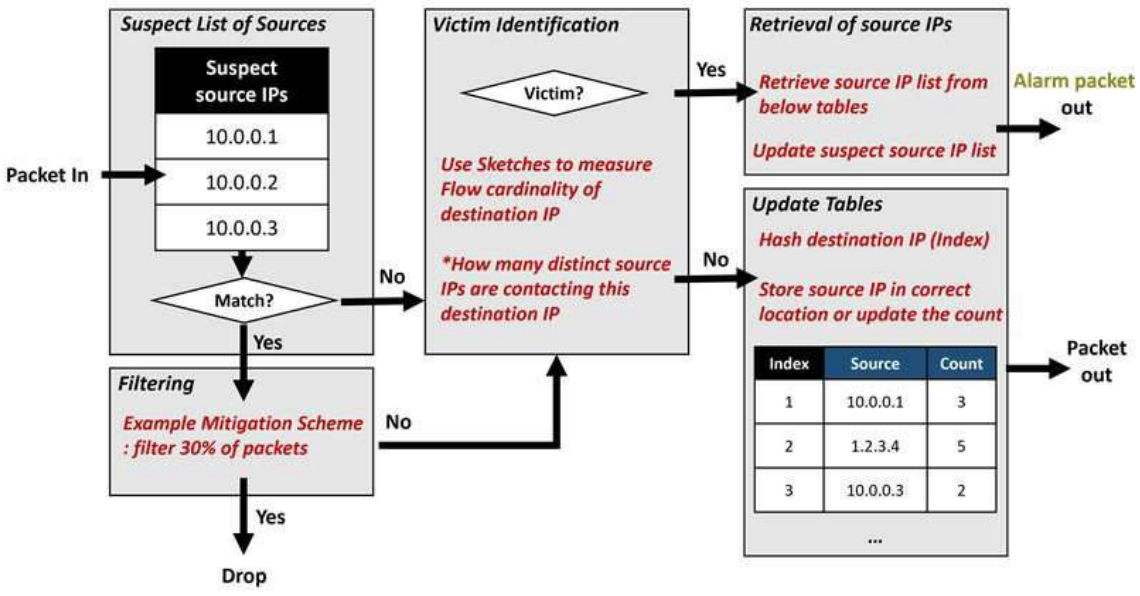
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 **프로그래밍 가능한 데이터 평면을 활용한 DDoS 공격 탐지 장치 및 방법**

(57) 요 약

프로그래밍 가능한(Programmable) 데이터 평면을 활용한 DDoS 공격 탐지 장치 및 방법이 개시된다. 상기 DDoS(Distributed Denial of Service) 공격 탐지 방법은 네트워크 시스템을 구성하는 프로그래밍 가능한 스위치에서 수행되는 DDoS 공격 탐지 방법으로써, 패킷이 수신되는 단계, 수신된 패킷이 필터링 대상 공격자로부터 송신된 것인지 여부를 판단하는 단계, 및 상기 수신된 패킷의 데스티네이션이 DDoS 공격의 피해자인지 여부를 판단하는 단계를 포함하고, 상기 피해자인지 여부를 판단하는 단계는 미리 정해진 시간 주기를 갖는 라운드(round) 내에서 상기 수신된 패킷의 데스티네이션 IP 주소로 패킷을 송신한 소스 IP 주소가 미리 정해진 n(n은 임의의 자연수) 개 이상인 경우에 상기 수신된 패킷의 데스티네이션을 피해자로 판단한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/0236 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711169318
과제번호 2020R1A2C3006786
부처명 과학기술정보통신부
과제관리(전문)기관명 한국연구재단
연구사업명 개인기초연구(과기정통부)
연구과제명 분산 AI 학습 지원을 위한 집단 엣지 네트워킹 기술 개발
기 여 율 1/2
과제수행기관명 고려대학교
연구기간 2022.03.01 ~ 2023.02.28
이 발명을 지원한 국가연구개발사업
과제고유번호 1711152525
과제번호 2021-0-01810-002
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 정보통신방송혁신인재양성
연구과제명 양자세계를 연결하는 초신뢰 양자인터넷 요소 기술 개발
기 여 율 1/2
과제수행기관명 고려대학교산학협력단
연구기간 2022.01.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

네트워크 시스템을 구성하는 프로그래밍 가능한(Programmable) 스위치에서 수행되는 DDoS(Distributed Denial of Service) 공격 탐지 방법에 있어서,

패킷이 수신되는 단계;

수신된 패킷이 필터링 대상 공격자로부터 송신된 것인지 여부를 판단하는 단계; 및

상기 수신된 패킷의 데스티네이션이 DDoS 공격의 피해자인지 여부를 판단하는 단계를 포함하고,

상기 피해자인지 여부를 판단하는 단계는 미리 정해진 시간 주기를 갖는 라운드(round) 내에서 상기 수신된 패킷의 데스티네이션 IP 주소로 패킷을 송신한 소스 IP 주소가 미리 정해진 n(n은 임의의 자연수) 개 이상인 경우에 상기 수신된 패킷의 데스티네이션을 피해자로 판단하는,

DDoS 공격 탐지 방법.

청구항 2

제1항에 있어서,

상기 프로그래밍 가능한 스위치는 상기 수신된 패킷의 데스티네이션 IP 주소로 상기 수신된 패킷을 다른 스위치를 경유하지 않고 직접 송신하는 스위치인,

DDoS 공격 탐지 방법.

청구항 3

제1항에 있어서,

상기 필터링 대상 공격자로부터 송신된 것인지 여부를 판단하는 단계는,

상기 수신된 패킷의 소스 IP 주소가 미리 저장되어 있는 공격자 리스트에 포함되어 있는 경우, 상기 수신된 패킷이 상기 필터링 대상 공격자로부터 송신된 것으로 판단하는,

DDoS 공격 탐지 방법.

청구항 4

제3항에 있어서,

상기 수신된 패킷이 상기 필터링 대상 공격자로부터 송신된 것으로 판단된 경우, 상시 수신된 패킷은 a(a는 0 보다는 크고 100 보다는 작거나 같은 실수)%의 확률로 필터링되는,

DDoS 공격 탐지 방법.

