



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0079175
(43) 공개일자 2017년07월10일

(51) 국제특허분류(Int. Cl.)

H04L 29/06 (2006.01)

(52) CPC특허분류

H04L 63/1416 (2013.01)

H04L 63/0428 (2013.01)

(21) 출원번호 10-2015-0189452

(22) 출원일자 2015년12월30일

심사청구일자 2015년12월30일

(71) 출원인

이화여자대학교 산학협력단

서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)

(72) 발명자

도인실

인천광역시 연수구 센트럴로 194, 201동 2705호(송도동, 더샵 센트럴파크2)

니샤트 모우라

대한민국 서울특별시 서대문구 봉원사길 35

채기준

서울특별시 강남구 강남대로136길 34

(74) 대리인

특허법인(유한)아이시스

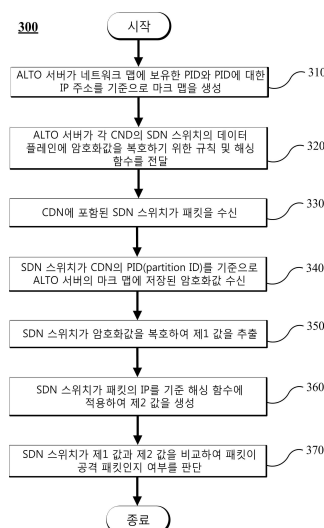
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 콘텐츠 전달 네트워크에서 네트워크 공격을 검출하는 방법 및 네트워크 공격을 검출하는 CDN 네트워크 시스템

(57) 요약

콘텐츠 전달 네트워크에서 네트워크 공격을 검출하는 방법은 CDN에 포함된 SDN(software defined network) 스위치가 패킷을 수신하는 단계, 상기 SDN 스위치가 상기 CDN의 PID(partition ID)를 기준으로 ALTO 서버로부터 상기 PID에 대응하는 암호화값을 수신하는 단계, 상기 SDN 스위치가 상기 암호화값을 복호하여 제1 값을 추출하는 단계, 상기 SDN 스위치가 상기 패킷의 IP를 기준 해싱 함수에 적용하여 제2 값을 생성하는 단계 및 상기 SDN 스위치가 상기 제1 값과 상기 제2 값을 비교하여 상기 패킷이 공격 패킷인지 또는 정상 패킷인지 여부를 판단하는 단계를 포함한다.

대표도 - 도4



(52) CPC특허분류

H04L 63/1458 (2013.01)

H04L 63/1483 (2013.01)

H04L 2463/142 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 2013R1A1A2011788

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 기초연구사업(학술진흥)

연구과제명 CDNi 환경에서의 안전하고 효율적인 서비스보안 기법

기 여 율 1/1

주관기관 이화여자대학교 산학협력단

연구기간 2015.06.01 ~ 2016.05.31

명세서

청구범위

청구항 1

CDN에 포함된 SDN(software defined network) 스위치가 패킷을 수신하는 단계;

상기 SDN 스위치가 상기 CDN의 PID(partition ID)를 기준으로 ALTO 서버로부터 상기 PID에 대응하는 암호화값을 수신하는 단계;

상기 SDN 스위치가 상기 암호화값을 복호하여 제1 값을 추출하는 단계;

상기 SDN 스위치가 상기 패킷의 IP를 기준 해싱 함수에 적용하여 제2 값을 생성하는 단계; 및

상기 SDN 스위치가 상기 제1 값과 상기 제2 값을 비교하여 상기 패킷이 공격 패킷인지 또는 정상 패킷인지 여부를 판단하는 단계를 포함하는 콘텐츠 전달 네트워크에서 네트워크 공격을 검출하는 방법.

청구항 2

제1항에 있어서,

상기 ALTO 서버가 상기 SDN 스위치의 데이터 플레인에 상기 암호화값을 복호하기 위한 규칙 및 상기 해싱 함수를 전달하는 단계를 더 포함하는 콘텐츠 전달 네트워크에서 네트워크 공격을 검출하는 방법.

청구항 3

제1항에 있어서,

상기 암호화값은 상기 ALTO 서버가 상기 ALTO 서버가 보유하는 상기 PID와 상기 PID에 대한 IP 주소를 상기 기준 해싱 함수를 이용하여 해싱하고, 상기 해싱한 값을 공유키 K로 암호화하고, 상기 공유키로 암호화한 값을 상기 PID로 XOR 연산하여 생성되는 콘텐츠 전달 네트워크에서 네트워크 공격을 검출하는 방법.

청구항 4

제3항에 있어서,

상기 제1 값을 추출하는 단계에서

상기 SDN 스위치는 상기 암호화값을 상기 공유키로 복호하고, 상기 복호한 값을 상기 PID로 XOR 연산하여 상기 제1 값을 추출하는 콘텐츠 전달 네트워크에서 네트워크 공격을 검출하는 방법.

청구항 5

제1항에 있어서,

상기 SDN 스위치는 상기 제1 값과 상기 제2 값이 동일하지 않으면 상기 패킷을 공격 패킷이라고 판단하고, 상기 패킷을 역추적하여 상기 패킷을 전달한 공격자에 대한 정보를 추출하는 단계를 더 포함하는 콘텐츠 전달 네트워크에서 네트워크 공격을 검출하는 방법.

