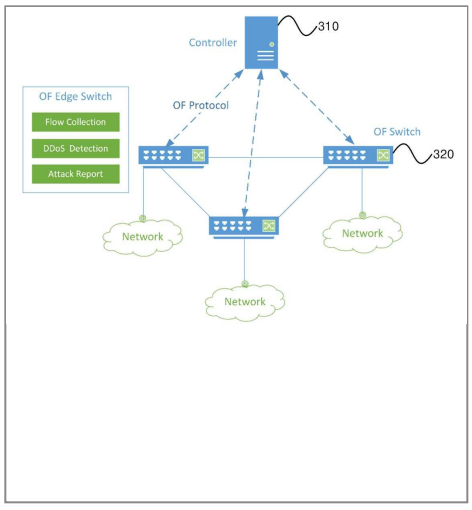
DDoS 공격이 탐지가 가능한 소프트웨어 정의 네트워크 및 이에 포함되는 스위치

SDN capable of detection DDoS attacks and switch including the same

(51) Int. CL	H04L 29/06(2006.01.01) H04L 12/935(2013.01.01)
(52) CPC	H04L 63/1416(2013.01) H04L 49/30(2013.01)
(21) Application No.(Date)	1020160134382 (2016.10.17)
(71) Applicant	Foundation of Soongsil University-Industry Cooperation
(11) Registration No.(Date)	1019001540000 (2018.09.12)
(65) Unex. Pub. No.(Date)	1020180041952 (2018.04.25)
(11) Publication No.(Date)	(2018.11.08)
(86) Int'l Application No.(Date)	
(87) Int'l Unex. Pub. No.(Date)	
(30) Priority info. (Country / No. / Date)	
Legal Status	Registered
Examination Status	Decision to grant (General)
Trial Info	
Kind	Domestic Application / New Application
Right of Org. Application No.(Date)	
Related Application No.	
Request for an examination(Date)	Y(2016.10.17)
Number of examination claims	2



KPA (Korea Patent Abstract) Disclosed are a software definition network capable of detecting DDos attacks and a switch included therein. The software definition network comprises: a controller placed in a control plane of the software definition network; and a plurality of switches placed in a data plane of the software defined network, wherein each of the plurality of switches collects packets received from a corresponding external network, and detects DDoS attacks by using the collected packets.

(71) Applicant

No.	Name	Country	Address
1	Foundation of Soongsil University-Industry Cooperation 숭실대학교산학협력단 (220060278499)	Korea	서울특별시 동작구 상도로 *** (상도동)

(72) Inventor

No.	Name	Country	Address
1	YOO, Myung Sik 유명식	Republic of Korea	서울특별시 서초구...
2	Nguyen Tri Hai 응웬트리하이	Viet Nam	서울특별시 동작구 상도로 ***, 형남공학관 ****호 (상도동)
3	CHOI, Jin Seok 최진석	Republic of Korea	서울특별시 동작구...

(74) Agent

No.	Name	Country	Address
1	Song in ho 송인호 (920050008309)	Korea	*th Floor Donglim Bldg. **, Gangnam-daero **-gil, Gangnam-gu, Seoul(IP-WIZ INTERNATIONAL PATENT & LAW OFFICE)
2	choi kwan rak 최관락 (920040002237)	Korea	*th Floor Donglim Bldg. **, Gangnam-daero **-gil, Gangnam-gu, Seoul(IP-WIZ INTERNATIONAL PATENT & LAW OFFICE)

Right holder(current)

Name	Country	Address
숭실대학교산학협력단	KR	서울특별시 동작구...

Legal Status

No.	Document Title(Eng.)	Receipt/Delivery Date	Status	Receipt/Delivery No.

No.	Document Title(Eng.)	Receipt/Delivery Date	Status	Receipt/Delivery No.
1	[Patent Application] Patent Application ([특허출원]특허출원서)	2016.10.17	Accepted (수리)	112016100348513
2	Request for Prior Art Search (선행기술조사의뢰서)	2018.02.06	Accepted (수리)	919999999999989
3	Report of Prior Art Search (선행기술조사보고서)	2018.04.09	Completion of Transmission (발송처리완료)	962018005831317
4	Notification of reason for refusal (의견제출통지서)	2018.05.14	Completion of Transmission (발송처리완료)	952018032433752
5	[Amendment to Description, etc.] Amendment ([명세서등 보정]보정서)	2018.06.29	Regarded as an acceptance of amendment (보정승인간주)	112018063999481
6	[Opinion according to the Notification of Reasons for Refusal] Written Opinion(Written Reply, Written Substantiation) ([거절이유 등 통지에 따른 의견]의견(답변, 소명)서)	2018.06.29	Accepted (수리)	112018063999335
7	[Amendment to Patent Application, etc.] Amendment ([출원서등 보정]보정서)	2018.07.11	Accepted (수리)	112018068554663
8	Decision to grant (등록결정서)	2018.09.10	Completion of Transmission (발송처리완료)	952018061805162
9	[Amendment to Patent Application, etc.] Amendment ([출원서등 보정]보정서)	2018.11.01	Accepted (수리)	112018108439468
10	([명세서등 보정]보정서(심사관 직권보정))	2018.11.02	Regarded as an acceptance of amendment (보정승인간주)	112018501993415

※ This following Claim Information is not including formula and image information. If you want to know these information, Check the Full Text infromation Please.