청구항 5

제4항에 있어서,

상기 피해자인지 여부를 판단하는 단계는,

상기 수신된 패킷이 상기 필터링 대상 공격자로부터 송신된 패킷이 아닌 것으로 판단된 경우 또는 상기 수신된 패킷이 상기 필터링 대상 공격자로부터 송신된 패킷으로 판단되었지만 필터링되지 않은 경우에 수행되는,

DDoS 공격 탐지 장치.

청구항 6

제1항에 있어서,

상기 피해자인지 여부를 판단하는 단계는 카운트민 스케치(Count-Min Sketch)의 데이터 구조를 이용하여 수행되고,

상기 카운트민 스케치에 포함되는 하나의 칸은 하나의 데스티네이션에 대응되고,

상기 카운트민 스케치에 포함되는 하나의 칸에서, 대응되는 데스티네이션으로 패킷을 송신한 소스 IP 주소의 해시한 값에 대응하는 인덱스의 공간에는 패킷이 수신된 라운드에 대한 정보가 기재되는,

DDoS 공격 탐지 장치.

청구항 7

제6항에 있어서,

상기 피해자인지 여부를 판단하는 단계는,

상기 카운트민 스케치 내에서 상기 수신된 패킷의 데스티네이션에 대응되는 칸에 기재된 현재 라운드의 개수를 상기 수신된 패킷의 데스티네이션 IP 주소로 패킷을 송신한 소스 IP 주소의 개수로 산출하는,

DDoS 공격 탐지 장치.

청구항 8

제1항에 있어서,

상기 수신된 패킷의 데스티네이션이 DDoS 공격의 피해자가 아닌 것으로 판단되는 경우, m(m은 임의의 자연수) 개의 해시 테이블들을 업데이트하는 단계를 더 포함하는,

DDoS 공격 탐지 장치.

청구항 9

제8항에 있어서,

상기 m 개의 해시 테이블들 각각의 인덱스는 패킷의 데스티네이션 IP 주소를 서로 상이한 해시 함수를 이용하여 해시하여 산출되는,

DDoS 공격 탐지 장치.

청구항 10

제9항에 있어서,

상기 업데이트하는 단계는,

상기 m 개의 해시 테이블들 중 제1 해시 테이블에서, 상기 수신된 패킷의 데스티네이션 IP 주소에 대응하는 인덱스의 저장 공간이 비어 있다면, 상기 수신된 패킷의 소스 IP 주소를 저장하고 소스 IP 주소에 대한 카운트 값을 1로 업데이트하는,

DDoS 공격 탐지 장치.

청구항 11

제10항에 있어서,

상기 업데이트하는 단계는,

상기 m 개의 해시 테이블들 중에서 제1 해시 테이블에서, 상기 수신된 패킷의 데스티네이션 IP 주소에 대응하는 인덱스의 저장 공간에 상기 수신된 패킷의 소스 IP 주소가 기재되어 있다면, 상기 수신된 패킷의 소스 IP 주소에 대한 카운트 값을 1 증가시키는,

DDoS 공격 탐지 장치.

청구항 12

제11항에 있어서,

상기 m 개의 해시 테이블들 중에서 제1 해시 테이블에서, 상기 수신된 패킷의 데스티네이션 IP 주소에 대응하는 인덱스의 저장 공간에 상기 수신된 패킷의 소스 IP 주소와 상이한 소스 IP 주소가 미리 저장되어 있다면, 상기 수신된 패킷의 소스 IP 주소를 저장하고 소스 IP 주소에 대한 카운트 값을 1로 업데이트하는,

DDoS 공격 탐지 장치.

청구항 13

제12항에 있어서,

상기 m 개의 해시 테이블들 중에서 제n(n은 2 보다 크거나 같고 m 보다 작거나 같은 자연수) 해시 테이블에서, 이전 해시 테이블에서 삭제된 데이터에 포함된 카운트 값과 상기 수신된 패킷의 데스티네이션 IP 주소를 해시한 값에 해당하는 인덱스에 기재된 소스 IP 주소의 카운트 값 중 큰 값에 해당하는 데이터만 상기 제n 해시 테이블에 유지되는,

DDoS 공격 탐지 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 프로그래밍 가능한 데이터 평면을 활용하여 DDoS 공격을 탐지하고 사전에 차단하는 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 프로그래밍 가능한 데이터 평면 기술은 사용자가 원하는 기능을 데이터 평면에 프로그래밍 가능하게 해주는 기술로, P4(Programming Protocol-Independent Packet Processor)와 같은 데이터 평면 프로그램 언어를 통해 사용자가 직접 파서 (Parser), 매치-액션 테이블(Match-Action Table) 등을 프로그래밍하여 기존의 기능을 수정 및 제거하거나 새로운 기능을 정의할 수 있다. 이러한 특성을 통해 기존에는 패킷 전달 기능만을 담당하던 데이터 평면을 사용자가 직접 프로그래밍하여 원하는 기능을 유연하게 제공하고 그것을 하드웨어 기반으로 빠르게 처리할 수 있게 하는 이점을 제공한다.

[0003] DDoS(Distributed Denial of Service) 공격은 특정 시스템에 과도한 트래픽을 보내거나 트래픽 발생을 유도함으로써 시스템의 자원을 고갈시켜 의도한 서비스를 사용자에게 제공할 수 없도록 하는 공격이다. 악의적인 의도로 시스템을 무력화시키기 위해 여러 대의 공격자를 분산적으로 배치하여 비정상적인 네트워크 성능 저하를 일으킨다. 최근에는 DDoS 공격의 대상이 되는 네트워크가 받는 악영향을 줄이고 공격자를 빠르게 찾아내서 공격을 차단하기 위한 다양한 기법들이 꾸준히 연구되고 있다.