청구항 6

제5항에 있어서,

상기 SDN 스위치는 상기 공격자에 대한 정보를 다른 CDN의 SDN 스위치에 전달하는 단계를 더 포함하는 콘텐츠 전달 네트워크에서 네트워크 공격을 검출하는 방법.

청구항 7

자신이 보유한 PID와 상기 PID에 대한 IP 주소를 기준으로 암호화값을 생성하고 저장하는 ALTO 서버; 및

사용자 단말이 요청한 패킷을 수신하고, 상기 ALTO 서버로부터 정보를 수신하는 라우터 및 상기 암호화값을 복

호하여 제1 값을 추출하고 상기 패킷의 IP를 기준 해싱 함수에 적용하여 제2 값을 생성하고, 상기 제1 값과 상기 제2 값을 비교하여 상기 패킷이 공격 패킷인지 여부 판단하는 SDN 스위치를 포함하는 제1 CDN 노드를 포함하는 네트워크 공격을 검출하는 CDNi 네트워크 시스템.

청구항 8

제7항에 있어서,

상기 ALTO 서버는 상기 SDN 스위치의 데이터 플레인에 상기 암호화값을 복호하기 위한 규칙 및 상기 해싱 함수를 전달하는 네트워크 공격을 검출하는 CDNi 네트워크 시스템.

청구항 9

제7항에 있어서,

상기 ALTO 서버는 자신이 보유한 상기 PID와 상기 PID에 대한 IP 주소를 상기 기준 해싱 함수를 이용하여 해싱하고, 상기 해싱한 값을 공유키 K로 암호화하고, 상기 공유키로 암호화한 값을 상기 PID로 XOR 연산하여 상기 암호화값을 생성하는 네트워크 공격을 검출하는 CDNi 네트워크 시스템.

청구항 10

제9항에 있어서,

상기 SDN 스위치는 상기 암호화값을 상기 공유키로 복호하고, 상기 복호한 값을 상기 PID로 XOR 연산하여 상기 제1 값을 추출하는 네트워크 공격을 검출하는 CDNi 네트워크 시스템.

청구항 11

제7항에 있어서,

상기 SDN 스위치는 상기 제1 값과 상기 제2 값이 동일하지 않으면 상기 패킷을 공격 패킷이라고 판단하고, 상기 패킷을 역추적하여 상기 패킷을 전달한 공격자에 대한 정보를 추출하는 네트워크 공격을 검출하는 CDNi 네트워크 시스템.

청구항 12

제11항에 있어서,

상기 SDN 스위치는 상기 공격자에 대한 정보를 제2 CDN 노드의 SDN 스위치에 전달하는 네트워크 공격을 검출하는 CDNi 네트워크 시스템.

발명의 설명

기술 분야

[0001] 이하 설명하는 기술은 CDN에서 네트워크 공격을 검출하는 기법에 관한 것이다.

배경 기술

[0002] CDN(Content Delivery Network)은 사용자(end user)에게 콘텐츠를 효과적으로 전달하기 위해 사용된다. 콘텐츠 제공자는 CDN을 이용하여 사용자에게 콘텐츠를 제공한다. 복수의 CDN을 효과적으로 사용하기 위하여 CDNi(CDN Interconnection)가 등장하기도 하였다.

[0003] 한편 최근 네트워크 분야에 SDN(Software Defined Network)이라는 개념이 상용화되었다. SDN은 물리적인 하드웨어 장치 대신에 프로그래밍이 가능한 소프트웨어로 네트워크 제어를 수행할 수 있다. SDN은 기본적으로 애플리케이션 플레인(application plane), 제어 플레인(control plane) 및 데이터 플레인(data plane)을 갖는다.

[0004] CDN은 ALTO(Application Layer Traffic Optimization) 서버를 포함하기도 한다. ALTO 서버는 네트워크에 대한 토폴로지(topology) 및 라우팅 비용(routing cost)에 대한 정보를 관리한다. ALTO 서버는 SDN 컨트롤러와 연동하여 일정한 랑데뷰(rendezvous) 서비스를 제공할 수 있다.

선행기술문헌

비특허문헌

- [0005] (비특허문헌 0001) H. Xie, T. Tsou, D. Lopez, H. Yin, V. Gurbani, "Alto and Software Defined Networking (SDN)," IETF 84, Vancouver
- (비특허문헌 0002) M. Nagaratna, Dr. V. K. Prasad, S. T. Kumar, "Detecting and Preventing IP-spoofed DDoS Attacks by Encrypted Marking based Detection And Filtering (EMDAF)," International Conference on Advances in Recent Technologies in Communication and Computing, pp. 753-755, 2009

발명의 내용

해결하려는 과제

- [0006] 네트워크가 ALTO 서버와 같은 집중적 제어 구성을 갖게되면 DDoS 공격과 같은 네트워크 공격에 취약할 수 있다.
- [0007] 이하 설명하는 기술은 CDN에서 스푸핑 IP를 검출하는 기법을 제공하고자 한다. 이하 설명하는 기술은 SDN에 기반한 스푸핑 IP를 검출하는 CDN을 제공하고자 한다.