Machine Translation

Claim

No.	Content

No.	Content
1	소프트웨어 정의 네트워크에 있어서, 상기 소프트웨어 정의 네트워크의 컨트롤 평면에 위치하는 컨트롤러; 및 상기 소프트웨어 정의 네트워크의 데이터 평면에 위치하는 복수의 스위치;를 포함하되, 상기 복수의 스위치 각각은, 대응되는 외부의 네트워크에서 수신되는 패킷들을 플로우 테이블을 활용하여 수집하고, 상기 수집된 패킷들에 대한 엔트로피가 기 설정된 임계값보다 작은 경우 DDoS 공격이 탐지된 것으로 판단하고, 상기 DDoS 공격이 탐지되는 경우 경고 메시지를 상기 컨트롤러로 전송하며, 상기 컨트롤러는 상기 경고 메시지를 전송한 스위치의 ID를 포함하는 모든 패킷을 분석하여 공격자가 포함된 외부 네트워크를 추적하며, 상기 엔트로피는 하기의 수학식과 같이 정의되는 것을 특징으로 하는 소프트웨어 정의 네트워크. 여기서, H는 상기 엔트로피, n는 윈도우 W 내의 패킷의 개수, 상기 p_i는 윈도우 W 내의 각각의 패킷들의 IP 주소의 확률, x는 패킷들의 목적지의 IP 주소, y는 패킷들이 발생되는 시간의 개수를 각각 의미함.
2	삭제
3	삭제
4	소프트웨어 정의 네트워크에 포함되는 스위치에 있어서, 대응되는 외부의 네트워크에서 수신되는 패킷들을 플로우 테이블을 활용하여 수집하는 수집부; 상기 수집된 패킷들에 대한 엔트로피가 기 설정된 임계값보다 작은 경우 DDoS 공격이 탐지하는 탐지부; 및 상기 DDoS 공격이 탐지되는 경우 경고 메시지를 컨트롤러로 전송하는 통신부;를 포함하되, 상기 컨트롤러는 상기 스위치의 ID를 포함하는 모든 패킷을 분석하여 공격자가 포함된 외부 네트워크를 추적하며, 상기 엔트로피는 하기의 수학식과 같이 정의되는 것을 특징으로 하는 스위치. 여기서, H는 상기 엔트로피, n는 윈도우 W 내의 패킷의 개수, 상기 p_i는 윈도우 W 내의 각각의 패킷들의 IP 주소의 확률, x는 패킷들의 목적지의 IP 주소, y는 패킷들이 발생되는 시간의 개수를 각각 의미함.
5	삭제

Designated States

Kind	Country
:: Empty ::	

※ The information is based on the citation information attached to a Notification of reason for refusal by the examiner.

Forward Citation

Citation

Country	Pub. Date	Pub. No	Title	IPC
Republic of Korea	1020140088340 A	2014.07.10	APPARATUS AND METHOD FOR PROCESSING DDoS IN A OPENFLOW SWITCH	G06F 21/56

Backward Citation

Citation

Application No	Application Date	Title	IPC
:: Empty ::			

Patent Kind Codes

View Graph

Family Patents

No.	Family No.	Country(code)	Country	Type
1	US20180109556	US	United States of America	A1

DOCDB Family info.

Family Patents

No.	Family No.	Country(code)	Country	Type
1	US2018109556 DOCDB	US	United States of America	A1

(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년11월08일
(11) 등록번호 10-1900154
(24) 등록일자 2018년09월12일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 12/935* (2013.01)
(52) CPC특허분류
H04L 63/1416 (2013.01)
H04L 49/30 (2013.01)
(21) 출원번호 10-2016-0134382
(22) 출원일자 2016년10월17일
심사청구일자 2016년10월17일
(65) 공개번호 10-2018-0041952
(43) 공개일자 2018년04월25일
(56) 선행기술조사문헌
KR1020140088340 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
숭실대학교산학협력단
서울특별시 동작구 상도로 369 (상도동)
(72) 발명자
유명식
서울특별시 서초구 신반포로3길 19 , 96동 408호 (반포동)
웅웬트리하이
서울특별시 동작구 상도로 369, 형남공학관 1103호 (상도동)
최진석
서울특별시 동작구 등용로 37, 108동 1609호 (상도동, 상도래미안1차아파트)
(74) 대리인
송인호, 최관락

