
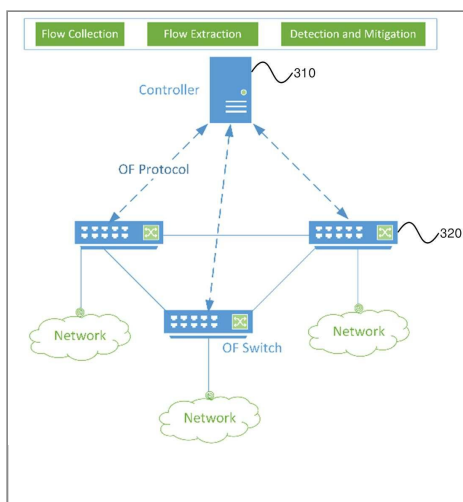


## 인공지능을 이용하여 DDoS 공격을 탐지하는 소프트웨어 정의 네트워크 및 이에 포함되는 컨트롤러

SDN capable of detection DDoS attacks using artificial intelligence and controller including the same

(51) Int. CL	H04L 29/06(2006.01.01) H04L 12/931(2013.01.01) G06N 3/02(2006.01.01)
(52) CPC 	H04L 63/1416(2013.01) H04L 63/1441(2013.01) H04L 49/35(2013.01) G06N 3/02(2013.01)
(21) Application No.(Date)	1020160134383 (2016.10.17)
(71) Applicant	Foundation of Soongsil University-Industry Cooperation
(11) Registration No.(Date)	1019077520000 (2018.10.05)
(65) Unex. Pub. No.(Date)	1020180041953 (2018.04.25)
(11) Publication No.(Date)	(2018.10.12)
(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)

A software defined network for detecting DDoS attacks using artificial intelligence and a controller included therein. The disclosed software defined network includes: the controller located on a control plane of the software defined network; and a plurality of switches located on a data plane of the software defined network. Each

of the plurality of switches collects a flow that is a set of packets, and transmits feature information about the flow to the controller. The controller detects the DDoS attacks by using the feature information about the flow and a back propagation neural network. Accordingly, the present invention can effectively detect and reduce the DDoS attacks applied to the controller. COPYRIGHT KIPO 2018

▶ (71) Applicant

No.	Name	Country	Address
1	Foundation of Soongsil University-Industry Cooperation 송실대학교산학협력단 (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
송실대학교산학협력단	KR	서울특별시 동작구...

## Legal Status

No.	Document Title(Eng.)	Receipt/Delivery Date	Status	Receipt/Delivery No.
1	[Patent Application] Patent Application ([특허출원]특허출원서)	2016.10.17	Accepted (수리)	112016100348669
2	Request for Prior Art Search (선행기술조사뢰서)	2018.02.06	Accepted (수리)	919999999999989
3	Report of Prior Art Search (선행기술조사보고서)	2018.04.09	Completion of Transmission (발 송처리완료)	962018005807017
4	Notification of reason for refusal (의견제출통지서)	2018.05.14	Completion of Transmission (발 송처리완료)	952018032434135
5	[Amendment to Description, etc.] Amendment ([명세서등 보정]보정서)	2018.06.29	Regarded as an acceptance of amendment (보정 승인간주)	112018064000632
6	[Opinion according to the Notification of Reasons for Refusal] Written Opinion(Written Reply, Written Substantiation) ([거절이유 등 통지에 따른 의견]의견(답변, 소 명서))	2018.06.29	Accepted (수리)	112018064000597
7	[Amendment to Patent Application, etc.] Amendment ([출원서등 보정]보정서)	2018.07.11	Accepted (수리)	112018068554517
8	Decision to grant (등록결정서)	2018.09.14	Completion of Transmission (발 송처리완료)	952018063130851