과제의 해결 수단

- [0008] 콘텐츠 전달 네트워크에서 네트워크 공격을 검출하는 방법은 CDN에 포함된 SDN(software defined network) 스위치가 패킷을 수신하는 단계, 상기 SDN 스위치가 상기 CDN의 PID(partition ID)를 기준으로 ALTO 서버로부터 상기 PID에 대응하는 암호화값을 수신하는 단계, 상기 SDN 스위치가 상기 암호화값을 복호하여 제1 값을 추출하는 단계, 상기 SDN 스위치가 상기 패킷의 IP를 기준 해싱 함수에 적용하여 제2 값을 생성하는 단계 및 상기 SDN 스위치가 상기 제1 값과 상기 제2 값을 비교하여 상기 패킷이 공격 패킷인지 또는 정상 패킷인지 여부를 판단하는 단계를 포함한다.
- [0009] 네트워크 공격을 검출하는 CDN 네트워크 시스템은 자신이 보유한 PID와 상기 PID에 대한 IP 주소를 기준으로 암호화값을 생성하고 저장하는 ALTO 서버 및 사용자 단말이 요청한 패킷을 수신하고, 상기 ALTO 서버로부터 정보를 수신하는 라우터 및 상기 암호화값을 복호하여 제1 값을 추출하고 상기 패킷의 IP를 기준 해싱 함수에 적용하여 제2 값을 생성하고, 상기 제1 값과 상기 제2 값을 비교하여 상기 패킷이 공격 패킷인지 여부 판단하는 SDN 스위치를 포함하는 제1 CDN 노드를 포함한다.

발명의 효과

- [0010] 이하 설명하는 기술은 ALTO 서버가 관리하는 추가적인 마크 맵을 이용하여, CDN의 SDN 스위치가 쉽게 패킷의 IP 스푸핑(spoofed IP) 여부를 판단할 수 있다.

도면의 간단한 설명

- [0011] 도 1은 CDN 네트워크 구조를 도시한 예이다.
- 도 2는 CDN 네트워크에 대한 구조를 도시한 다른 예이다.
- 도 3은 ALTO 서버가 관리하는 맵에 대한 예이다.
- 도 4는 콘텐츠 전달 네트워크에서 네트워크 공격을 검출하는 방법에 대한 순서도의 예이다.

발명을 실시하기 위한 구체적인 내용

- [0012] 이하 설명하는 기술은 다양한 변형을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 이하 설명하는 기술을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 이하 설명하는 기술의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.
- [0013] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 해당 구성요소들은 상기 용어

들에 의해 한정되지는 않으며, 단지 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 이하 설명하는 기술의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0014] 본 명세서에서 사용되는 용어에서 단수의 표현은 문맥상 명백하게 다르게 해석되지 않는 한 복수의 표현을 포함하는 것으로 이해되어야 하고, "포함한다" 등의 용어는 실시된 특징, 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 의미하는 것이지, 하나 또는 그 이상의 다른 특징들이나 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 배제하지 않는 것으로 이해되어야 한다.

[0015] 도면에 대한 상세한 설명을 하기에 앞서, 본 명세서에서의 구성부들에 대한 구분은 각 구성부가 담당하는 주기능 별로 구분한 것에 불과함을 명확히 하고자 한다. 즉, 이하에서 설명할 2개 이상의 구성부가 하나의 구성부로 합쳐지거나 또는 하나의 구성부가 보다 세분화된 기능별로 2개 이상으로 분화되어 구비될 수도 있다. 그리고 이하에서 설명할 구성부 각각은 자신이 담당하는 주기능 이외에도 다른 구성부가 담당하는 기능 중 일부 또는 전부의 기능을 추가적으로 수행할 수도 있으며, 구성부 각각이 담당하는 주기능 중 일부 기능이 다른 구성부에 의해 전담되어 수행될 수도 있음은 물론이다.

[0016] 또, 방법 또는 동작 방법을 수행함에 있어서, 상기 방법을 이루는 각 과정들은 문맥상 명백하게 특정 순서를 기재하지 않은 이상 명기된 순서와 다르게 일어날 수 있다. 즉, 각 과정들은 명기된 순서와 동일하게 일어날 수도 있고 실질적으로 동시에 수행될 수도 있으며 반대의 순서대로 수행될 수도 있다.

[0018] 도 1은 CDNi 네트워크(100) 구조를 도시한 예이다. CDNi 네트워크는 복수의 개별 CDN을 포함한다. 도 1은 CDNi 네트워크(100)가 CDN1(120A) 및 CDN2(120B)를 갖는 예를 도시하였다. CDNi 네트워크(100)는 복수의 개별 CDN을 연결하여 기본적으로 사용자(end user)에게 가장 가까운 CDN으로부터 콘텐츠를 제공한다. 도 1에서 사용자 단말(50)이 콘텐츠를 서비스 서버(80)에 요청한다. 서비스 서버(80)는 콘텐츠를 사용자에게 제공하는 서비스를 수행하는 주체이다. 서비스 서버(80)는 콘텐츠 요청을 수신하면 이를 CDNi 네트워크(100)에 전달한다.

