



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년05월30일
(11) 등록번호 10-1741357
(24) 등록일자 2017년05월23일

(51) 국제특허분류(Int. Cl.)

H04L 12/801 (2013.01) H04L 12/813 (2013.01)
H04L 12/823 (2013.01) H04L 12/851 (2013.01)
H04L 12/891 (2013.01) H04L 12/931 (2013.01)
H04L 29/06 (2006.01)

(52) CPC특허분류

H04L 47/29 (2013.01)
H04L 47/20 (2013.01)

(21) 출원번호 10-2016-0016971

(22) 출원일자 2016년02월15일

심사청구일자 2016년02월15일

(56) 선행기술조사문헌

KR1020110061217 A*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

이화여자대학교 산학협력단

서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)

(72) 발명자

니샤트 모우라

대한민국 서울특별시 서대문구 봉원사길 35

도인실

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

채기준

서울특별시 강남구 강남대로136길 34, 402호

(74) 대리인

특허법인(유한)아이시스

전체 청구항 수 : 총 6 항

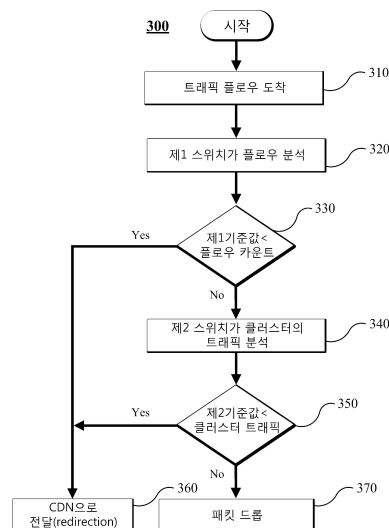
심사관 : 김성태

(54) 발명의 명칭 SDN에서 비정상 트래픽을 검출하는 방법 및 비정상 트래픽을 검출하는 장치

(57) 요약

SDN에서 비정상 트래픽을 검출하는 방법은 SDN 컨트롤러에 연결된 제1 스위치가 트래픽 플로우를 수신하는 단계, 상기 제1 스위치가 상기 플로우의 크기가 제1 기준값 이상인 경우 상기 플로우를 제2 스위치에 전달하는 단계, 상기 제2 스위치가 상기 플로우에 포함된 패킷을 사전에 정의된 클러스터로 분류하는 단계 및 상기 제2 스위치가 상기 분류한 클러스터의 트래픽이 제2 기준값 이상인 경우 상기 패킷을 드롭하는 단계를 포함한다.

대표도 - 도4



(52) CPC특허분류

H04L 47/2441 (2013.01)

H04L 47/32 (2013.01)

H04L 47/41 (2013.01)

H04L 49/70 (2013.01)

H04L 63/1408 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 2013R1A1A2011788

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 기초연구사업(학술진흥)

연구과제명 CDNi 환경에서의 안전하고 효율적인 서비스 보안 기법

기 여 율 1/1

주관기관 이화여자대학교 산학협력단

연구기간 2015.06.01 ~ 2016.05.31

공지예외적용 : 있음

명세서

청구범위

청구항 1

SDN 컨트롤러에 연결된 제1 스위치가 트래픽 플로우를 수신하는 단계;

상기 제1 스위치가 상기 플로우의 크기가 제1 기준값 이상인 경우 상기 플로우를 제2 스위치에 전달하는 단계;

상기 제2 스위치가 상기 플로우에 포함된 패킷을 분석하여 상기 플로우를 사전에 정의된 클러스터로 분류하는 단계; 및

상기 제2 스위치가 상기 분류한 클러스터에 속한 플로우의 트래픽이 제2 기준값 이상인 경우 상기 패킷을 드롭하는 단계를 포함하는 SDN에서 비정상 트래픽을 검출하는 방법.

청구항 2

제1항에 있어서,

상기 제1 스위치는

상기 플로우를 상기 SDN 컨트롤러에 전달하고, 상기 SDN 컨트롤러는 상기 플로우에 포함된 패킷 내의 정보를 기준으로 플로우 테이블에 적용할 규칙을 전달받는 단계를 더 포함하는 SDN에서 비정상 트래픽을 검출하는 방법.

청구항 3

제2항에 있어서,

상기 제1 스위치는 상기 플로우 테이블을 사용하여 상기 플로우를 분석하고, 상기 플로우의 카운트 값이 상기 제1 기준값 이상인 경우 상기 플로우를 상기 제2 스위치에 전달하는 SDN에서 비정상 트래픽을 검출하는 방법.