Machine Translation 

## Claim

No.	Content
-----	---------

No.	Content
1	<p>소프트웨어 정의 네트워크에 있어서,</p> <p>상기 소프트웨어 정의 네트워크의 컨트롤 평면에 위치하는 컨트롤러; 및</p> <p>상기 소프트웨어 정의 네트워크의 데이터 평면에 위치하는 복수의 스위치;를 포함하되,</p> <p>상기 복수의 스위치 각각은 패킷들의 집합인 플로우를 수집하고, 상기 수집된 플로우에 대한 특징 정보를 상기 컨트롤러로 전송하며,</p> <p>상기 컨트롤러는, 미리 준비된 학습 플로우의 특징 정보를 역 전파 신경망에 다수 회 입력하여 학습 과정을 통해 DDoS 탐지를 위한 모델인 DDoS 탐지 모델을 생성하고, 상기 수집된 플로우의 특징 정보를 상기 DDoS 탐지 모델의 입력 레이어로 입력하여 DDoS 공격을 탐지하되, 상기 DDoS 탐지 모델의 출력 레이어로 상기 수집된 플로우가 악성 플로우인지 정상 플로우인지를 여부가 출력되며,</p> <p>상기 학습 플로우 및 상기 수집된 플로우 각각의 특징 정보는 플로우 내의 패킷들의 개수 정보, 플로우 내의 바이트의 개수 정보, 플로우를 수집하는 소요 시간 정보 및 플로우의 프로토콜 정보를 포함하고,</p> <p>상기 수집된 플로우가 악성 플로우로 판단되는 경우, 상기 컨트롤러는 명령들을 상기 복수의 스위치로 전송하고, 상기 복수의 스위치 각각은 상기 명령들에 기초하여 동작하되, 상기 명령들은 상기 복수의 스위치 각각의 포워딩을 활성화하는 명령, 악의적인 호스트의 트래픽을 차단하는 명령 및 트래픽을 다시 복원하는 명령을 포함하는 것을 특징으로 하는 소프트웨어 정의 네트워크.</p>
2	삭제
3	삭제
4	<p>소프트웨어 정의 네트워크에 포함되는 컨트롤러에 있어서,</p> <p>미리 준비된 학습 플로우의 특징 정보를 역 전파 신경망에 다수 회 입력하여 학습 과정을 통해 DDoS 탐지를 위한 모델인 DDoS 탐지 모델을 생성하는 모델 생성부;</p> <p>상기 소프트웨어 정의 네트워크에 포함된 복수의 스위치에서 수집된 플로우에 대한 특징 정보를 상기 복수의 스위치 각각으로부터 수신하는 통신부; 및</p> <p>상기 수집된 플로우에 관한 특징 정보 및 역 전파 신경망을 이용하여 DDoS 공격을 탐지하는 탐지부;를 포함하되,</p> <p>상기 탐지부는 상기 수집된 플로우의 특징 정보를 상기 DDoS 탐지 모델의 입력 레이어로 입력하여 DDoS 공격을 탐지하되, 상기 DDoS 탐지 모델의 출력 레이어로 상기 수집된 플로우가 악성 플로우인지 정상 플로우인지를 여부가 출력되며,</p> <p>상기 학습 플로우 및 상기 수집된 플로우 각각의 특징 정보는 플로우 내의 패킷들의 개수 정보, 플로우 내의 바이트의 개수 정보, 플로우를 수집하는 소요 시간 정보 및 플로우의 프로토콜 정보를 포함하고,</p> <p>상기 수집된 플로우가 악성 플로우로 판단되는 경우, 상기 통신부는 명령들을 상기 복수의 스위치로 전송하고, 상기 복수의 스위치 각각은 상기 명령들에 기초하여 동작하되, 상기 명령들은 상기 복수의 스위치 각각의 포워딩을 활성화하는 명령, 악의적인 호스트의 트래픽을 차단하는 명령 및 트래픽을 다시 복원하는 명령을 포함하는 것을 특징으로 하는 컨트롤러.</p>
5	삭제

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	1020160093791 A	2016.08.09	-	-

▶ 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	US20180109557	US	United States of America	A1

▶ DOCDB Family info. 