[0019] 도 1에서는 서비스 서버(80)가 CDN1(120A)에 콘텐츠 요청을 전달하는 예를 도시하였다. 서비스 서버(80)는 콘텐츠 서비스 사업자에 속하고, CDN(120A 및 120B)은 통신 사업자에 속할 수 있다. 각 CDN(120A 및 120B)은 일반적으로 일정한 지역에 서비스를 제공하는 네트워크 망에 해당한다. 경우에 따라 CDN(120A 및 120B)은 서로 다른 통신 사업자의 망일 수도 있다. 서비스 서버(80)는 자신과 가까운 또는 서비스 서버(80)를 직접 관리하는 CDN1(120A)에 콘텐츠 요청을 전달할 수 있다.

[0020] CDN1(120A)는 콘텐츠 요청을 수신하면 사용자 단말(50)에 콘텐츠를 제공할 CDN 및 에지 서버를 선택한다. CDN1(120A)는 일정한 알고리즘을 통해 콘텐츠를 제공할 CDN 및 에지 서버를 선택할 수 있다. 도 1에서는 ALTO 서버(110)를 도시하였다. 후술하겠지만 ALTO 서버(110)는 CDN1(120A)이 사용자 단말(50)에 콘텐츠를 제공할 CDN 및 에지 서버를 선택하는데 필요한 일정한 정보를 제공할 수 있다. 도 1은 CDN1(120A)에 3개의 에지 서버(125A, 126A 및 127A)를 도시하였다. CDN1(120A)는 CDN2(120B)의 에지 서버(127B)를 서비스 제공 지점으로 선택했다고 가정한다. CDN1(120A)은 CDN2(120B)에 연결된 또는 CDN2(120B)에 가장 가까운 에지 서버(127A)를 통해 CDN2에 콘텐츠 요청을 전달한다. 도 1에서 CDN2(120B)는 3개의 에지 서버(125B, 126B 및 127B)를 갖는 것으로 도시하였다. CDN2(120B)는 사용자 단말(50)에 가장 가까운 에지 서버(127B)를 통해 콘텐츠를 제공하게 된다. 보다 구체적으로는 사용자 단말(50)의 콘텐츠 제공 요청이 CDN2(120B)의 에지 서버(127B)에 전달(redirect)되고, 이후 CDN2(120B)의 에지 서버(127B)를 통해 요청한 콘텐츠가 제공된다.

[0022] ALTO 서버를 사용하는 CDN과 같이 집중적(centralized) 제어장치를 갖는 네트워크는 외부 공격에 취약할 수 있다. ALTO 서버가 해킹 공격의 집중적 타깃이 되기 때문이다. 이하 설명하는 기술은 CDN(CDNi) 및 SDN으로 구성되는 집중적 시스템에서 네트워크 공격을 막기 위한 기법에 관한 것이다. 예컨대, IP 스푸핑(spoofing)과 같은 공격에 대비하기 위한 것이다.

[0023] 이하 설명하는 기술은 ALTO 서버와 SDN 컨트롤러를 사용하여 spoofed IP 공격을 방어할 수 있는 네트워크에 관한 것이다. ALTO 서버와 SDN 컨트롤러는 스푸핑 IP를 검출하기 위한 도구(tool)로 사용하는 것이다. 이하 SDN 컨트롤러는 스위치 역할을 한다는 의미에서 SDN 스위치라고 명명한다. SDN은 전송한 바와 같이 데이터 플레인,

제어 플레인 및 애플리케이션 플레인을 갖는다. SDN에 대한 자세한 구조(architecture)를 설명하지 않는다.

[0024] 도 2는 CDNi 네트워크(200)에 대한 구조를 도시한 다른 예이다. 도 2의 CDNi 네트워크는 개별 CDN, SDN 스위치 및 ALTO 서버를 포함한다. 도 2에서 CDNi 네트워크(200)는 두 개의 CDN(220 및 230)을 구비한 예를 도시하였다. 도 2에서 CDNi 네트워크(200)는 ALTO 서버(210)를 구비한다. CDN1(220)은 ALTO 클라이언트(221), SDN 스위치(222) 및 에지 서버(225)를 포함한다. CDN2(230)은 ALTO 클라이언트(231), SDN 스위치(232) 및 에지 서버(235)를 포함한다. ALTO 클라이언트(221, 231)는 ALTO 서버(210)와 정보를 주고 받는 객체를 말한다. ALTO 클라이언트(221, 231)는 또한 사용자 단말로부터 일정한 콘텐츠 요청을 수신하기도 한다. ALTO 클라이언트를 다른 말로 요청 라우터(request router)라고도 한다. 한편 도 3에서는 콘텐츠를 요청하는 사용자 단말(240)을 도시하였다. CDN1(220)의 PID는 "PID1"이고, CDN2(230)의 PID는 "PID2"이고, 사용자 단말(또는 사용자 단말이 속한 네트워크)의 PID는 "PID3"이다.

[0025] ALTO 서버(210)는 IP 망에 배치되고, IP 망의 프로토콜에 참여(passive listening)하여 네트워크의 정보를 자동으로 읽고 관리한다. CDN(220, 230)의 ALTO 클라이언트(221, 231)는 각 ALTO 서버(210)로부터 IP 망에 대한 정보를 수신하여 콘텐츠를 전달한 에지 서버를 결정한다. 도 2에서는 SDN 기반의 SDN 스위치(222, 232)가 존재한다.