청구항 4

제1항에 있어서,

상기 제2 스위치는 소스 IP 주소, 목적지 IP 주소, 프로토콜, 소스 포트 및 목적지 포트 중 적어도 하나를 사용하여 상기 패킷을 상기 클러스터로 분류하는 SDN에서 비정상 트래픽을 검출하는 방법.

청구항 5

플로우의 종류에 따른 규칙을 저장하는 SDN 컨트롤러;

트래픽 플로우를 수신하면 수신한 상기 플로우를 상기 SDN에 전달하고, 상기 SDN으로부터 상기 플로우에 대응하는 규칙을 수신하고, 상기 규칙을 사용한 플로우 테이블을 사용하여 상기 플로우를 분석하는 제1 스위치; 및

상기 제1 스위치가 전달하는 상기 플로우에 포함된 패킷의 정보를 기준으로 상기 플로우를 사전에 설정된 클러스터로 분류하고, 상기 분류한 클러스터에 속한 플로우의 트래픽을 분석하는 제2 스위치를 포함하되,

상기 제1 스위치는 상기 플로우의 카운트값이 제1 기준값 이상인 경우에 상기 플로우를 상기 제2 스위치에 전달하고, 상기 제2 스위치는 상기 클러스터에 속한 플로우의 트래픽이 제2 기준값 이상인 경우 상기 플로우를 드롭하는 비정상 트래픽을 검출하는 장치.

청구항 6

제5항에 있어서,

상기 제2 스위치는 소스 IP 주소, 목적지 IP 주소, 프로토콜, 소스 포트 및 목적지 포트 중 적어도 하나를 사용하여 상기 패킷을 상기 클러스터로 분류하는 비정상 트래픽을 검출하는 장치.

발명의 설명

기술 분야

[0001] 이하 설명하는 기술은 SDN에 기반한 네트워크에서 데이터 플레인의 비정상 패킷을 검출하는 기법에 관한 것이다.

배경 기술

[0002] 최근 네트워크 분야에 SDN(Software Defined Network)이라는 개념이 상용화되었다. SDN은 물리적인 하드웨어 장치 대신에 프로그래밍이 가능한 소프트웨어로 네트워크 제어를 수행할 수 있다.

선행기술문헌

비특허문헌

[0003] (비특허문헌 0001) C. Estan, S. Savage, G. Varghese, "Automatically Inferring Patterns of Resource Consumption in Network Traffic", ACM SIGCOMM Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications.

발명의 내용

해결하려는 과제

[0004] SDN에 기반한 네트워크는 중앙 집중적 제어 방식을 갖게되고, 따라서 네트워크 공격에 취약하다고 볼 수 있다. 이하 설명하는 기술은 SDN에서 비정상 트래픽(공격성 트래픽)을 검출하는 기법을 제공하고자 한다.

과제의 해결 수단

[0005] SDN에서 비정상 트래픽을 검출하는 방법은 SDN 컨트롤러에 연결된 제1 스위치가 트래픽 플로우를 수신하는 단계, 상기 제1 스위치가 상기 플로우의 크기가 제1 기준값 이상인 경우 상기 플로우를 제2 스위치에 전달하는 단계, 상기 제2 스위치가 상기 플로우에 포함된 패킷을 사전에 정의된 클러스터로 분류하는 단계 및 상기 제2 스위치가 상기 분류한 클러스터의 트래픽이 제2 기준값 이상인 경우 상기 패킷을 드롭하는 단계를 포함한다.

[0006] 비정상 트래픽을 검출하는 장치는 플로우의 종류에 따른 규칙을 저장하는 SDN 컨트롤러, 트래픽 플로우를 수신하면 수신한 상기 플로우를 상기 SDN에 전달하고, 상기 SDN으로부터 상기 플로우에 대응하는 규칙을 수신하고, 상기 규칙을 사용한 플로우 테이블을 사용하여 상기 플로우를 분석하는 제1 스위치 및 상기 제1 스위치가 전달하는 상기 플로우에 포함된 패킷을 사전에 설정된 클러스터로 분류하고, 상기 분류한 클러스터의 트래픽을 분석하는 제2 스위치를 포함한다. 상기 제1 스위치는 상기 플로우의 카운트값이 제1 기준값 이상인 경우에 상기 플로우를 상기 제2 스위치에 전달하고, 상기 제2 스위치는 상기 클러스터의 트래픽이 제2 기준값 이상인 경우 상기 플로우를 드롭한다.