[0004] DDoS 공격의 탐지와 사전 차단을 위해서는 공격과 공격자를 정확히 탐지하여 차단하는 것이 중요하다. 기존의 프로그래밍 가능한 데이터 평면을 활용한 DDoS 탐지와 사전 차단 기법들은 대부분 공격 트래픽을 전송하는 소스 중심의 기법들이다. 소스 중심의 기법들은 정해진 시간 동안 몇 개 이상의 패킷을 전송하는 소스들이 존재할 때 DDoS 공격이 이루어지고 있으며, 해당 소스들이 공격자라고 판단하는 탐지 기법과, 공격자라고 판단되는 소스들에서 온 트래픽을 막아내는 사전 차단 기법을 사용한다. 하지만 이는 네트워크 상황에 따라 DDoS 공격을 정확히 탐지하기 힘든 경우가 존재하여 공격과 공격자 탐지의 정확도가 떨어진다. 예를 들어, 대부분의 DDoS 공격은 공격자가 다른 여러 사람의 IP를 부당하게 취득하여, 한 소스 당 전송하는 패킷의 수는 적지만 한꺼번에 다량의 패킷을 받는 피해자의 시스템을 마비시키는 형태의 공격이다. 그러나 소스 중심의 기법들은 정해진 시간 동안 많은 패킷을 전송하는 소스가 있을 때 DDoS 공격이 이루어지고 있다고 판단하고 해당 소스들을 공격자로 판단하기 때문에 공격과 공격자를 탐지하는 정확도가 떨어진다.

[0005] 또한, 대부분의 기존 기법들은 공격과 공격자를 정확히 탐지하여 막기 위해 연산 능력과 메모리가 부족한 프로그래밍 가능한 스위치 대신 외부 컨트롤러가 개입한다. 외부 컨트롤러에서는 프로그래밍 가능한 스위치 내에서는 불가능한 스위치 레지스터의 초기화를 하거나, 스위치의 레지스터를 컨트롤러로 가져가서 프로그래밍 가능한 스위치에서는 할 수 없는 나눗셈, 곱셈 등의 연산을 활용하여 레지스터에 저장된 정보를 분석하는 등의 작업을

수행한다. 하지만 이러한 기법들은 컨트롤러와 스위치 사이의 통신으로 인한 지연시간과 트래픽이 증가한다는 문제점이 있다.

[0006] 그리고, 기존의 프로그래밍 가능한 스위치에서의 DDoS 공격 탐지/사전 차단 기법들은 대부분 하나의 스위치에서만 동작하도록 설계되어 여러 개의 스위치가 존재하는 네트워크의 일반적인 상황을 고려하지 않는다. 기존 기법들은 네트워크의 엣지 스위치에서 작동하도록 설계되어 공격을 탐지하고 공격자가 전송하는 트래픽을 막아낸다. 하지만 공격의 피해자로부터 거리가 먼 엣지 스위치에서는, 공격 트래픽이 잠재적으로 서로 다른 여러 개의 소스를 거쳐 들어오기 때문에 진행 중인 공격의 피해자가 있음을 제대로 인식하지 못하여 놓칠 가능성이 높다. 이를 해결하기 위해 반대로 피해자의 바로 앞의 스위치에서 DDoS 공격 탐지/사전 차단 기법을 적용한다면 정확도는 높을 수 있으나, 피해자 근처에 도달할 때까지 공격 트래픽이 폐기되지 않기 때문에 네트워크의 자원이 소진된다.

[0007] 따라서, 본 발명에서는 앞서 언급한 문제들을 해결한 DDoS 공격 탐지/사전 차단 기법을 제안한다. 기존의 소스 중심의 기법에서는 정해진 시간 동안 몇 개 이상의 패킷을 전송하는 소스들이 있을 때 DDoS 공격이 이루어지고 있으며 해당 소스들이 공격자라고 판단한다. 그래서 여러 사람의 IP를 부당하게 취득하여 공격자로 활용하는 DDoS 공격의 경우 한 소스 당 전송하는 패킷이 적어 정확히 공격과 공격자 소스를 탐지할 수 없다. 제안하는 기법에서는 n 개 이상의 서로 다른 소스로부터 패킷을 받는 DDoS 공격의 피해자를 특정하는 피해자 중심의 기법을 활용한다. 따라서 DDoS 공격의 피해자에게 패킷을 전송하는 소스를 찾아내서 막기 때문에 한 소스 당 전송하는 패킷의 수가 적더라도 공격과 공격자 탐지의 정확도가 높다. 또한, 기존 기법들은 외부 컨트롤러의 개입으로 인해 지연시간과 트래픽이 증가한다는 문제점이 있다. 제안하는 기법에서는 컨트롤러의 개입 없이도 프로그래밍 가능한 스위치에서 할 수 있는 연산만을 활용하며, 한 라운드 동안 특정 데스티네이션에 패킷을 보낸 서로 다른 소스가 몇 개인지 세는 방식을 사용한다. 이를 통해 컨트롤러의 도움으로 초기화를 하지 않아도 DDoS 공격의 피해자를 특정할 수 있다. 또한, 기존 기법들은 하나의 스위치에서만 동작한다. 네트워크 자원의 손실을 방지하고 공격을 빠르게 막기 위해서는 DDoS 공격 탐지/사전 차단 기법이 엣지 스위치에서 이루어져야 하나, 공격 탐지의 정확도를 높이기 위해서는 피해자 근처의 스위치에서 이 과정이 이루어져야 한다. 따라서 제안하는 기법은 공격과 공격자 탐지의 정확도를 높이기 위해 공격받는 피해자에 직접 연결된 스위치에서 해당 피해자가 DDoS 공격을 받고 있음을 확인하고, 그 피해자에게 패킷을 전송하는 top-k 소스들을 공격자로 식별하여 해당 IP 주소들의 리스트를 생성한다. 해당 리스트에 저장되어있는 소스 IP 주소를 가진 패킷이 들어오면, 필터링을 통해 DDoS 공격에 대한 사전 차단이 이루어진다. 또한, 해당 리스트를 알림 패킷의 헤더에 저장하여 다른 스위치들에게도 전달한다. 이 과정을 반복하여 DDoS 공격의 피해자로부터 먼 곳에 있는 스위치까지 점진적으로 리스트를 전달하여 필터링이 이루어지기 때문에, 공격자로부터 가까운 곳에서 공격을 막을 수 있어, 공격 트래픽이 피해자 근처까지 도달하여 네트워크 자원이 소진되는 것을 방지한다.