[0026] ALTO 서버(210)는 PID(Partition ID)라는 식별자를 갖는 복수의 영역으로 분할되는 맵을 관리한다. CDN에 도착한 패킷은 SDN 스위치를 통해 CDN에 전달된다. 따라서 SDN 스위치가 공격 패킷과 정상 패킷 구별하는 기능을 수행할 수 있다. 공격 패킷을 검출하는 방법을 간략하게 설명하면 ALTO 서버(210)는 추가적인 맵으로 마크 맵(mark map)을 생성하여 PID 및 IP 주소를 저장한다. SDN 스위치(222, 232)는 ALTO 서버가 제공하는 마크 맵(map)에서 암호화된 정보를 수신하고, 일정한 규칙에 따라 복호한다. 그리고 SDN 스위치(222, 232)는 자신이 수신한 패킷에 포함된 IP 주소와 상기 ALTO 서버(210)로부터 수신한 암호화 정보를 비교하여 공격 패킷인지 여부를 판단한다. SDN 스위치(222, 232)는 마킹 맵을 기반으로 스푸핑 IP를 검출한다. 이후 CDN에서 공격 패킷을 검출하는 과정을 자세하게 설명한다. 이하 설명의 편의를 위해 SDN 스위치(232)가 공격 패킷을 검출한다고 가정한다.

[0028] ALTO 서버의 맵 마킹(marking)

[0029] ALTO 서버(210)는 기본적으로 네트워크 맵(network map)과 비용 맵(cost map)을 포함한다. 네트워크 맵은 PID에 대한 IP 주소를 맵핑한 데이터이다. 비용 맵은 라우팅 비용에 대한 정보를 나타내는 데이터이다. 도 2의 ALTO 서버(210)는 마크 맵(mark map)이라는 맵을 추가로 생성하고 관리한다. 마크 맵은 암호화된 PID 및 IP 주소를 포함한다. 마크 맵은 특정 PID 및 IP 주소를 갖는 패킷이 전달되면 해당 패킷이 정상 패킷인지 또는 스푸핑 패킷인지를 판단하는데 사용된다. 스푸핑 패킷은 스푸핑 IP(spoofed IP)를 갖는 패킷을 의미한다. ALTO 서버(210)는 자신이 보유한 정보를 이용하여 마크 맵을 아래의 표 1과 같은 알고리즘을 사용하여 생성할 수 있다.

[0030] 아래 표 1은 패킷에 대해 PID 및 IP 주소를 포함하는 암호화 마크를 생성하는 알고리즘에 관한 것이다.

표 1

[0031]

<pre><Marking algorithm> K is a 16 bit shared key For a packet P with ip address IP_p PID_x be the partition ID whrere x is 1,2,3,... and so on. Initialize PID_x.ip = 0 E(ip) = K XOR H(IP_p) If PID_x.ip = 0 PID_x.ip = E(ip) XOR PID_x Else pass</pre>

[0032] 상기 알고리즘(Marking algorithm)에 대한 내용을 설명한다. ALTO 서버(210)는 자신의 네트워크 맵에 보유하고 있는 정보를 이용하여 마크 맵을 생성한다. 상기 알고리즘은 ALTO 서버(210)가 IP 주소와 해당 IP 주소가 속한

PID에 대한 정보를 네트워크 맵에서 추출한 것을 전제로 한다.