발명의 효과

[0007] 이하 설명하는 기술은 SDN에서 플로우 분석 기법과 클러스터 분석 기법을 조합하여 오버헤드가 적으면서도 비정상 트래픽을 효과적으로 검출하게 한다.

도면의 간단한 설명

[0008] 도 1은 CDN 네트워크 구조를 도시한 예이다.

도 2는 SDN 아키텍처를 도시한 예이다.

도 3은 SDN에 기반한 비정상 트래픽을 탐지하는 장치에 대한 구성을 도시한 블록도의 예이다.

도 4는 SDN에서 비정상 트래픽을 검출하는 방법에 대한 순서도의 예이다.

발명을 실시하기 위한 구체적인 내용

- [0009] 이하 설명하는 기술은 다양한 변경을 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.
- [0010] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 해당 구성요소들은 상기 용어들에 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/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.
- [0011] 본 명세서에서 사용되는 용어에서 단수의 표현은 문맥상 명백하게 다르게 해석되지 않는 한 복수의 표현을 포함하는 것으로 이해되어야 하고, "포함한다" 등의 용어는 설시된 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.
- [0012] 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.
- [0013] 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.
- [0015] 이하 설명하는 기술은 SDN에서 비정상 트래픽을 검출하는 기법에 관한 것이다. SDN은 다양한 네트워크에서 사용될 수 있다. 대표적으로 CDN(Content Delivery Network)에서 사용될 수 있다. SDN에 기반한 네트워크의 예로 CDN에 대해 설명한다.
- [0016] 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.
- [0017] 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.
- [0018] 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. 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.