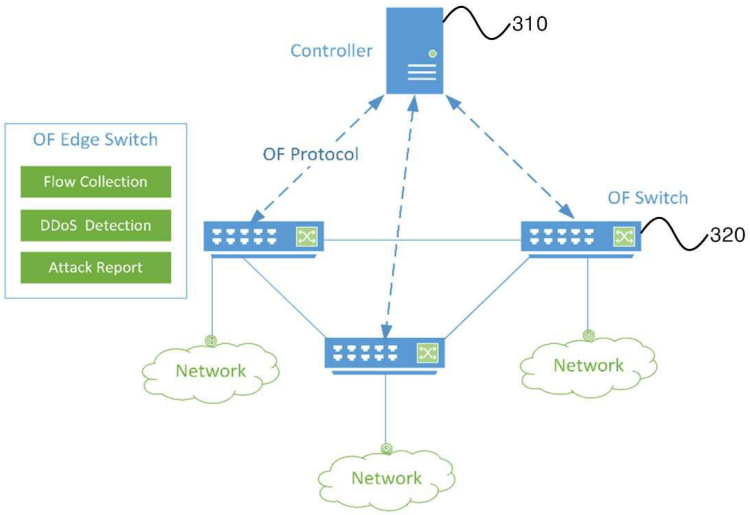
전체 청구항 수 : 총 2 항 심사관 : 문형섭

(54) 발명의 명칭 **DDoS 공격이 탐지가 가능한 소프트웨어 정의 네트워크 및 이에 포함되는 스위치**

(57) 요 약

DDoS 공격이 탐지가 가능한 소프트웨어 정의 네트워크 및 이에 포함되는 스위치가 개시된다. 개시된 소프트웨어 정의 네트워크는 상기 소프트웨어 정의 네트워크의 컨트롤 평면에 위치하는 컨트롤러; 및 상기 소프트웨어 정의 네트워크의 데이터 평면에 위치하는 복수의 스위치;를 포함하되, 상기 복수의 스위치 각각은, 대응되는 외부의 네트워크에서 수신되는 패킷들을 수집하고, 상기 수집된 패킷들을 이용하여 DDoS 공격을 탐지한다.

대 표 도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호	1711070396
부처명	과학기술정보통신부
연구관리전문기관	정보통신기술진흥센터
연구사업명	대학ICT연구센터육성지원사업
연구과제명	인터넷 인프라 시스템 기술 개발 및 전문 인력 양성
기 여 율	1/1
주관기관	숭실대학교 산학협력단
연구기간	2018.01.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

소프트웨어 정의 네트워크에 있어서,

상기 소프트웨어 정의 네트워크의 컨트롤 평면에 위치하는 컨트롤러; 및

상기 소프트웨어 정의 네트워크의 데이터 평면에 위치하는 복수의 스위치;를 포함하되,

상기 복수의 스위치 각각은, 대응되는 외부의 네트워크에서 수신되는 패킷들을 플로우 테이블을 활용하여 수집하고, 상기 수집된 패킷들에 대한 엔트로피가 기 설정된 임계값보다 작은 경우 DDoS 공격이 탐지된 것으로 판단하고, 상기 DDoS 공격이 탐지되는 경우 경고 메시지를 상기 컨트롤러로 전송하며,

상기 컨트롤러는 상기 경고 메시지를 전송한 스위치의 ID를 포함하는 모든 패킷을 분석하여 공격자가 포함된 외부 네트워크를 추적하며,

상기 엔트로피는 하기의 수학식과 같이 정의되는 것을 특징으로 하는 소프트웨어 정의 네트워크.

$$H = -\sum_{1}^{n} p_i \log p_i$$

Where

$$p_i = \frac{x_i}{n}$$

$$W = \{(x_1, y_1), (x_2, y_2), \ldots\}$$

여기서, H는 상기 엔트로피, n는 윈도우 W 내의 패킷의 개수, 상기 p_i는 윈도우 W 내의 각각의 패킷들의 IP 주소의 확률, x는 패킷들의 목적지의 IP 주소, y는 패킷들이 발생되는 시간의 개수를 각각 의미함.

청구항 2

삭제

청구항 3

삭제

청구항 4

소프트웨어 정의 네트워크에 포함되는 스위치에 있어서,

대응되는 외부의 네트워크에서 수신되는 패킷들을 플로우 테이블을 활용하여 수집하는 수집부;

상기 수집된 패킷들에 대한 엔트로피가 기 설정된 임계값보다 작은 경우 DDoS 공격이 탐지하는 탐지부; 및

상기 DDoS 공격이 탐지되는 경우 경고 메시지를 컨트롤러로 전송하는 통신부;를 포함하되,

상기 컨트롤러는 상기 스위치의 ID를 포함하는 모든 패킷을 분석하여 공격자가 포함된 외부 네트워크를 추적하며,

상기 엔트로피는 하기의 수학식과 같이 정의되는 것을 특징으로 하는 스위치.

$$H = -\sum_{1}^{n} p_i \log p_i$$

Where

$$p_i = \frac{x_i}{n}$$

$$W = \{(x_1, y_1), (x_2, y_2), \ldots\}$$

여기서, H는 상기 엔트로피, n는 윈도우 W 내의 패킷의 개수, 상기 p_i는 윈도우 W 내의 각각의 패킷들의 IP 주소의 확률, x는 패킷들의 목적지의 IP 주소, y는 패킷들이 발생되는 시간의 개수를 각각 의미함.