- [0033] 패킷 P는 IP_p 라는 IP 주소를 갖는다고 가정한다. PIDx는 영역 x에 대한 PID이다. PIDx.ip는 0의 값을 갖도록 초기화한다. 후술하겠지만 PIDx.ip는 암호화된 마크를 저장하는 변수이다.
- [0034] ALTO 서버(210)는 IP 주소(IP_p)를 일정한 해싱 기법(예컨대, MD5)으로 해싱하고, 16 비트 길이를 갖는 임의의 키(K)와 XOR 연산을 한다. 결국 이 과정은 패킷의 IP 주소를 일정하게 암호화하는 것이다. 여기서 K는 해싱 기법에서 산출되는 결과의 길이에 대응하는 길이를 갖게될 것이다. 상기 알고리즘에서는 설명의 편의를 위해 16 비트의 길이를 갖는 것으로 가정하였다. 암호화된 IP 주소는 변수 E(ip)에 저장된다.
- [0035] PID.xip가 '0'인 경우 PIDx.ip는 E(ip)와 PIDx를 XOR 연산으로 암호화한 값을 저장한다. 변수 PID.xip는 암호화된 마크에 해당하며 암호화된 패킷의 IP 주소 및 해당 네트워크의 PID를 암호화한 값을 저장한다. PID.xip가 '0'이 아닌 값을 갖고 있다면 이미 특정 값을 저장하고 있는 것이므로 별도의 암호화값을 저장하지 않는다.
- [0036] 상기 알고리즘을 통해 ALTO 서버(210)는 수신한 패킷에 대한 암호화된 마크를 생성하고, 해당 정보를 마크 맵에 저장하고 관리한다. 도 3은 ALTO 서버(210)가 관리하는 맵에 대한 예이다. ALTO 서버(210)는 기본적으로 네트워크 맵(network map)과 비용 맵(cost map)을 관리한다. 네트워크 맵은 PID와 해당 PID에 대한 IP 주소를 포함한다. 도 3에서는 네트워크 맵은 PID1, PID2 및 PID3에 대한 정보를 저장하고 있다. 비용 맵은 라우팅 비용에 관한 정보를 저장한다. 도 3에서 비용 맵은 PID1이 PID3에 콘텐츠를 전달하는 비용은 '5'이고, PID2가 PID3에 콘텐츠를 전달하는 비용은 '3'이라는 정보를 저장한다.
- [0037] 나아가 ALTO 서버(210)는 전술한 마크 맵(mark map)을 추가로 보유하고 관리한다. 마크 맵은 전술한 바와 같이 각 PID에 대해 PID와 PID에 대한 IP 주소를 일정하게 가공하여 암호화한 값을 저장한다.
- [0039] **SDN 스위치의 공격 패킷 처리**
- [0040] 특정 CDN의 SDN 스위치(232)는 일정한 콘텐츠 요청 메시지(패킷)을 수신하게 된다. SDN 스위치(232)는 ALTO 서버(210)가 관리하는 마크 맵으로부터 일정한 정보를 수신하여 공격 패킷 여부를 판단한다. SDN 스위치(232)는 자신이 속한 CDN의 PID를 기준으로 ALTO 서버(210)로부터 PIDx.ip를 수신한다. SDN 스위치(232)는 수신한 PIDx.ip와 네트워크의 PID를 XOR 연산하여 E(ip)를 추출한다. SDN 스위치(232)는 E(ip)를 공유키 K로 복호하여 $H(IP_p)$ 에 해당하는 제1 값을 추출한다. 공유키 K는 사전에 ALTO 서버(210)와 SDN 스위치(232)에 공유되었다고 가정한다.
- [0041] SDN 스위치(232)는 수신한 패킷에 포함된 IP 주소를 상기 알고리즘과 동일한 해싱 함수(H)로 해싱하여 제2 값을 생성한다. 따라서 SDN 스위치(232)는 해싱 함수에 대한 정보도 사전에 알고 있어야 한다.
- [0042] SDN 스위치(232)는 제1 값과 제2 값이 일치하는지 확인한다. 이를 통해 SDN 스위치(232)는 패킷에서 요청된 IP 주소와 PID 조합이 실제 존재하는 결정할 수 있다. 즉, SDN 스위치(232)는 제1 값과 제2 값이 일치한다면 정상 패킷이라고 판단하고, 제1 값과 제2 값이 일치하지 않는다면 스푸핑 패킷이라고 판단할 수 있다.
- [0043] SDN은 일정한 규칙을 스위치에 전달하는 애플리케이션을 구동한다. SDN 스위치(232)는 애플리케이션이 전달하는 규칙을 이용하여 수신한 패킷에 대한 처리를 수행할 수 있다. 아래 표 2는 SDN 스위치(232)가 수신한 패킷을 처리하는 동작에 대한 수도 코드의 예이다.

표 2

[0044]

```

Application for spoofed IP

if
    (p.IP!= spoofed)
    {
        check other conditions;
    }
Else if
    (p.IP= spoofed)
    {
        spoof ip actions
        {
            trace packet;
            drop packet;
            broadcast msg;
        }
    }

```

[0045] SDN 스위치(232)는 수신한 패킷의 IP가 스푸핑 IP가 아닌 경우, 다음 동작을 수행한다. SDN 스위치(232)는 수신한 패킷의 IP가 스푸핑 IP인 경우, 패킷을 역 추적하고, 해당 패킷을 블록(drop)하고, 역 추적 결과에 따른 공격자 정보를 포함하는 메시지를 다른 CDN에 있는 SDN에 브로드캐스팅한다.

[0047] 전술한 ALTO 서버(210)의 동작과 SDN 스위치(232)의 동작을 정리하면 도 4와 같다. 도 4는 콘텐츠 전달 네트워크에서 네트워크 공격을 검출하는 방법(300)에 대한 순서도의 예이다.

[0048] ALTO 서버는 네트워크 맵에 보유한 PID와 PID에 대한 IP 주소를 기준으로 전술한 바와 같이 마크 맵을 생성하고 관리한다(310). ALTO 서버는 자신이 마크 맵을 생성한 일정한 암호화 규칙 및 해싱 함수를 각 CDN에 속한 SDN 스위치의 데이터 플레인에 전달한다(320).

[0049] 이후 CDN에 속한 SDN 스위치가 패킷을 수신한다(330). 이때 SDN 스위치가 수신하는 패킷은 최초 사용자 단말로부터 전달되는 콘텐츠 요청일 수 있다. 또는 SDN 스위치가 수신하는 패킷은 하나의 CDN에서 다른 CDN으로 전달하는 콘텐츠 요청일 수도 있다. 또는 SDN 스위치가 수신하는 패킷은 CDNi 네트워크에서 사용자 단말에 대한 콘텐츠 서비스를 제공할 CDN과 에지 서버를 선택한 후 사용자 단말로부터 선택한 CDN에 전달되는 패킷일 수도 있다.

[0050] SDN 스위치는 자신이 속한 CDN의 PID를 기준으로 ALTO 서버로부터 해당 PID에 대응하는 암호화값(PIDx.ip)를 수신한다(340). 이때 경우에 따라서는 SDN 스위치가 자신이 속한 CDN의 PID가 아니라, 수신한 패킷의 IP에 해당하는 PID를 기준으로 암호화값을 수신할 수도 있을 것이다.