- [0019] ALTO 서버를 사용하는 CDNi 또는 SDN에 기반한 개별 CDN은 소프트웨어로 네트워크를 제어하는 제어 장치가 외부 공격에 취약할 수 있다.
- [0021] 이제 SDN에 대해 간략하게 설명한다. 과거에는 대부분의 통신이 클라이언트와 서버 간에서 일어났지만 현재의 애플리케이션은 데이터를 사용자에게 제공하기 전에 다양한 애플리케이션 서버와 DB들을 액세스하면서 대량의 east-west, sever-to-server 트래픽을 만들어 내고 있다. 한편 가상화 기술은 네트워크에 연결된 서버의 수를 급증시켰고, 호스트의 물리적 위치에 대한 가정을 근본적으로 바꾸어 놓았다. 가상화 기술이 등장하기 이전에는 애플리케이션이 하나의 서버에서 실행되었고 클라이언트와 트래픽을 주고 받았지만, 오늘의 애플리케이션은 다수의 가상 머신(VM)에 분산되어 있으며 VM은 서버의 부하를 재조정하고 최적화하기 위해 위치를 이동하는 수준에 이르고 있다. 이는 플로우의 end-points가 시간에 따라 급격히 변하게 만드는 요인이 된다. 이를 해결하기 위한 새로운 개념으로 SDN이 등장하였다.
- [0022] SDN은 제어평면과 전달평면을 분리하는 개념이다. 일반적으로 SDN과 OpenFlow가 밀접한 관련이 있다. 다만 SDN은 훨씬 더 큰 개념으로 네트워크 구조 혹은 새로운 패러다임이며, OpenFlow는 SDN을 위한 인터페이스 기술의 하나이다. 네트워크의 지능은 SDN 컨트롤러에 집중화되어 네트워크 전체를 관리하며 네트워크는 하나의 논리적인 스위치로 간주된다. 관리자(또는 NMS)는 표준화된 인터페이스를 통해 전체 네트워크를 벤더에 의존하지 않고 제어할 수 있고, 네트워크 설계와 운용을 보다 단순화할 수 있게 된다. 또한 SDN은 네트워크 장치를 단순화할 수도 있다. 즉, 장치를 설계할 때에 수백~수천 개의 프로토콜(RFC) 처리를 고려하지 않아도 되며, 단순히 SDN 컨트롤러로부터의 명령을 받아 데이터를 처리하는 기능만 갖추도록 하면 되기 때문이다.
- [0023] 도 2는 SDN 아키텍처를 도시한 예이다. SDN(Software Defined Network)은 애플리케이션 플레인(application plane), 제어 플레인(control plane) 및 데이터 플레인(data plane)을 갖는다. 데이터 플레인 Openflow에 기반한 스위치 및 라우터를 포함한다. 제어 플레인 Openflow와 데이터 플레인 OS(Operating System)와 통신하면서 네트워크를 관리한다. SDN은 네트워크 제어를 위한 알고리즘을 소프트웨어적으로 구현하기 때문에 네트워크 제어를 비교적 손쉽게 할 수 있다. 따라서 CDN 등에 SDN을 이용하면 콘텐츠 전달 서비스를 보다 효율적으로 제공할 수 있다. 다만 SDN에 기반한 네트워크는 중앙 집중적 제어 방식을 갖게 되고, 따라서 네트워크 공격에 취약하다고 볼 수 있다.
- [0024] OpenFlow는 SDN 컨트롤러와 네트워크 장치간의 인터페이스 규격으로 사용되고 있는 기술이다. OpenFlow의 가장 큰 특징은 제어 평면과 데이터 평면을 분리하고, 이들을 연결하는 표준 인터페이스로 OpenFlow 프로토콜을 사용한다는 것이다. OpenFlow 프로토콜을 사용하면, 제어 및 데이터 평면을 하드웨어가 아닌 소프트웨어로도 구현할 수 있으며, 이 소프트웨어를 범용 서버에 설치하여 신속하게 새로운 기능을 구현할 수 있다. OpenFlow는 프로토콜 계층 1~4까지의 헤더 정보를 하나로 조합하여 패킷(프레임)의 동작을 지정할 수 있다. 제어 평면의 프로그램을 수정하면 계층 4까지의 범위에서 사용자가 자유롭게 새로운 프로토콜을 만들 수 있고, 특정 서비스나 애플리케이션에 최적화된 네트워크를 사용자가 구현할 수도 있다. 즉, OpenFlow는 패킷을 제어하는 기능과 전달하는 기능을 분리하고 프로그래밍을 통해 네트워크를 제어하는 기술이라고 정의할 수 있다.
- [0026] 이하 설명하는 기술은 SDN에 기반한 네트워크에서 데이터 플레인의 비정상 패킷을 검출하는 기법이다. 이하 설명하는 기술은 OpenFlow 프로토콜을 사용하는 스위치를 이용하여 비정상 패킷을 검출한다. 이하 설명하는 기술은 트래픽의 플로우(flow) 분석과 클러스터(cluster) 분석을 이용하여 비정상 패킷을 검출한다. 간략하게 각각의 기법에 대해 설명한다.
- [0027] 패킷을 전송하는 소스로부터 특정 목적지 사이의 트래픽은 패킷 플로우(flow) 또는 플로우(flow)에 해당한다. 플로우에 대한 정보는 트래픽의 비정상 여부를 탐지하는데 중요하다. 패킷 자체를 분석하는 것보다 플로우를 분석하는 것이 보다 효율적이다. 다만 플로우 분석은 연산에 많은 오버헤드(overhead)가 발생할 수 있다. 네트워크 장비 차원에서 이를 지원하기 위하여 Cisco NetFlow와 InMon의 sFlow와 같은 Flow 포맷을 정의하여 네트워크 장비에서 Flow 정보를 제공하고 있다. 또한 IETF IPFIX Working Group에서는 다양한 분석 응용 분야들에 통합적으로 적용할 수 있는 표준화된 플로우 포맷을 제정하고 있다.
- [0028] 한편 패킷을 이용한 트래픽 분석은 트래픽 카테고리 결정과 같은 분석에 취약한 면이 있다. 트래픽 카테고리는 프로토콜이나 포트(port)에 기반하여 분석할 수 있다. 이러한 단점을 극복하고자 복수의 헤더 필드를 분석하여 트래픽을 분석하는 클러스터(cluster) 기법이 등장하였다.
- [0029] 클러스터 기법은 소스 IP 주소(Source IP), 목적지 IP 주소(Destination IP), 프로토콜(Protocol), 소스 포트(source port) 및 목적지 포트(destination port) 중 적어도 하나를 기준으로 패킷을 분석한다. (i) 예컨대, 클러스터를