청구항 5

삭제

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 DDoS 공격이 탐지가 가능한 소프트웨어 정의 네트워크(SDN: Software Defined Network) 및 이에 포함되는 스위치(switch)에 관한 것이다.

배 경 기 술

[0002] 인터넷은 우리의 일상에서 이제 불가분의 중요한 역할을 하고 있으며 사물 인터넷이 본격적으로 일상에 적용될 시에는 이 역할은 더욱 커질 것이라 예상한다. 하지만 종래의 네트워크 장비는 미리 정해진 룰에 따라 작동이 되는 시스템으로서, 관리 시 어려움이 있으며, 새로운 기능을 추가 할 시에는 연관된 모든 장비를 업데이트 또는 교체해야 하는 불편함이 존재한다. 그리고, 각종 새로운 악성 공격으로부터도 보안 상의 취약성을 보이고 있다.

[0003] 따라서, 이를 해결하고자 등장한 것이 소프트웨어 정의 네트워크(SDN: Software Defined Network)이다. 소프트웨어 정의 네트워크는 기존의 네트워크 장비와는 달리 컨트롤 평면(control plane)과 데이터 평면(data plane)이 분리된다. 따라서, 네트워크 구조가 단순화되어 있고, 네트워크 관리를 유연하게 해주며, 기존 네트워크보다 악성 공격에 대하여 일부 강점이 있다. 하지만, 소프트웨어 정의 네트워크도 보안에 관하여는 완벽한 해결책이 없으며 여전히 취약한 면이 있는 것도 사실이다.

[0004] 특히, DDoS 공격은 여러 대의 공격자를 분산 배치하여 각 공격자들이 동시에 서비스 거부 공격(DoS: Denial of Service attack)을 수행함으로써 시스템이 더 이상 정상적 서비스를 제공할 수 없도록 하는 공격을 의미한다. 즉, 소프트웨어 정의 네트워크에서, 컨트롤 평면과 데이터 평면 사이에서 DDoS 공격이 수행되는 경우 컨트롤러가 정상적으로 데이터 계층에 지시를 내리지 못하여 할 수 있으며, 만약 이러한 공격을 통해 스위치에 위조된 패킷을 대량으로 전달한다면 소프트웨어 정의 네트워크는 과부하가 걸려 정상적인 작동이 제한된다.

[0005] 최근 들어, 많은 연구자들이 소프트웨어 정의 네트워크에서의 DDoS 공격 탐지 및 완화에 대한 연구를 수행하고 있으나, 아직까지 소프트웨어 정의 네트워크의 컨트롤러에 가해지는 DDoS 공격을 완전하게 탐지하여 막아내는 방법이 존재하지 않는 문제점이 있다.

발명의 내용

해결하려는 과제

[0006] 상기한 바와 같은 종래기술의 문제점을 해결하기 위해, 본 발명에서는 분산된 방식으로 DDoS 공격을 탐지하기

위한 소프트웨어 정의 네트워크 및 이에 포함되는 스위치를 제안하고자 한다.

[0007] 본 발명의 다른 목적들은 하기의 실시예를 통해 당업자에 의해 도출될 수 있을 것이다.

과제의 해결 수단

[0008] 상기한 목적을 달성하기 위해 본 발명의 바람직한 일 실시예에 따르면, 소프트웨어 정의 네트워크에 있어서, 상기 소프트웨어 정의 네트워크의 컨트롤 평면에 위치하는 컨트롤러; 및 상기 소프트웨어 정의 네트워크의 데이터 평면에 위치하는 복수의 스위치;를 포함하되, 상기 복수의 스위치 각각은, 대응되는 외부의 네트워크에서 수신되는 패킷들을 수집하고, 상기 수집된 패킷들을 이용하여 DDoS 공격을 탐지하는 것을 특징으로 하는 소프트웨어 정의 네트워크가 제공된다.

[0009] 상기 복수의 스위치 각각은, 상기 DDoS 공격이 탐지되는 경우 경고 메시지를 상기 컨트롤러로 전송할 수 있다.

[0010] 상기 복수의 스위치 각각은, 하기의 수학식과 같이 정의되는 엔트로피가 기 설정된 임계값보다 작은 경우 DDoS 공격이 탐지된 것으로 판단할 수 있다.

$$H = -\sum_{1}^{n} p_i \log p_i$$

Where

$$p_i = \frac{x_i}{n}$$

$$W = \{(x_1, y_1), (x_2, y_2), \ldots\}$$

[0011]

[0012] 여기서, H는 상기 엔트로피, n는 윈도우 W 내의 패킷의 개수, 상기 p_i는 윈도우 W 내의 각각의 패킷들의 IP 주소의 확률, x는 패킷들의 목적지의 IP 주소, y는 패킷들이 발생되는 시간의 개수를 각각 의미함.