Family Patents

No.	Family No.	Country(code)	Country	Type
1	US2018109557 <b>DOC</b>	US	United States of America	A1



**(19) 대한민국특허청(KR)**  
**(12) 등록특허공보(B1)**

(45) 공고일자 2018년10월12일  
 (11) 등록번호 10-1907752  
 (24) 등록일자 2018년10월05일

(51) 국제특허분류(Int. Cl.)  
 H04L 29/06 (2006.01) G06N 3/02 (2006.01)  
 H04L 12/931 (2013.01)  
 (52) CPC특허분류  
 H04L 63/1416 (2013.01)  
 G06N 3/02 (2013.01)  
 (21) 출원번호 10-2016-0134383  
 (22) 출원일자 2016년10월17일  
 심사청구일자 2016년10월17일  
 (65) 공개번호 10-2018-0041953  
 (43) 공개일자 2018년04월25일  
 (56) 선행기술조사문헌  
 KR1020160093791 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

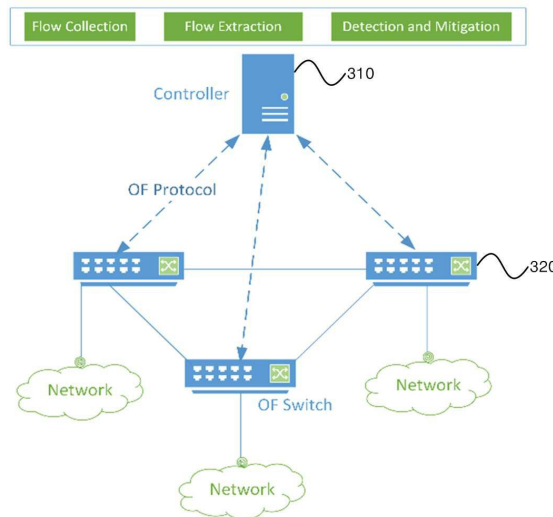
심사관 : 문형섭

(54) 발명의 명칭 **인공지능을 이용하여 DDoS 공격을 탐지하는 소프트웨어 정의 네트워크 및 이에 포함되는 컨트롤러**

**(57) 요약**

인공지능을 이용하여 DDoS 공격을 탐지하는 소프트웨어 정의 네트워크 및 이에 포함되는 컨트롤러가 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 패킷들의 집합인 플로우를 수집하고, 상기 플로우에 대한 특정 정보를 상기 컨트롤러로 전송하며, 상기 컨트롤러는 상기 플로우에 관한 특정 정보 및 역 전파 신경망을 이용하여 DDoS 공격을 탐지한다.

**대표도 - 도3**



(52) CPC특허분류

*H04L 49/35* (2013.01)

*H04L 63/1441* (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711070396

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보통신기술인력양성

연구과제명 인터넷 인프라 시스템 기술 개발 및 전문 인력 양성

기 여 율 1/1

주관기관 숭실대학교산학협력단

연구기간 2018.01.01 ~ 2018.12.31

---

## 명세서

### 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 패킷들의 집합인 플로우를 수집하고, 상기 수집된 플로우에 대한 특징 정보를 상기 컨트롤러로 전송하며,

상기 컨트롤러는, 미리 준비된 학습 플로우의 특징 정보를 역 전파 신경망에 다수 회 입력하여 학습 과정을 통해 DDoS 탐지를 위한 모델인 DDoS 탐지 모델을 생성하고, 상기 수집된 플로우의 특징 정보를 상기 DDoS 탐지 모델의 입력 레이어로 입력하여 DDoS 공격을 탐지하되, 상기 DDoS 탐지 모델의 출력 레이어로 상기 수집된 플로우가 악성 플로우인지 정상 플로우인지를 여부가 출력되며,

상기 학습 플로우 및 상기 수집된 플로우 각각의 특징 정보는 플로우 내의 패킷들의 개수 정보, 플로우 내의 바이트의 개수 정보, 플로우를 수집하는 소요 시간 정보 및 플로우의 프로토콜 정보를 포함하고,