[0051] SDN 스위치는 암호화값을 전술한 바와 같이 일정하게 복호하여 제1 값을 추출한다(350). SDN 스위치는 또 자신이 수신한 패킷에 포함된 IP를 사전에 ALTO 서버로부터 전달받은 해싱 함수에 적용하여 제2 값을 생성한다(360). SDN 스위치는 제1 값과 제2 값을 비교하여 현재 수신한 패킷이 공격 패킷인지 여부를 판단한다(370). SDN 스위치는 제1 값과 제2 값이 동일하지 않은 경우 현재 수신한 패킷을 공격 패킷이라고 판단할 수 있다. SDN 스위치는 공격 패킷은 무시하고, 다음 절차를 진행하지 않는다.

[0052] 도 4에서는 도시하지 않았지만, 이후 SDN 스위치는 공격 패킷을 전달한 공격자(단말)을 역 추적할 수 있다. SDN 스위치는 공격자에 대한 정보(IP 주소 등)를 다른 CDN에 있는 SDN 스위치에 전달할 수 있다. 즉 CDNi에 있는 모든 SDN 스위치에 공격자 정보를 공유하는 것이다.

[0054] 본 실시예 및 본 명세서에 첨부된 도면은 전술한 기술에 포함되는 기술적 사상의 일부를 명확하게 나타내고 있는 것에 불과하며, 전술한 기술의 명세서 및 도면에 포함된 기술적 사상의 범위 내에서 당업자가 용이하게 유추

할 수 있는 변형 예와 구체적인 실시예는 모두 전술한 기술의 권리범위에 포함되는 것이 자명하다고 할 것이다.

부호의 설명

[0055]