[0013] 또한, 본 발명의 다른 실시예에 따르면, 소프트웨어 정의 네트워크에 포함되는 스위치에 있어서, 대응되는 외부의 네트워크에서 수신되는 패킷들을 수집하는 수집부; 및 상기 수집된 패킷들을 이용하여 DDoS 공격을 탐지하는 탐지부;를 포함하는 것을 특징으로 하는 스위치가 제공된다.

발명의 효과

[0014] 본 발명에 따른 소프트웨어 정의 네트워크는 적은 오버헤드로 DDoS 공격을 정확하게 탐지하는 장점이 있다.

도면의 간단한 설명

[0015] 도 1은 소프트웨어 정의 네트워크(SDN: Software Defined Network)의 기본 구조를 도시한 도면이다.

도 2는 소프트웨어 정의 네트워크에 사용되는 OpenFlow의 구조를 도시한 도면이다.

도 3은 본 발명의 일 실시예에 따른 소프트웨어 정의 네트워크(SDN: Software Defined Network)의 개략적인 구조를 도시한 도면이다.

도 4는 본 발명의 일 실시예에 따른 스위치의 개략적인 구성을 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0016] 본 명세서에서 사용되는 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "구성된다" 또는 "포함한다" 등의 용어는 명세서상에 기재된 여러 구성 요소들, 또는 여러 단계들을 반드시 모두 포함하는 것으로 해석되지 않아야 하며, 그 중 일부 구성 요소들 또는 일부 단계들은 포함되지 않을 수도 있고, 또는 추가적인 구성 요소 또는 단계들을 더 포함할 수 있는 것으로 해석되어야 한다. 또한, 명세서에 기재된 "...부", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는

하드웨어 또는 소프트웨어로 구현되거나 하드웨어와 소프트웨어의 결합으로 구현될 수 있다.

[0017] 이하, 본 발명의 대상이 되는 소프트웨어 정의 네트워크에 대해 간략하게 설명하기로 한다.

[0018] 도 1은 소프트웨어 정의 네트워크(SDN: Software Defined Network)의 기본 구조를 도시한 도면이고, 도 2는 소프트웨어 정의 네트워크에 사용되는 OpenFlow의 구조를 도시한 도면이다.

[0019] 도 1을 참조하면, 소프트웨어 정의 네트워크는 크게 데이터 평면(data plane)과 대응되는 인프라스트럭처 계층(infrastructure layer)과, 컨트롤 평면(control plane)과 대응되는 컨트롤 계층(control layer)과, 애플리케이션 계층(application layer)으로 나뉜다. 데이터 계층은 소프트웨어 정의 네트워크의 특정 인터페이스를 통해 제어를 받는 계층으로서, 데이터 흐름의 전송을 담당한다. 컨트롤 계층은 데이터의 흐름을 제어하는 계층으로서 애플리케이션과 네트워크 서비스를 통하여 데이터 흐름을 라우팅 할 것인지, 전달을 할 것인지, 거절할 것인지를 결정한다. 또한 데이터 계층의 동작들을 정리하여 API(Application Programming Interface) 형태로 애플리케이션 계층에 전달한다. 마지막으로 애플리케이션 계층은 제어 계층에서 제공한 API들을 이용하여 네트워크의 다양한 기능들을 수행 할 수 있도록 한다.

[0020] 한편, 전통적인 네트워크에서 라우터, 스위치와 같은 네트워크 장비는 트래픽 제어와 규칙을 담당한다. 그러므로 네트워크의 라우팅 정보는 스위치와 라우터에서 저장한다. 이와 같은 네트워크 구조는 네트워크가 변화할 때마다 관리자가 관련 인터넷 설비를 배치해야 한다는 문제가 있고, 데이터 센터나 그룹 네트워크 환경은 잦은 네트워크 변화로 자원을 낭비한다.

[0021] OpenFlow은 위와 같은 전통적인 네트워크의 단점을 보완하는 컨트롤러와 네트워크 장치간의 인터페이스 규격으로 사용되고 있는 기술이다. 도 2를 참조하면, OpenFlow는 제어 평면과 데이터 평면을 분리하여 네트워크를 운용할 수 있게 함으로써 네트워크 트래픽을 제어할 수 있는 기능과 전달할 수 있는 기능을 분리하며 소프트웨어를 제작하여 네트워크를 제어할 수 있도록 해준다. OpenFlow 프로토콜을 사용하면, 제어 및 데이터 평면을 하드웨어가 아닌 소프트웨어로도 구현할 수 있으며, 이 소프트웨어를 범용 서버에 설치하여 신속하게 새로운 기능을 구현할 수 있다.

[0022] 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 기술이다.