선행기술문헌

비특허문헌

[0008] (비특허문헌 0001) L. Gonzalez, L. Castanheira, J. —Marques, A. Schaeffer-Filho and L. Gaspary, "BUNGEE: An Adaptive Pushback Mechanism for DDoS Detection and Mitigation in P4 Data Planes," in Proc. 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 393-401, Virtual Online Conference, May 2021.

(비특허문헌 0002) D. Ding, M. Savi, F. Pederzolli, M. Campanella and D. Siracusa, "In-Network Volumetric DDoS Victim Identification Using Programmable Commodity Switches," IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1191-1202, June 2021.

발명의 내용

해결하려는 과제

[0009] 본 발명이 이루고자 하는 기술적인 과제는 프로그래밍 가능한 데이터 평면을 활용한 DDoS 공격 탐지 장치 및 방법을 제공하는 것이다.

과제의 해결 수단

[0010] 본 발명의 일 실시예에 따른, 네트워크 시스템을 구성하는 프로그래밍 가능한(Programmable) 스위치에서 수행되는 DDoS(Distributed Denial of Service) 공격 탐지 방법은 패킷이 수신되는 단계, 수신된 패킷이 필터링 대상 공격자로부터 송신된 것인지 여부를 판단하는 단계, 및 상기 수신된 패킷의 데스티네이션이 DDoS 공격의 피해자인지 여부를 판단하는 단계를 포함하고, 상기 피해자인지 여부를 판단하는 단계는 미리 정해진 시간 주기를 갖는 라운드(round) 내에서 상기 수신된 패킷의 데스티네이션 IP 주소로 패킷을 송신한 소스 IP 주소가 미리 정해진 n(n은 임의의 자연수) 개 이상인 경우에 상기 수신된 패킷의 데스티네이션을 피해자로 판단한다.

발명의 효과

[0011] 본 발명을 통해 DDoS 공격의 피해자를 프로그래밍 가능한 데이터 평면을 활용해 파악하여, DDoS 공격의 피해자에게 트래픽을 전송하는 공격자 소스들을 특정할 수 있다. 성능 평가를 위해 시뮬레이션을 진행하고 기존 DDoS 공격 탐지 및 사전 차단 기법과 비교를 진행하였다. 비교 기법인 BUNGEE(비특허문헌 1)는 정해진 시간 동안 몇 개 이상의 패킷을 전송하는 소스들이 존재할 때 DDoS 공격이 이루어지고 있으며, 해당 소스들이 공격자라고 판단하는 소스 중심 기법이다.

도면의 간단한 설명

[0012] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시예에 따른, DDoS 탐지 동작의 전반적인 과정을 나타낸다.

도 2는 DDoS 공격 피해자 탐지 과정을 설명하기 위한 카운트민 스케치(Count-Min Sketch) 구조를 도시한다.

도 3은 DDoS 공격의 피해자에게 패킷을 전송하는 공격자를 찾아내는 과정을 나타낸다.

도 4는 본 발명의 네트워크 환경을 나타낸 시스템 모델이다.

도 5는 본 발명의 일 실시예에 따른, 프로그래밍 가능한 데이터 평면을 활용한 DDoS 탐지 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시예들에 한정되지 않는다.

[0014] 본 발명의 개념에 따른 실시예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0015] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0016] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0017] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는

이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0018] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0019] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시예들을 상세히 설명한다. 그러나, 특허출원의 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0020] 우선, 본 발명의 전체적인 동작 과정을 설명한다.

[0021] 도 1은 본 발명의 일 실시예에 따른, DDoS 탐지 동작의 전반적인 과정을 나타낸다.

[0022] 도 1을 참조하면, 첫 번째로, 패킷이 들어오면(Packet In) 해당 패킷의 소스(source) IP 주소를 스위치(예컨대, 프로그래밍 가능한 스위치(Programmable switch))에서 가지고(또는 유지하고) 있는 필터링 대상 공격자 IP 주소들의 리스트와 비교한다. 만약, 패킷의 소스 IP 주소가 리스트에 존재한다면 정해진 확률로 필터링을 하고, 아니라면(즉, 패킷의 소스 IP 주소가 리스트에 존재하지 않는다면) 해당 패킷의 데스티네이션(destination, 목적지) IP 주소가 n(n은 임의의 자연수) 개 이상의 서로 다른 소스로부터 패킷을 받는 DDoS 공격의 피해자인지 확인하는 두 번째 단계로 넘어간다. 만약 피해자가 존재한다면 해당 피해자에게 패킷을 전송하는 top-k(k는 임의의 자연수) 소스들을 리스트에 저장한 후 해당 소스로부터 오는 패킷들을 필터링하고, 리스트를 헤더에 저장한 알림 패킷을 생성하여 다른 스위치들에게 전송한다. 반면, 만약 피해자가 존재하지 않는다면 패킷의 소스 IP 주소를 카운트하기 위해 새로 스위치의 테이블에 저장하거나, 이미 테이블에 저장되어 있다면 카운트를 1 증가시킨다.