50 : 사용자 단말

80 : 서비스 서버

100 : CDNi 네트워크

110 : ALTO 서버

120A, 120B : CDN

125A, 126A, 127A, 125B, 126B, 127B : 에지 서버

200 : CDNi 네트워크

210 : ALTO 서버

220, 230 : CDN

221, 231 : ALTO 클라이언트

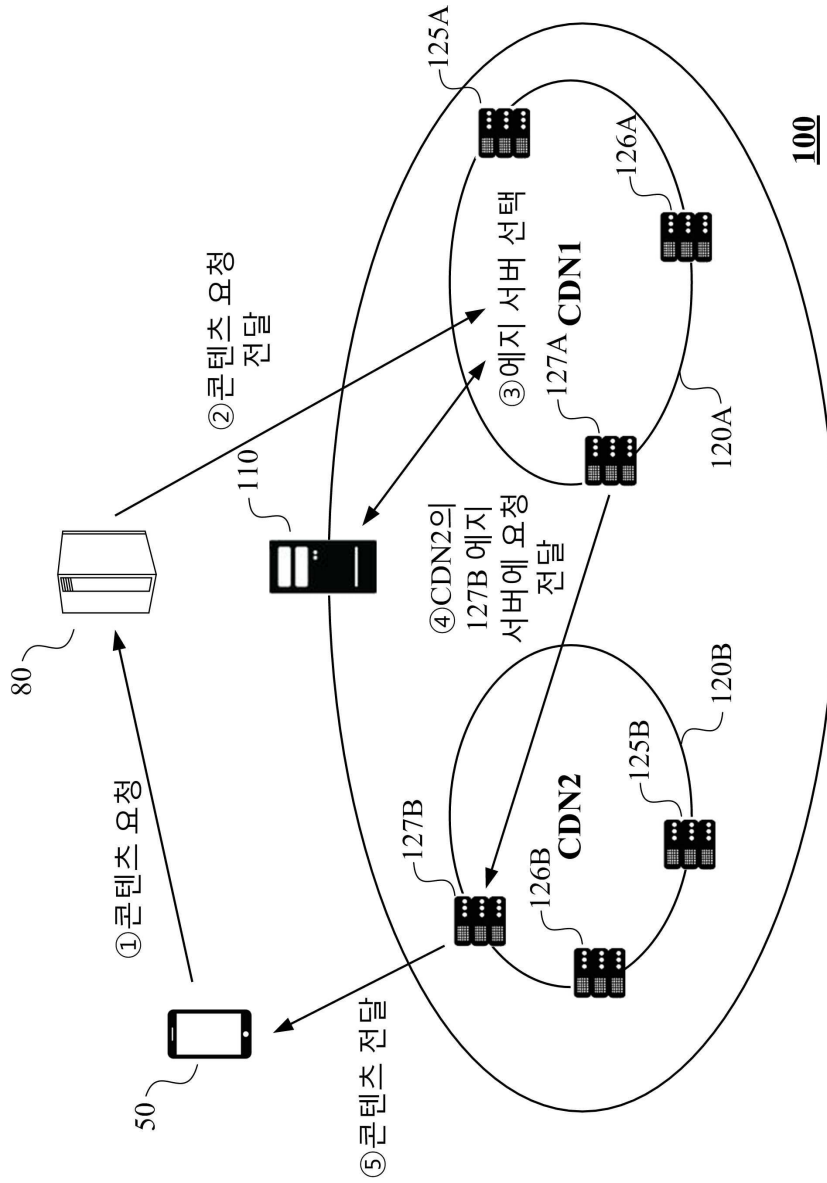
222, 232 : SDN 스위치

225, 235 : 에지 서버

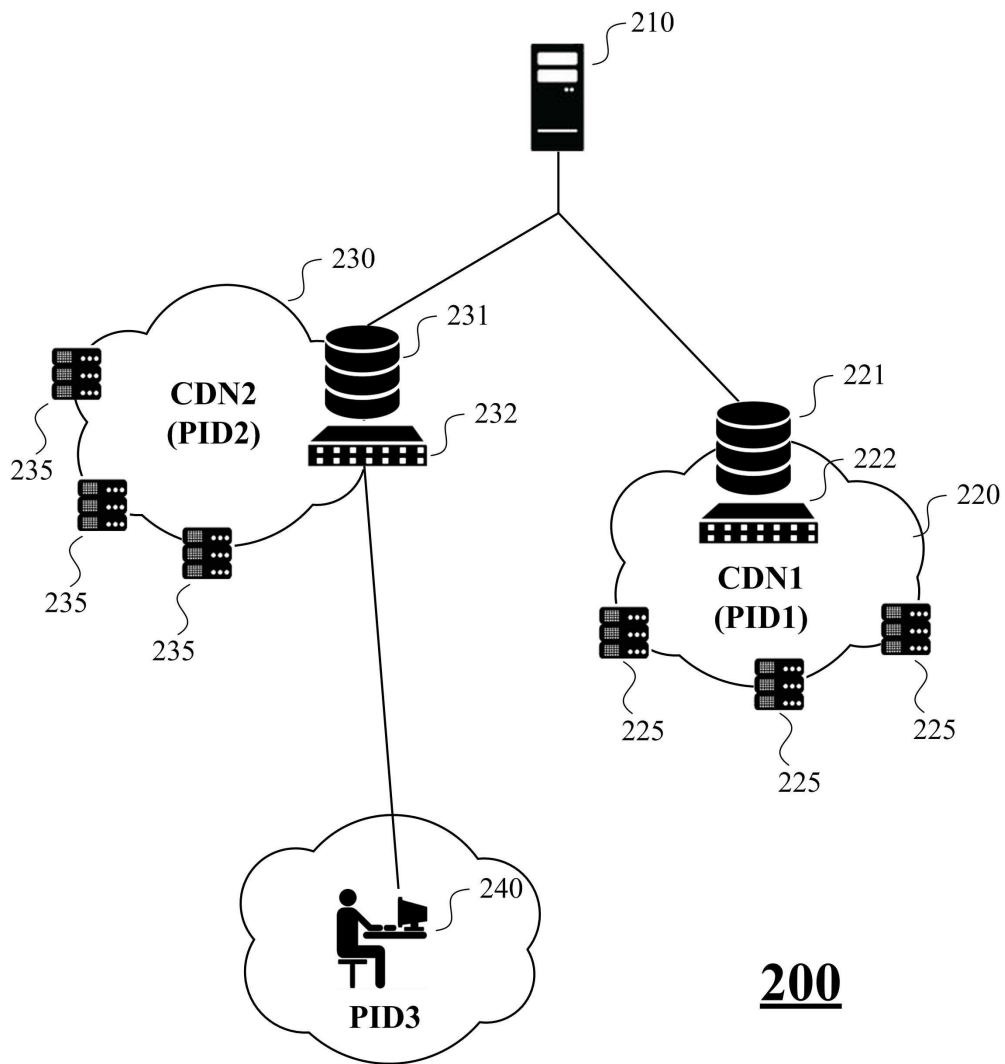
240 : 사용자 단말

도면

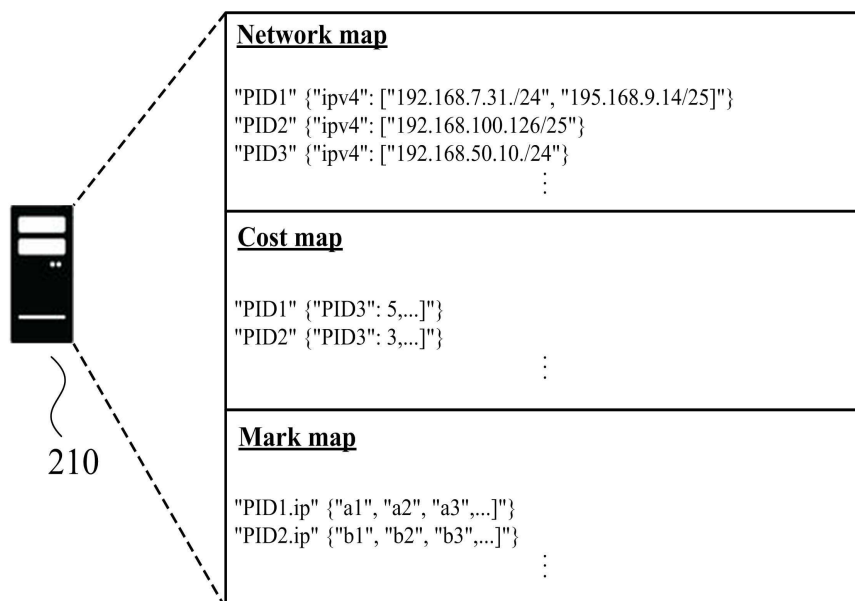
도면1



도면2



도면3



도면4