[0023] 상기에서 설명된 내용을 참조하여 본 발명의 일 실시예에 따른 DDoS 공격이 탐지가 가능한 소프트웨어 정의 네트워크를 상세하게 설명한다.

[0024] 도 3은 본 발명의 일 실시예에 따른 소프트웨어 정의 네트워크(SDN: Software Defined Network)의 개략적인 구조를 도시한 도면이다.

[0025] 도 3을 참조하면, 본 발명의 일 실시예에 따른 소프트웨어 정의 네트워크(300)는, 일례로 OpenFlow(OF) 인터페이스를 사용하며, 컨트롤러(310) 및 복수의 스위치(320)를 포함한다.

[0026] 컨트롤러(310)는 OpenFlow 인터페이스를 따르는 OF 컨트롤러로서, 컨트롤 평면에 위치한다. 컨트롤러(310)는 네트워크의 모든 제어 명령, 데이터 트래픽의 전달을 수행하며, 전체 네트워크를 직접적으로 제어한다.

[0027] 복수의 스위치(320) 각각은 OpenFlow 인터페이스를 따르는 OF 스위치로서, 데이터 평면에 위치하며, 대응되는 외부 네트워크와 연결된다.

[0028] 즉, 컨트롤러(310)는 복수의 스위치(320) 각각에 명령을 전송하고, 각각의 스위치(320)는 수신된 명령에 따라 패킷을 목적지로 전송하거나 수정, 폐기하는 등의 처리를 한다. OpenFlow 프로토콜을 이용하여, 컨트롤러(310)는 패킷의 포워딩 방법이나 VLAN 우선순위 값 등을 스위치(320)에 전달하여 수행되도록 하며, 스위치(320)는 장애정보와 사전에 등록된 플로우 엔트리가 없는 패킷에 대한 정보를 컨트롤러에 문의하고 그 결정을 받아 처리한다.

[0029] 특히, 컨트롤러(310)는 경로 계산을 주 역할로 수행하는 것으로서, 패킷을 전송할 때 몇 가지 매개 변수를 기반으로 경로를 결정한다. 사용하는 매개 변수로는 최단경로(SPF)나 회선 속도 외에 사용자가 지정한 경로의 가중치나 부하 분산 조건 등이 있다. 컨트롤러(310)가 계산한 경로 정보는 TLS(Transport Layer Security) 또는 일반 TCP 연결을 통해 스위치(320)에 보내지며 플로우 테이블에 저장된다. 이후 스위치(320)는 패킷을 수신할

때마다 플로우 테이블을 확인하고 그 프레임을 지정된 경로로 전송한다.

[0030] 한편, 복수의 스위치(320) 각각은 외부의 네트워크에서 수신되는 패킷들을 수집하고, 수집된 패킷들을 이용하여 DDoS 공격을 탐지할 수 있다. 즉, 본 발명에 따르면, 소프트웨어 정의 네트워크에 대한 DDoS 공격은 복수의 스위치(320)에서 분산되어 탐지할 수 있다.

[0031] 보다 상세하게, 컨트롤러(310)에서 DDoS 공격을 탐지하는 것으로 가정하는 경우, 복수의 스위치(320) 각각은 플로우 테이블을 컨트롤러(310)로 주기적으로 전송하고 컨트롤러(310)는 각각의 플로우 테이블을 통해 전체적인 플로우의 정보를 수집한 후 이를 분석하여 DDoS 공격이 있었는지의 여부를 감지할 수 있다. 그러나, 컨트롤러(310)에서 모든 DDoS 공격의 탐지가 수행되는바 플로우 수집 및 프로세싱이 컨트롤 평면에 집중되어 과부하(오버로드)가 큰 단점이 있다.

[0032] 따라서, 본 발명은 이와 같은 문제점을 해결하기 위해 복수의 스위치(320) 각각에서 분산적으로 DDoS 공격의 탐지를 수행하며, 특히 컨트롤러(310)의 명령을 받지 않고 자체적으로 DDoS 공격의 탐지를 수행한다. 이에 따라 컨트롤러(310) 및 스위치(320) 사이에 빈번한 플로우 수집에 의한 과부하가 발생되지 않는 장점이 있다.

[0033] 이하, 도 4를 참조하여 본 발명의 일 실시예에 따른 스위치(320)을 설명하기로 한다.

[0034] 도 4는 본 발명의 일 실시예에 따른 스위치(320)의 개략적인 구성을 도시한 도면이다.

[0035] 도 4를 참조하면, 본 발명의 일 실시예에 따른 스위치(320)는 수집부(321), 탐지부(322) 및 통신부(323)를 포함한다.

[0036] 수집부(321)는 외부의 네트워크에서 수신되는 패킷들을 수집한다. 이 때, 패킷들은 통신부(323)를 통해 수신될 수 있다.

[0037] 즉, 수집부(321)는 스위치(31) 내의 플로우 테이블을 활용하여 각 플로우 항목의 패킷 수의 카운터의 복사본을 추가하여 확장하여 패킷들을 수집할 수 있다. 그 결과 모니터링 기간 동안 플로우 정보를 용이하게 수집한다.