[0023] **동작 과정 1 : DDoS 공격의 피해자를 탐지하는 과정**

[0024] 도 2는 프로그래밍 가능한 스위치로 들어온 패킷의 데스티네이션 IP 주소가 n 개 이상의 소스로부터 패킷을 받는 DDoS 공격의 피해자인지 확인하는 과정을 나타낸다. 기존의 기법들은 소스 중심의 기법이기 때문에 정해진 시간 동안 많은 패킷을 전송하는 소스가 있을 때 DDoS 공격이 이루어지고 있다고 판단하고 해당 소스들을 공격자로 판단한다. 그러나 공격자가 여러 소스를 부당하게 취득하는 DDoS 공격의 경우 한 소스당 전송하는 패킷이 적어 공격과 공격자 소스를 정확히 탐지할 수 없다. 따라서, 제안하는 기법에서는 n 개 이상의 서로 다른 소스로부터 패킷을 받는 DDoS 공격의 피해자를 특정하여 DDoS 공격의 피해자에게 패킷을 전송하는 소스들을 찾아내서 막는다. 따라서 한 소스당 전송하는 패킷이 적은 공격이더라도 공격을 정확히 탐지할 수 있다. 또한 피해자에게 패킷을 전송하는 소스들을 공격자로 식별하여 그들의 IP 주소만 리스트에 저장하여 필터링하기 때문에, 공격자들을 정확히 탐지하여 사전에 차단할 수 있다.

[0025] 기존 기법에서는, 제한된 메모리로 들어온 모든 패킷에 대해 n 개 이상의 소스로부터 패킷을 받는 DDoS 공격의 피해자가 존재하는지 확인하기 위해 확률적 자료구조인 임의의 크기(예컨대, d×w의 크기, d와 w는 임의의 자연수로 예시적인 값은 3과 1024임)의 카운트민 스케치(Count-Min Sketch)의 변형 구조를 활용한다. 카운트민 스케치의 한 칸을 비트스트링(bitstring) 구조로 변형하여 소스 IP 주소를 해시(hash)한 인덱스의 위치에 해당하는 레지스터를 1로 업데이트한다(비특허문헌 2 참조). 이렇게 스케치의 한 칸 안에 있는 1의 개수를 카운트하여 해당 데스티네이션에 몇 개의 서로 다른 소스 IP들이 패킷을 보냈는지 알 수 있다. 하지만, 이 구조는 외부 컨트롤러의 도움을 받아 매 라운드(round)마다 레지스터를 초기화해야 한다는 한계가 존재한다.

[0026] 따라서, 제안하는 기법에서는 카운트민 스케치의 한 칸을 비트스트링(bitstring)이 아닌 스트링(string) 구조로 활용하여 들어온 패킷이 몇 번째 라운드에 해당하는지를 기록한다. 즉, 소스 IP 주소를 해시한 인덱스의 위치에 현재 라운드를 기록할 수 있다. 이에 따르면, 동일한 라운드의 개수를 카운트함으로써, 임의의 라운드(예컨대, 해당 라운드) 내에 하나의 데스티네이션에 패킷을 보낸 서로 다른 소스가 몇 개인지 카운트할 수 있어, 매 라운드마다 컨트롤러의 도움으로 초기화를 하지 않아도 DDoS 공격의 피해자를 알아낼 수 있다. 여기서, 카운트민 스케치를 이루는 하나의 칸은 하나의 데스티네이션에 대응한다. 구체적인 예로써, 도 2에서 제29라운드에 해당 데스티네이션으로 패킷을 송신한 소스는 3 개임을 알 수 있다.

[0027] **동작 과정 2 : DDoS 공격의 피해자에게 패킷을 전송하는 공격자를 찾아내는 과정**

[0028] 도 3은 DDoS 공격의 피해자에게 패킷을 전송하는 공격자를 찾아내는 과정을 나타낸다. 앞서 스위치로 들어온 패킷의 데스티네이션 IP 주소가 DDoS 공격의 피해자인지 확인하는 과정을 거쳐, 만약 피해자가 아니라면 스위치의 해시 테이블 구조에 해당 소스 IP 주소를 업데이트한다. 적은 메모리만을 사용하여 DDoS 공격의 피해자에 패킷을 전송하는 공격자 IP 주소의 목록을 얻기 위해, 서로 다른 m(m는 임의의 자연수) 개의 해시 테이블을 이용(또는 유지)할 수 있다.

[0029] 해시 테이블들은 각각 서로 다른 해시 함수를 이용하여 패킷의 데스티네이션 IP 주소의 인덱스를 계산한다. 만약 테이블의 해당 인덱스의 칸이 비어 있다면, 들어온 패킷의 소스 IP 주소를 그 위치에 저장하고, 카운트를 1로 업데이트한다. 만약 테이블의 해당 인덱스의 칸에 같은 소스 IP 주소가 이미 저장되어 있다면 카운트를 1 증가시킨다.

[0030] 만약 테이블의 해당 인덱스의 칸이 비어 있지 않고 저장된 소스 IP 주소가 들어온 패킷의 소스 IP 주소와 다르다면, 첫 테이블과 그 이후의 m-1 개의 테이블에 대해 서로 다른 동작을 취해준다. 첫 테이블에 한해서는 해당 칸이 이미 차 있더라도 새로 들어오는 패킷에 대해 우선순위를 부여하여 새로운 소스 IP 주소를 저장하고 카운트를 1로 업데이트한다. 그리고, 첫 테이블에 원래 있던 소스 IP 주소와 카운트 값은 메타데이터로 복사되어 두 번째 테이블로 전달된다. 첫 테이블 이후의 m-1 개의 테이블들에서는 패킷의 데스티네이션 IP 주소의 인덱스에 해당하는 칸이 이미 차 있다면(즉, 소스 IP 주소와 카운트 값이 이미 기재되어 있다면), 해당 테이블에 저장된 카운트 값과 다른 테이블에서 밀려난 소스 IP 주소의 카운트 값을 비교하여 큰 값이 저장되고 작은 값은 다음 테이블로 밀려나게 된다. 총 m 개의 테이블을 지나면서 카운트가 작은 소스 IP 주소들은 상대적으로 카운트가 큰 소스 IP 주소들에 의해 밀려나서 저장되지 않는다.

[0031] 앞서 스위치로 들어온 패킷의 데스티네이션 IP 주소가 DDoS 공격의 피해자라면, m 개의 테이블에서 패킷의 데스티네이션 IP 주소가 해시된 인덱스의 칸에 저장된 소스 IP 주소들을 찾아내 공격자로 식별하여 필터링 리스트에 추가할 수 있다.