"SrcIP=10.8.200.3, DstIP=*, Proto=TCP, SrcPort=80, DstPort=*"로 정의할 수 있다. 이는 주소가 10.8.200.3 인 서버로부터 전달되는 웹 트래픽을 의미한다. 여기서 SrcIP는 소스 IP 주소, DstIP는 목적지 IP 주소, Proto는 프로토콜, SrcPort는 소스 포트, DstPort는 목적지 포트를 나타낸다. *는 해당 항목을 한정하지 않고 모든 경우를 포함한다는 의미이다. 예컨대, "DstIP=*"는 모든 목적지 IP 주소를 포함한다는 의미이다. 다른 말로 하면 목적지 IP 주소는 클러스터를 정의하는데 사용하지 않는다는 의미이기도 하다. (ii) "SrcIP=*, DstIP=172.27.0.0/16, Proto=TCP, SrcPort=low, DstPort=high"라고 정의된 클러스터는 로우(low) 포트를 출발하여 특정 프리픽스(prefix)를 갖는 목적지의 하이(high) 포트로 진입하는 TCP 트래픽을 의미한다. 로우 포트는 포트 번호가 1024 미만인 경우라고 정의할 수 있다. 하이 포트는 포트 번호가 1024 이상인 경우라고 정의할 수 있다. (iii) "SrcIP=*, DstIP=*, Proto=ICMP, SrcPort=*, DstPort=*"라고 정의된 클러스터는 모든 ICMP(Internet Control Message Protocol) 트래픽을 의미한다. 따라서 클러스터 기법은 특정 애플리케이션의 트래픽, 특정 클라이언트에 전달되는 트래픽, 특정한 웹 서버의 트래픽 등과 같이 트래픽을 구분하여 분석할 수 있다. 클러스터 기법은 경우에 따라 완벽하게 특정 클러스터를 형성(분류)하지 못할 수도 있다. 또한 클러스터 기법은 사전에 정의된 클러스터를 벗어나는 경우 분석을 할 수 없다는 단점이 있다.

[0031] 이하 설명하는 기술은 플로우 분석과 클러스터 분석 기법을 조합하여 네트워크의 비정상 상태(공격 상태 등)를 판단하고자 한다. 이하 설명하는 기술은 SDN에서 플로우 분석과 클러스터 분석을 모두 운용할 수 있는 시스템 구조를 제시한다. 예컨대, SDN에 기반한 CDN에서 이하 설명하는 기술을 사용하여 비정상 트래픽을 구분할 수 있다.

[0033] 도 3은 SDN에 기반한 비정상 트래픽을 탐지하는 장치(200)에 대한 구성을 도시한 블록도의 예이다. 도 3은 설명의 편의를 위한 CDN을 기준으로 도시하였다. 비정상 트래픽을 탐지하는 장치(200)는 CDN에서 외부 트래픽을 최초로 수신하는 라우터 또는 게이트웨이와 같은 장치일 수 있다. 비정상 트래픽을 탐지하는 장치(200)는 크게 SDN 컨트롤러(210), 제1 스위치(220) 및 제2 스위치(230)를 포함한다.

[0034] SDN은 비정상 트래픽을 판단하기 위해 두 개의 스위치를 사용한다. 두 개의 스위치 중 하나의 제1 스위치(220)가 먼저 플로우 분석을 수행하고, 이후 나머지 하나의 제2 스위치(230)가 클러스터 분석을 수행한다. 제1 스위치(210) 및 제2 스위치(230)는 모두 Openflow를 이용하여 동작할 수 있다.

[0035] SDN 컨트롤러(210)는 스위치에 명령을 하고, 스위치는 그 명령에 따라 패킷을 목적지로 전송하거나 수정, 폐기하는 등의 처리를 한다. 일반적으로 L2 스위치에 OpenFlow 프로토콜을 펌웨어로 추가하여 OpenFlow 스위치를 구성하고 컨트롤러는 소프트웨어로 구현한다. OpenFlow 스위치는 다수의 플로우 테이블을 가질 수 있다.