[0038] 그리고, 탐지부(322)는 수집된 패킷들을 이용하여 DDoS 공격을 탐지한다.

[0039] 보다 상세하게, 탐지부(322)는 하기의 수학식 1과 같이 정의되는 엔트로피가 기 설정된 임계값보다 작은 경우 DDoS 공격이 탐지된 것으로 판단할 수 있다. 이에 따라, 탐지부(322)는 실시간으로 대용량의 트래픽을 처리할 수 있다.

수학식 1

[0040]
$$H = -\sum_{1}^{n} p_i \log p_i$$

Where

$$p_i = \frac{x_i}{n}$$

$$W = \{(x_1, y_1), (x_2, y_2), \ldots\}$$

[0041] 여기서, H는 엔트로피, n는 윈도우 W 내의 패킷의 개수, p_i는 윈도우 W 내의 각각의 패킷들의 IP 주소의 확률, x는 패킷들의 목적지의 IP 주소, y는 패킷들이 발생되는 시간의 개수를 각각 의미한다.

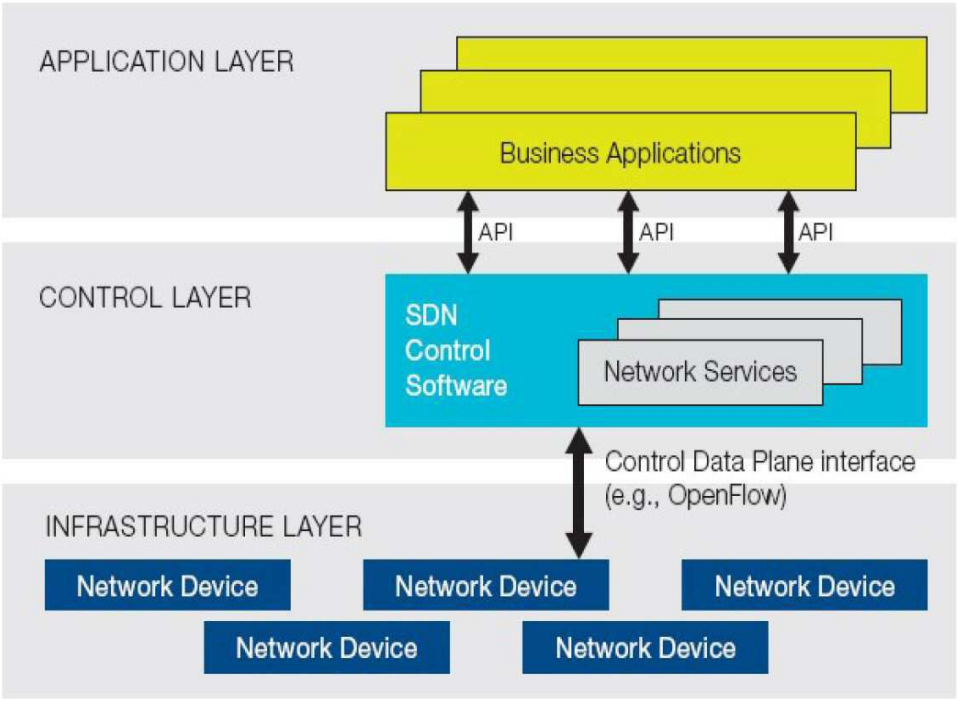
[0042] 또한, 통신부(330)는 DDoS 공격이 탐지되는 경우 경고 메시지를 컨트롤러(310)로 전송한다. 이 후, 컨트롤러(310)는 스위치(320)의 ID를 가진 모든 패킷을 표시하여 공격자가 포함된 외부 네트워크를 다시 추적할 수 있다.

[0043] 요컨대, 본 발명의 일 실시예에 따른 스위치(320)는 컨트롤러(310)에 가해지는 DDoS 공격을 효과적으로 탐지 및 완화할 수 있다. 또한, 확장성 측면에서 하나의 스위치(320)는 로컬 네트워크에서의 DDoS 공격을 검출할 수 있었지만 모든 스위치(320)를 분산 실행하여 DDoS 공격을 탐지하는 경우 전체 네트워크의 공격을 탐지할 수 있다.