[0032] **동작 과정 3 : DDoS 공격자 소스들의 리스트를 다른 스위치들에게 전달하는 과정**

[0033] 도 4는 본 발명의 네트워크 환경을 나타낸 시스템 모델이다. 시스템은 복수의 소스 장치들(컴퓨팅 장치를 의미할 수 있음)과 복수의 데스티네이션 장치(컴퓨팅 장치를 의미할 수 있음)를 포함할 수 있고, 각 장치들은 적어도 하나의 스위치(프로그래밍 가능한 스위치를 의미할 수 있음)를 통해 통신할 수 있다. 즉, 프로그래밍 가능한 스위치들이 네트워크 상에 배포되어 있다고 가정한다.

[0034] DDoS 공격의 피해자(즉, 데스티네이션 장치)에 직접 연결된 스위치에서 그 피해자에게 패킷을 전송하는 top-k 소스들을 공격자로 식별하고 해당 소스들의 리스트를 생성할 수 있다. 이를 통해 공격을 피해자에 가까운 곳에서 탐지하여 공격과 공격자 탐지의 정확도를 높일 수 있다. 그리고 나서 해당 리스트를 알림 패킷의 헤더에 저장하여 다른 스위치들에게도 전달할 수 있다. 스위치들은 해당 소스로부터 오는 패킷에 대한 필터링을 통해 DDoS 공격을 사전 차단할 수 있다. 위 과정을반복하여 DDoS 공격의 피해자로부터 먼 곳에 있는 스위치들에게도 점진적으로 필터링 리스트를 전달한다. 이를 통해 공격자로부터 가까운 곳에서 공격을 막을 수 있어, 공격 트래픽이 피해자 근처까지 도달하여 네트워크 자원이 소진되는 것을 방지할 수 있다.

[0035] 아래 표 1은 실제 DDoS 공격 데이터를 활용하여 시뮬레이션을 한 결과를 나타낸다. 본 발명은 비교기법보다 정밀도와 재현율이 높아 정밀도와 재현율의 조화 평균인 F1 스코어(Score) 또한 높다. 비교 기법인 Bungee는 미리 정해진 임계값 이하로 패킷을 전송하는 공격자를 정확히 감지하지 못하기 때문에 거짓 음성의 비율이 높다. 반면에, 본 발명은 먼저 피해자를 파악한 후 피해자에게 패킷을 전송한 top-k 소스들을 공격자로 식별하기 때문에 정해진 값 이하로 패킷을 전송하는 공격자라도 정확하게 탐지할 수 있다.

[0036] [표 1]

[0037]

Method	Precision	Recall	F1 Score
BUNGEE	0.99	0.69	0.82
Proposed Method	1	0.97	0.98

[0038] 도 5는 본 발명의 일 실시예에 따른, 프로그래밍 가능한 데이터 평면을 활용한 DDoS 탐지 방법을 설명하기 위한 흐름도이다.

[0039] 도 5를 참조하면, DDoS 탐지 방법은 적어도 프로세서(Processor)나 컨트롤러(Controller) 및/또는 메모리(memory)를 포함하는 컴퓨팅 장치에 의해 수행될 수 있다. 즉, DDoS 탐지 방법을 이루는 각 단계들 중 적어도 일부는 컴퓨팅 장치에 포함되는 프로세서나 컨트롤러의 동작으로 이해될 수도 있고, 이에 따라 컴퓨팅 장치는 DDoS 탐지 장치로 명명될 수도 있다. 구체적인 예로, 컴퓨팅 장치는 프로그래밍 가능한 스위치로 구현될 수 있다. 또한, 제안하는 DDoS 탐지 방법은 데스티네이션 장치에 최근접한(또는 직접 연결된) 스위치에서 동작하는 방법일 수 있기 때문에, 컴퓨팅 장치는 데스티네이션 장치와 직접 연결되어 있는(또는 데스티네이션 장치로 다른 스위치를 경유하지 않고 직접 패킷을 전송하는) 프로그래밍 가능한 스위치를 의미할 수 있다. 이하에서, DDoS 탐지 방법을 설명함에 있어, 앞선 기재와 중복되는 내용에 관하여는 그 구체적인 기재를 생략하기로 한다.

[0040] 우선, 임의의 패킷이 수신된다(S110). 패킷은 임의의 소스 장치로부터 직접 또는 적어도 하나의 스위치를 경유하여 수신될 수 있다.

[0041] 다음으로, 필터링 대상 공격자 여부가 확인(판단 또는 결정의 의미로 이해될 수도 있음)된다(S120). 필터링 대상 공격자 여부는 미리 저장되어 있는 공격자 리스트(의심자 리스트(Suspect)로 명명될 수도 있음)에 포함된 소스 IP 주소와 수신된 패킷의 소스 IP 주소를 비교함으로써 수행될 수 있다. 수신된 패킷을 송신한 소스 IP 주소가 공격자 리스트에 포함되는 경우, 수신된 패킷은 필터링 대상 공격자로부터 송신된 것으로 판단될 수 있다.

[0042] 일 실시예에 따르면, 수신된 패킷이 필터링 대상 공격자로부터 송신된 것으로 판단되는 경우, 확률 기반의 필터링 동작이 수행될 수 있다. 즉, a(a는 0 보다는 크고 100 보다는 작거나 같은 임의의 실수로써, 예시적인 값은 30임)%의 확률로 수신된 패킷은 필터링되거나 필터링되지 않을 수 있다. 즉, 수신된 패킷은 드랍(Drop)되거나 드랍되지 않고 다음 동작이 수행될 수도 있다.

[0043] 다음으로, DDoS 공격의 피해자 여부가 확인(판단 또는 결정의 의미로 이해될 수도 있음)된다(S130). S130 단계는 수신된 패킷이 필터링 대상 공격자가 송신한 패킷이 아니라고 판단되는 경우 또는 수신된 패킷이 필터링 대상 공격자가 송신한 패킷이라고 판단되었지만 필터링되지 않은 경우에 수행될 수 있다.