상기 수집된 플로우가 악성 플로우로 판단되는 경우, 상기 컨트롤러는 명령들을 상기 복수의 스위치로 전송하고, 상기 복수의 스위치 각각은 상기 명령들에 기초하여 동작하되, 상기 명령들은 상기 복수의 스위치 각각의 포워딩을 활성화하는 명령, 악의적인 호스트의 트래픽을 차단하는 명령 및 트래픽을 다시 복원하는 명령을 포함하는 것을 특징으로 하는 소프트웨어 정의 네트워크.

#### 청구항 2

삭제

#### 청구항 3

삭제

#### 청구항 4

소프트웨어 정의 네트워크에 포함되는 컨트롤러에 있어서,

미리 준비된 학습 플로우의 특징 정보를 역 전파 신경망에 다수 회 입력하여 학습 과정을 통해 DDoS 탐지를 위한 모델인 DDoS 탐지 모델을 생성하는 모델 생성부;

상기 소프트웨어 정의 네트워크에 포함된 복수의 스위치에서 수집된 플로우에 대한 특징 정보를 상기 복수의 스위치 각각으로부터 수신하는 통신부; 및

상기 수집된 플로우에 관한 특징 정보 및 역 전파 신경망을 이용하여 DDoS 공격을 탐지하는 탐지부;를 포함하되,

상기 탐지부는 상기 수집된 플로우의 특징 정보를 상기 DDoS 탐지 모델의 입력 레이어로 입력하여 DDoS 공격을 탐지하되, 상기 DDoS 탐지 모델의 출력 레이어로 상기 수집된 플로우가 악성 플로우인지 정상 플로우인지를 여부가 출력되며,

상기 학습 플로우 및 상기 수집된 플로우 각각의 특징 정보는 플로우 내의 패킷들의 개수 정보, 플로우 내의 바이트의 개수 정보, 플로우를 수집하는 소요 시간 정보 및 플로우의 프로토콜 정보를 포함하고,

상기 수집된 플로우가 악성 플로우로 판단되는 경우, 상기 통신부는 명령들을 상기 복수의 스위치로 전송하고, 상기 복수의 스위치 각각은 상기 명령들에 기초하여 동작하되, 상기 명령들은 상기 복수의 스위치 각각의 포워딩을 활성화하는 명령, 악의적인 호스트의 트래픽을 차단하는 명령 및 트래픽을 다시 복원하는 명령을 포함하는



것을 특징으로 하는 컨트롤러.

**청구항 5**

삭제

**발명의 설명**

**기술 분야**

[0001] 본 발명의 실시예들은 인공지능을 이용하여 DDoS 공격을 탐지할 수 있는 소프트웨어 정의 네트워크(SDN: Software Defined Network) 및 이에 포함되는 컨트롤러(controller)에 관한 것이다.

**배경 기술**

[0002] 인터넷은 우리의 일상에서 이제 불가분의 중요한 역할을 하고 있으며 사물 인터넷이 본격적으로 일상에 적용될 시에는 이 역할은 더욱 커질 것이라 예상된다. 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, DDoS 공격은 인터넷에 연결되어 있는 많은 수의 컴퓨터에 바이러스를 감염시켜 원격 컴퓨터에서 특정 목적지로 동시에 공격을 진행하여 해당 목적지의 시스템의 오작동 및 회선의 대역폭을 소모시켜 서비스를 제대로 하지 못하도록 하는 공격 방법이다. DDoS 공격의 종류로는 대역폭 소진 공격, 자원 고갈 공격 등이 있다.