[0036] SDN에서는 트래픽 플로우의 식별 정보와 플로우 처리 방식을 포함하고 있는 플로우 테이블(Flow Table)을 관리하고 있으며, 실제 사용자 트래픽이 발생하면 플로우 테이블에서 플로우가 일치하는 플로우 엔트리(Flow entry)에 대한 정보를 확인하고, 플로우 엔트리에 따라 패킷 처리 동작 방식을 결정하게 된다. SDN에 따른 패킷 처리 동작 방식에는 트래픽 포워딩(Forwarding), 트래픽 드롭(Drop), 트래픽 변경(Modify), 트래픽 큐잉(Queuing) 등이 있다. 스위치 또는 라우터 등과 같은 네트워크 장치의 QoS 제공 방식에는 플로우 단위 미터링 기반의 Rate-limiting 등과 같은 기본적인 QoS 기능과 포트별 큐를 활용한 DiffServ. 등과 같은 향상된 QoS 기능이 있다. 네트워크 장치는 미터링 관리 테이블을 가지고 있으며, 이를 통해서 플로우 테이블의 플로우 엔트리별 패킷량을 관리하고, 특정 플로우의 대역폭을 제어할 수 있게 된다. 네트워크 장치는 Rate-limiting, Shaping, Policing 등과 같은 플로우 대역폭을 제어하는 방식을 결정할 수 있고, 최대 대역폭, 최소 대역폭 등의 정밀한 대역폭을 제한할 수도 있다.

[0038] 제1 스위치(220)는 진입하는 플로우에 적합한 규칙(rule)을 SDN 컨트롤러(210)에 요청한다. 제1 스위치(220)는 플로우에 포함된 패킷을 SDN 컨트롤러(210)에 보내고, SDN 컨트롤러(210)는 패킷에 포함된 정보(메시지)를 기준으로 특정 규칙을 결정한다. 제1 스위치(220)는 플로우를 분석하는 규칙을 SDN 컨트롤러(210)로부터 전달받고, 해당 규칙을 플로우 테이블에 적용하여 플로우를 분석한다. 이에 반하여 제2 스위치(230)는 사전에 설정한 규칙을 이용하여 트래픽을 분석한다. 제2 스위치(230)는 전술한 클러스터 기법을 적용하여 트래픽을 분석한다. 예컨대, 제2 스위치(230)가 사전에 설정된 규칙이 "SrcIP=10.8.200.3, DstIP=*, Proto=TCP, SrcPort=80, DstPort=*"라면 제2 스위치는 주소가 10.8.200.3인 서버로부터 전달되는 웹 트래픽을 분석한다.

[0040] 제1 스위치(220)는 SDN 컨트롤러(210)로부터 전달받은 규칙을 사용하여 수신한 플로우를 분석한다. 제1 스위치(220)는 플로우 테이블에 SDN 컨트롤러(210)로부터 전달받은 규칙을 적용하여 플로우를 분석한다. 제1 스위치(220)는 수신한 플로우의 크기가 제1 기준값 미만인 경우, 해당 플로우에 포함된 패킷을 CDN(CDNi)에 전달(redirection)한다. 제1 스위치(220)는 플로우의 크기가 제1 기준값 이상인 경우 공격 가능성이 있다고 판단하

여 해당 플로우(패킷)를 제2 스위치(230)로 전달한다.

[0041] 제2 스위치(230)는 수신한 플로우를 사전에 설정한 클러스터 정의에 따라 분석한다. 제2 스위치(230)는 수신한 플로우를 특정 클러스터의 트래픽으로 분류하고, 해당 클러스터의 트래픽이 제2 기준값 이상인 경우 해당 패킷을 널(null) 포트를 보내고 드롭(drop)한다. 즉, 제2 스위치(230)는 해당 클러스터의 트래픽의 양이 제2 기준값 이상인 경우 공격성 패킷이라고 판단한다. 제2 스위치(230)는 해당 클러스터의 트래픽 양이 제2 기준값 미만인 경우 해당 플로우에 포함된 패킷을 CDN(CDNi)에 전달(redirection)한다.

[0042] 한편 제1 스위치(220) 및 제2 스위치(230)가 트래픽 분석을 직접 수행하지 않고, 연결된 SDN 컨트롤러(210)가 트래픽을 분석할 수 있다. 이 경우 SDN 컨트롤러(210)는 트래픽 분석 결과에 따른 제어 정보를 각 스위치(220, 230)에 전달할 수 있다.

[0043] 도 4는 SDN에서 비정상 트래픽을 검출하는 방법에 대한 순서도의 예이다. SDN에 트래픽 플로우가 도착하면(310), 제1 스위치가 먼저 플로우를 분석한다(320). 플로우의 카운트가 제1 기준값 미만이면(330의 Yes), 제1 스위치는 플로우를 CDN으로 전달한다(360). 플로우의 카운트가 제1 기준값 이상이면(330의 No), 제1 스위치는 플로우를 제2 스위치에 전달한다. 이후 제2 스위치가 클러스터의 트래픽을 분석한다(340). 제2 스위치는 클러스터의 트래픽이 제2 기준값 미만이면(350의 Yes) 플로우(패킷)를 CDN으로 전달한다(360). 제2 스위치는 클러스터의 트래픽이 제2 기준값 이상이면(350의 No) 해당 플로우(패킷)을 널 포트로 보내 드롭한다(370).