[0044] 피해자 여부는 수신된 패킷의 데스티네이션 IP 주소에 기초하여 판단될 수 있다. 예컨대, (미리 정해진 시간 주기를 갖는) 현재 라운드에서 수신된 패킷의 데스티네이션 IP 주소로 패킷을 송신한 소스 IP 주소가 n 개 이상인 경우, 해당 데스티네이션 IP 주소(또는 해당 네스티네이션 장치)가 DDoS 공격의 피해자로 결정될 수 있다. 이때, 현재 수신된 패킷의 소스 IP 주소를 포함하여 n 개 이상인 경우 또는 현재 수신된 패킷의 소스 IP 주소를 포함하지 않은 상태에서 n 개 이상인 경우를 의미할 수 있다.

[0045] 실시예에 따라, 데스티네이션 IP 주소로 패킷을 송신한 소스 IP 주소의 개수는 상술한 카운트-민 스케치의 데이터 구조를 이용하여 산출될 수 있다. 이를 위해, 하나의 데스티네이션 IP 주소에 대응하는 카운트민 스케치의 한 칸에, 수신된 패킷의 소스 IP 주소를 해시한 값에 해당하는 인덱스 위치에 현재 라운드 정보를 기재할 수 있다. 이에 따라, 현재 라운드를 카운트함으로써 해당 데스티네이션 IP 주소로 패킷을 송신한 소스 IP 주소의 개수를 산출할 수 있다. 이때, 현재 수신된 패킷의 소스 IP 주소는 DDoS 공격 피해자 탐지 과정에서 이용될 수도 있고 이용되지 않을 수도 있다.

[0046] 수신된 패킷의 데스티네이션 IP 주소가 DDoS 공격의 피해자로 결정된 경우, 수신된 패킷은 드랍될 수 있다. 또한, 수신된 패킷의 데스티네이션 IP 주소로 패킷을 송신한 상위 k(top-k, k는 임의의 자연수) 개의 소스 IP 주소를 포함하는 메시지(또는 (알람) 패킷)이 생성되고, 생성된 패킷은 인접한 스위치로 전송될 수 있다. 예시적으로, top-k 개의 소스 IP 주소에 대한 리스트가 헤더(header)에 저장된 패킷이 전송될 수 있다.

[0047] S130 단계에서, 수신된 패킷의 데스티네이션 IP 주소가 DDoS 공격의 피해자가 아닌 것으로 판단된 경우, 테이블이 업데이트될 수 있다(S140). 테이블은 앞서 설명한 m 개의 해시 테이블을 의미할 수 있다. 테이블 업데이트 동작에 관한 구체적인 설명은 생략하기로 한다.

[0048] 이상에서 설명된 장치는 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 집합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성 요소는, 예를 들어, 프로세서, 콘트롤러, ALU(Arithmetic Logic Unit), 디지털 신호 프로세서(Digital Signal Processor), 마이크로컴퓨터, FPA(Field Programmable array), PLU(Programmable Logic Unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(Operation System, OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사

용되는 것으로 설명된 경우도 있지만, 해당 기술 분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(Processing Element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(Parallel Processor)와 같은, 다른 처리 구성(Processing Configuration)도 가능하다.

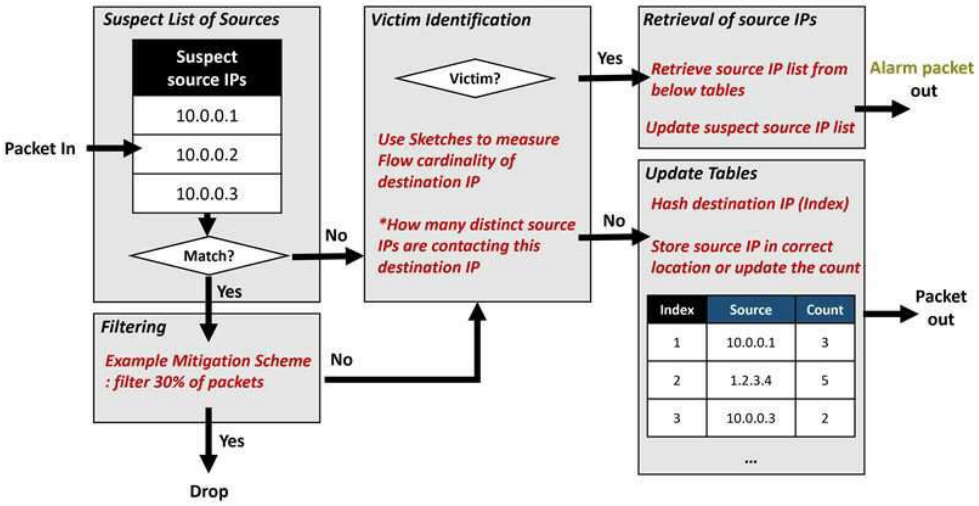
[0049] 소프트웨어는 컴퓨터 프로그램(Computer Program), 코드(Code), 명령(Instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(Collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성 요소(Component), 물리적 장치, 가상 장치(Virtual Equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(Signal Wave)에 영구적으로, 또는 일시적으로 구체화(Embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0050] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM, DVD와 같은 광기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-optical Media), 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

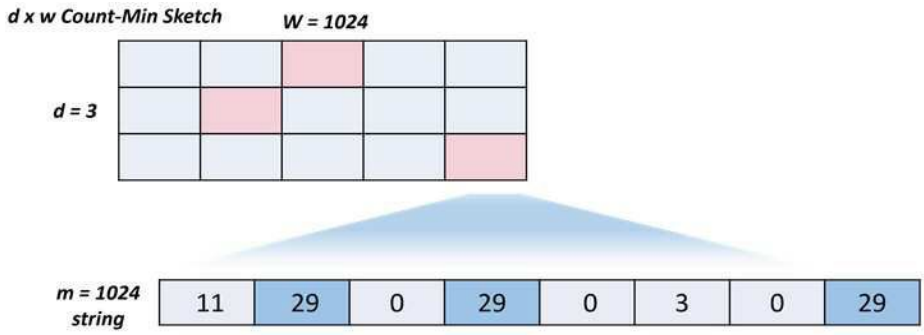
[0051] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성 요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성 요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