[0005] 한편, 소프트웨어 정의 네트워크에서, 메모리 크기의 제한으로 인해 컨트롤러(controller) 및 네트워크 디바이스인 스위치( switch) 내에서의 플로우 테이블의 크기는 제한되어 있으며, DDoS 공격은 이러한 점을 이용하여 연속적인 스푸핑(Spoofing) 요청을 패킷에 주입할 수 있다. 이에 따라, 컨트롤러에 도착하는 패킷의 양이 비정상적으로 많아지게 되며, 컨트롤러는 정상적인 트래픽을 처리할 수 없게 되며, 공격자는 지속적인 공격을 통해 네트워크의 성능을 저하시키거나 심지어는 강제적으로 시스템을 종료시킬 수 있게 된다.

[0006] 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**

[0007] 상기한 바와 같은 종래기술의 문제점을 해결하기 위해, 본 발명에서는 인공지능을 이용하여 DDoS 공격을 탐지할 수 있는 소프트웨어 정의 네트워크(SDN: Software Defined Network) 및 이에 포함되는 컨트롤러(controller)를 제안하고자 한다.

[0008] 본 발명의 다른 목적들은 하기의 실시예를 통해 당업자에 의해 도출될 수 있을 것이다.

**과제의 해결 수단**

[0009] 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 패킷들의 집합인 플로우를 수집하고,

상기 플로우에 대한 특징 정보를 상기 컨트롤러로 전송하며, 상기 컨트롤러는 상기 플로우에 관한 특징 정보 및 역 전파 신경망을 이용하여 DDoS 공격을 탐지하는 것을 특징으로 하는 소프트웨어 정의 네트워크가 제공된다.

[0010] 상기 컨트롤러는 미리 준비된 학습 플로우의 특징 정보를 상기 역 전파 신경망에 입력하여 DDoS 탐지를 위한 모델인 DDoS 탐지 모델을 생성하고, 상기 플로우에 관한 정보를 상기 DDoS 탐지 모델에 입력하여 DDoS 공격을 탐지할 수 있다.

[0011] 상기 플로우에 대한 특징 정보는 상기 플로우 내의 패킷들의 개수 정보, 상기 플로우 내의 바이트의 개수 정보, 상기 플로우를 수집하는 소요 시간 정보 및 상기 플로우의 프로토콜 정보를 포함할 수 있다.

[0012] 또한, 본 발명의 다른 실시예에 따르면, 소프트웨어 정의 네트워크에 포함되는 컨트롤러에 있어서, 패킷들의 집합인 플로우에 관한 특징 정보를 상기 소프트웨어 정의 네트워크에 포함된 복수의 스위치 각각으로부터 수신하는 통신부; 및 상기 플로우에 관한 특징 정보 및 역 전파 신경망을 이용하여 DDoS 공격을 탐지하는 탐지부;를 포함하는 것을 특징으로 하는 컨트롤러가 제공된다.

**발명의 효과**

[0013] 본 발명에 따른 소프트웨어 정의 네트워크는 컨트롤러에 가해지는 DDoS 공격을 효과적으로 검출하고 완화시킬 수 있는 장점이 있다.

**도면의 간단한 설명**

- [0014] 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 컨트롤러의 개략적인 구성을 도시한 도면이다.
- 도 5는 본 발명에서 사용되는 역 전파 신경망의 개념을 설명하기 위한 도면이다.

**발명을 실시하기 위한 구체적인 내용**

[0015] 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.

[0016] 이하, 본 발명의 대상이 되는 소프트웨어 정의 네트워크에 대해 간략하게 설명하기로 한다.

[0017] 도 1은 소프트웨어 정의 네트워크(SDN: Software Defined Network)의 기본 구조를 도시한 도면이고, 도 2는 소프트웨어 정의 네트워크에 사용되는 OpenFlow의 구조를 도시한 도면이다.

[0018] 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.

[0019] 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.