[0045] 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 유추할 수 있는 변형 예와 구체적인 실시예는 모두 전술한 기술의 권리범위에 포함되는 것이 자명하다고 할 것이다.

부호의 설명

[0046] 50 : 사용자 단말

80 : 서비스 서버

100 : CDNi 네트워크

110 : ALTO 서버

120A, 120B : CDN

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

200 : 비정상 트래픽을 탐지하는 장치

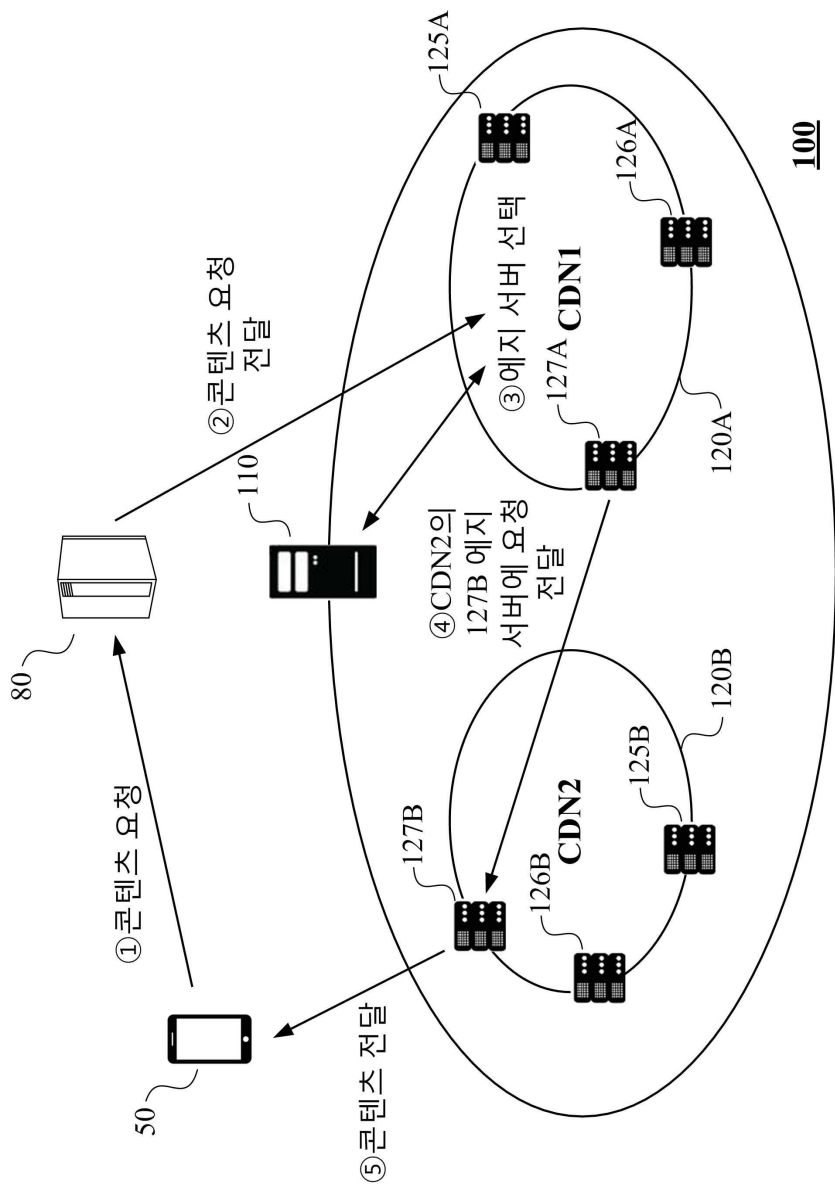
210 : SDN 컨트롤러

220 : 제1 스위치

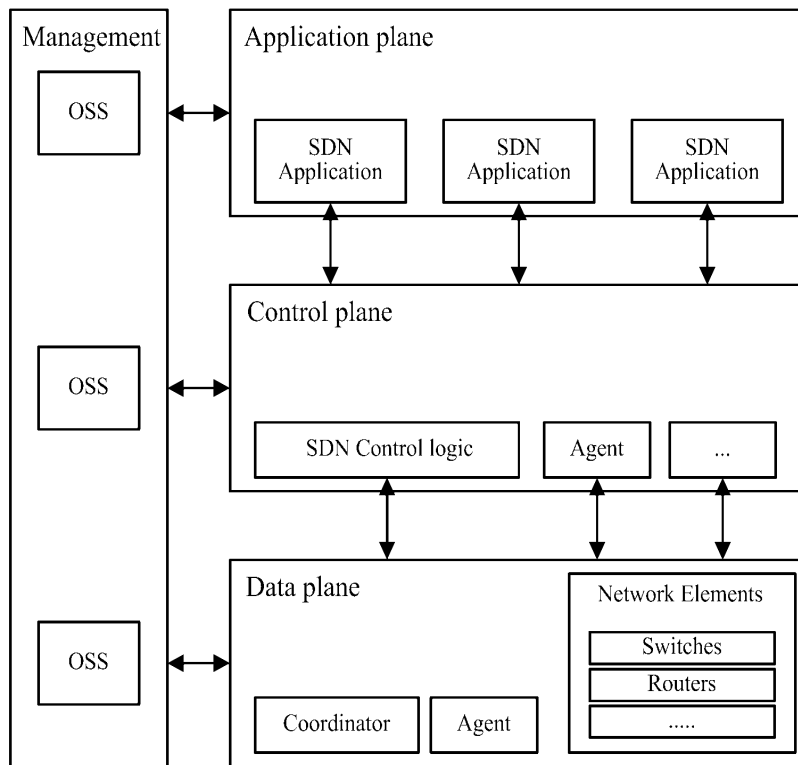
230 : 제2 스위치

도면

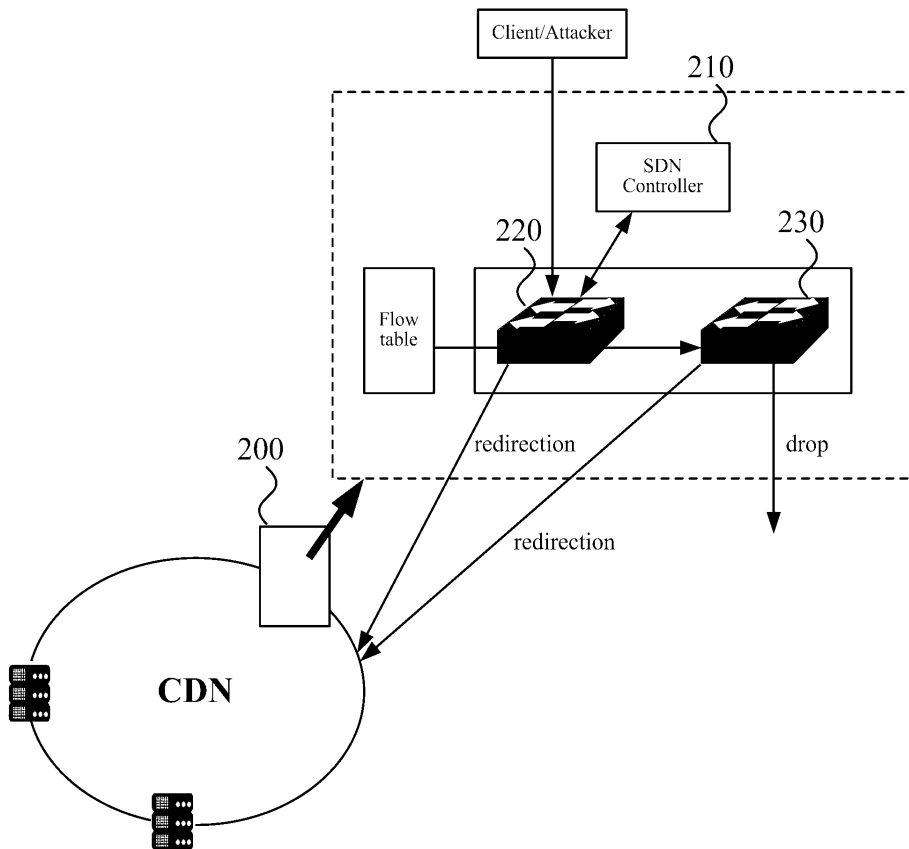
도면1



도면2



도면3



도면4