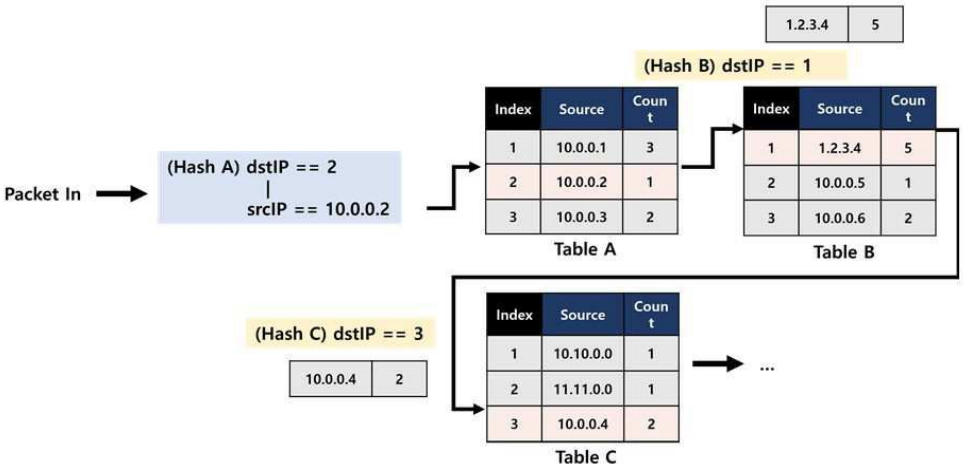
도면1



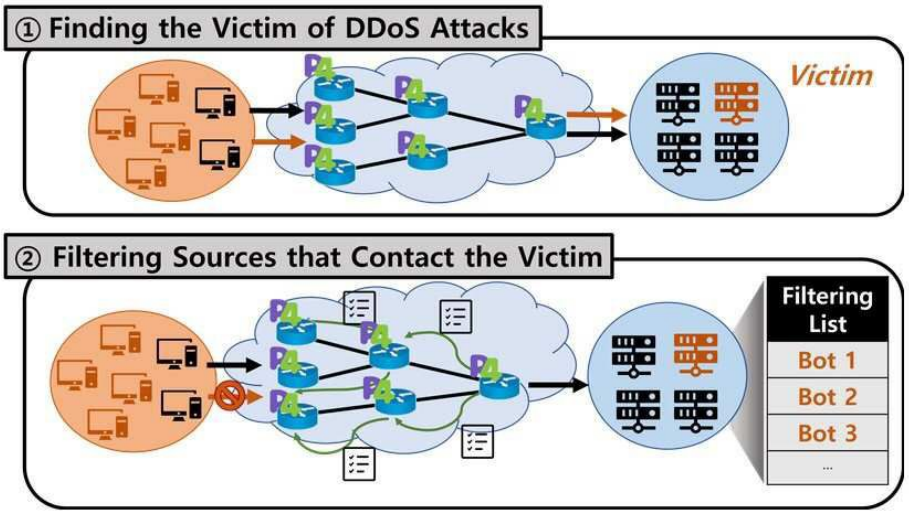
도면2


d x w Count-Min Sketch
W = 1024
d = 3
m = 1024
string
11
29
0
29
0
3
0
29

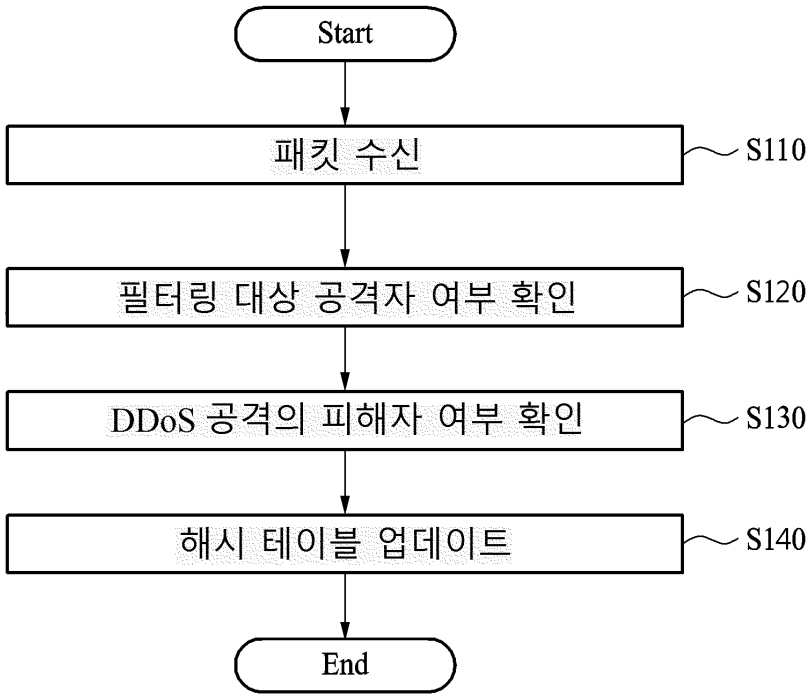
도면3


1.2.3.4
5
(Hash B) dstIP == 1
Packet In
(Hash A) dstIP == 2
|
srcIP == 10.0.0.2
Index
Source
Count
1
10.0.0.1
3
2
10.0.0.2
1
3
10.0.0.3
2
Table A
Index
Source
Count
1
1.2.3.4
5
2
10.0.0.5
1
3
10.0.0.6
2
Table B
(Hash C) dstIP == 3
10.0.0.4
2
Index
Source
Count
1
10.10.0.0
1
2
11.11.0.0
1
3
10.0.0.4
2
Table C
...

도면4


① Finding the Victim of DDoS Attacks
Victim
② Filtering Sources that Contact the Victim
Filtering List
Bot 1
Bot 2
Bot 3
...

도면5


Start
패킷 수신
S110
필터링 대상 공격자 여부 확인
S120
DDoS 공격의 피해자 여부 확인
S130
해시 테이블 업데이트
S140
End