- [0020] 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.
- [0021] 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.
- [0022] 상기에서 설명된 내용을 참조하여 본 발명의 일 실시예에 따른 DDoS 공격이 탐지가 가능한 소프트웨어 정의 네트워크를 상세하게 설명한다.
- [0023] 도 3은 본 발명의 일 실시예에 따른 소프트웨어 정의 네트워크(SDN: Software Defined Network)의 개략적인 구조를 도시한 도면이다.
- [0024] 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.
- [0025] 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.
- [0026] 복수의 스위치(320) 각각은 OpenFlow 인터페이스를 따르는 OF 스위치로서, 데이터 평면에 위치하며, 대응되는 외부 네트워크와 연결된다.
- [0027] 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.
- [0028] 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 프레임이 지정된 경로로 전송한다.
- [0029] 한편, 복수의 스위치(320) 각각은 외부의 네트워크에서 수신되는 패킷들의 집합인 플로우를 수집한다. 즉, 플로우는 일정한 소요 시간에서 수집되며, 동일한 외부 네트워크를 통과하고 동일한 특성을 갖는 연속적인 패킷의 집합을 의미한다. 플로우 엔트리는 넓은 범위의 유용한 통계 정보로 구성되어 있으며, 통계 정보는 플로우를 수집하는 소요 시간, 플로우 내의 패킷들의 개수, 플로우 내의 바이트의 개수, 플로우의 프로토콜, IP 주소, 서비스 포트 등을 포함한다.
- [0030] 본 발명의 일 실시예에 따르면, 복수의 스위치(320) 각각은 플로우에 대한 특징 정보를 산출하고, 이를 컨트롤러(310)로 전송할 수 있다. 여기서, 플로우에 대한 특징 정보는 네트워크 트래픽의 종류 마다 다양할 수 있으며, 본 발명에 따른 플로우에 대한 특징 정보는 4-튜플(4-tuple) 정보로서, 플로우 내의 패킷들의 개수 정보, 플로우 내의 바이트의 개수 정보, 플로우를 수집하는 소요 시간 정보 및 플로우의 프로토콜 정보(TCP SYN, ICMP, UDP)를 포함할 수 있다.
- [0031] 그리고, 컨트롤러(310)는 복수의 스위치(320) 각각에서 수신된 플로우에 관한 특징 정보 및 역 전파 신경망(BPNN: Back Propagation Neural Network)을 이용하여 DDoS 공격을 탐지한다.
- [0032] 이하, 도 4를 참조하여 본 발명의 일 실시예에 따른 컨트롤러(310)의 동작을 상세하게 설명한다.
- [0033] 도 4는 본 발명의 일 실시예에 따른 컨트롤러(310)의 개략적인 구성을 도시한 도면이다.