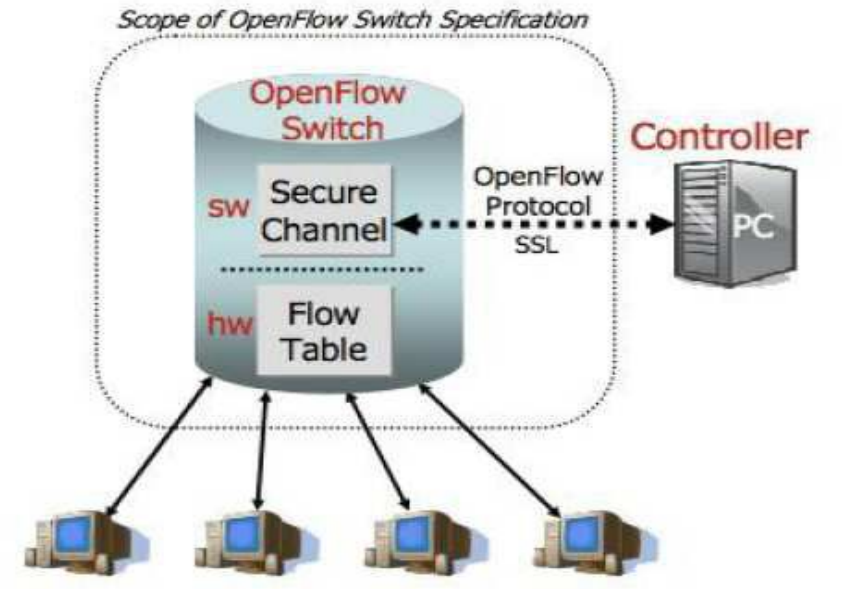
[0044] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

도면

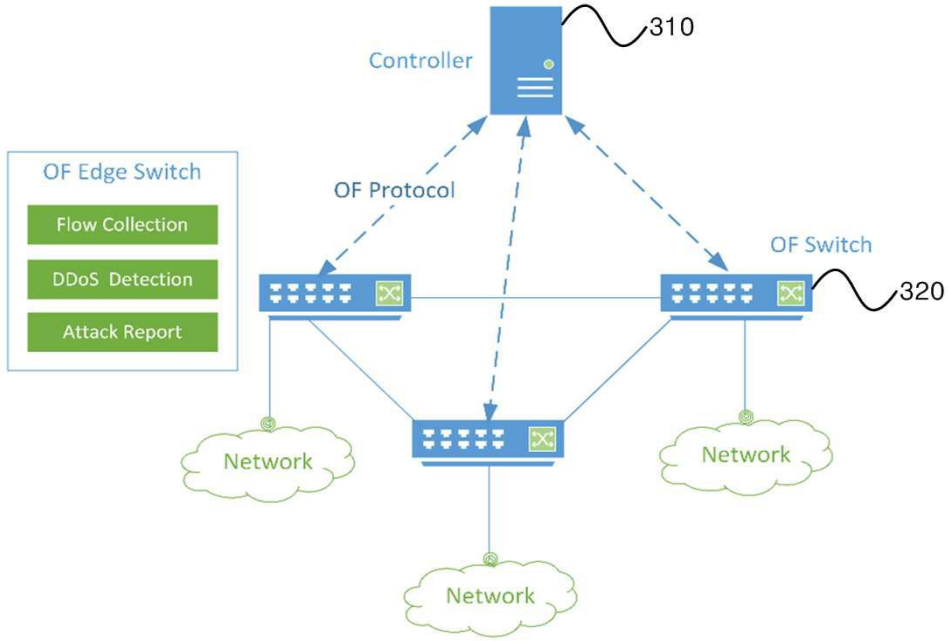
도면1



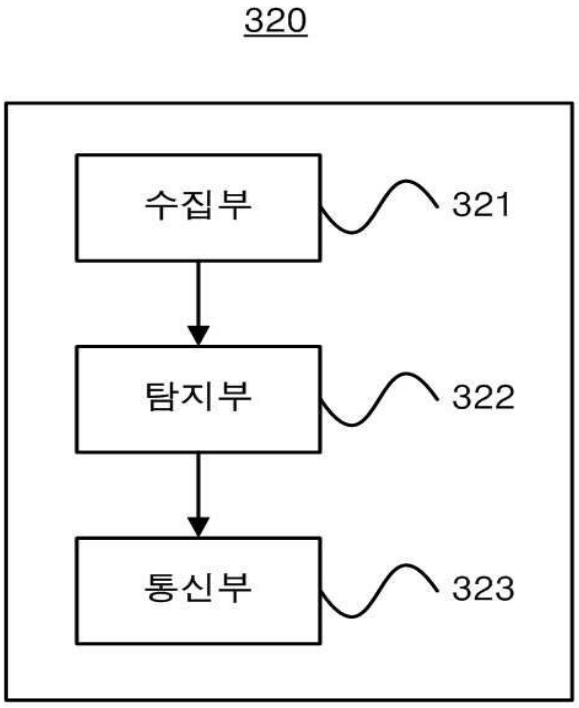
도면2


Scope of OpenFlow Switch Specification
OpenFlow Switch
sw
Secure Channel
hw
Flow Table
OpenFlow Protocol
SSL
Controller
PC

도면3


Controller
310
OF Edge Switch
Flow Collection
DDoS Detection
Attack Report
OF Protocol
OF Switch
320
Network
Network
Network

도면4



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 4

【변경전】

상기 컨트롤러로 전송하는 통신부;

【변경후】

컨트롤러로 전송하는 통신부;