- [0034] 도 4를 참조하면, 본 발명의 일 실시예에 따른 컨트롤러(310)는 모델 생성부(311), 통신부(312) 및 탐지부(313)를 포함할 수 있다.
- [0035] 모델 생성부(311)는 미리 준비된 학습 플로우의 특징 정보를 역 전과 신경망에 입력하여 DDoS 탐지를 위한 모델인 DDoS 탐지 모델을 생성한다. 여기서, 학습 플로우의 특징 정보 역시 통신부(312)를 통해 미리 수신된 특징 정보일 수 있다.
- [0036] 이하, 도 5를 참조하여 본 발명에서 사용되는 역 전과 신경망의 개념을 설명하기로 한다.
- [0037] 인공 신경망(Artificial Neural Network)은 단순한 기능을 수행하는 뉴런(Neuron)이 모여서 복잡한 기능을 수행하는 뇌를 이루는 것에 영감을 받아서 확립된 모델로서, 인공 신경망의 노드 또는 퍼셉트론(perceptron)이 은 뉴런의 역할을 수행한다. 즉, 하나의 뉴런이 일정 수준의 역치가 넘어가는 신호를 다른 뉴런으로 전달하는 동작과 비슷하게 인공 신경망의 노드 역시 입력된 신호를 활성화 함수로 계산한 뒤, 가중치(weight)와 함께 다른 노드(node)에게 전달한다.
- [0038] 인공 신경망 중 하나인 역 전과 신경망은 도 5과 같은 구조를 가질 수 있다. 역 전과 신경망은 실제 값과 머신 러닝(machine learning)의 모델로부터 계산된 값 사이의 오차를 역순으로 전파하여 오차를 줄여가는 알고리즘이다.
- [0039] 도 5를 참조하면, 역 전과 신경망은 입력 레이어(input layer), 중간 레이어인 은닉 레이어(hidden layer) 및 출력 레이어(output layer)를 포함하며, 역 전과 신경망으로부터 계산된 출력 레이어의 값과 실제 값 사이의 오차가 존재하는 경우, 오차를 줄이기 위해서 가중치와 은닉 레이어의 값을 역으로 수정한다.
- [0040] 보다 상세하게, 입력 레이어, 은닉 레이어 및 출력 레이어에는 하나 이상의 뉴런이 포함된다. 입력 레이어에 포함된 각각의 뉴런들은 입력 정보를 수신하며, 중간 레이어의 각각의 뉴런으로 정보가 전달된다.
- [0041] 중간 레이어는 정보 산출을 담당하는 내부 정보 처리 레이어이다. 중간 레이어는 감도의 수요(demand of sensitivity)에 기초하여 단일 은닉 레이어로 구성될 수도 있고 복수의 은닉 레이어로 구성될 수도 있다. 중간 레이어에서 중간 산출된 정보는 마지막의 은닉 레이어의 뉴런에서 출력 레이어의 뉴런으로 전송된다.
- [0042] 만약, 실제 출력 값이 기대 출력 값과 매칭되거나 또는 학습 과정이 상한에 도달하는 경우 출력 값이 출력되며, 그렇지 않는 경우 백 전파가 시작된다. 백 전파 과정 동안 각 레이어의 가중치는 경사 하강법(gradient descent algorithm)에 따라 조절될 수 있다. 네트워크 출력 에러가 허용 가능한 수준으로 감소될 때까지 또는 학습 과정이 기 설정된 상한에 도달하는 경우 이러한 과정은 계속된다.
- [0043] 한편, DDoS 탐지 모델은 상기에서 설명한 역 전과 신경망과 동일한 구조를 가질 수 있다.
- [0044] 정리하면, 모델 생성부(311)는 학습 플로우의 특징 정보인 학습 플로우의 패킷들의 개수 정보, 학습 플로우 내의 바이트의 개수 정보, 학습 플로우를 수집하는 소요 시간 정보 및 학습 플로우의 프로토콜 정보를 역 전과 신경망의 입력 레이어에 입력하고, 학습 과정을 복수회 반복하여 DDoS 탐지를 위한 모델인 DDoS 탐지 모델을 생성한다.
- [0045] 다음으로, 통신부(312)는 복수의 스위치(320) 각각에서 전송된 플로우에 대한 특징 정보를 수신한다. 이 때, 상기에서 언급한 바와 같이 플로우에 대한 특징 정보는 플로우 내의 패킷들의 개수 정보, 플로우 내의 바이트의 개수 정보, 플로우를 수집하는 소요 시간 정보 및 플로우의 프로토콜 정보를 포함할 수 있다.
- [0046] 계속하여, 탐지부(313)는 복수의 스위치(320)에서 수신된 플로우에 관한 특징 정보를 DDoS 탐지 모델에 입력하여 DDoS 공격을 탐지한다. 즉, 복수의 스위치(320)에서 수신된 플로우에 관한 특징 정보가 DDoS 탐지 모델의 입력 레이어로 입력하고, DDoS 탐지 모델의 출력 레이어로 플로우가 악성 플로우인지 정상 플로우인지를 여부를 판단한다.
- [0047] 만약, 탐지부(313)에서 플로우가 악성 플로우로 판단되는 경우, 컨트롤러(310)는 이러한 플로우를 막기 위해 플로우 추가 요청을 통신부(312)를 통해 전송하고, 이 규칙은 관련된 다음 플로우를 차단하는 스위치(320)에 의해 실행된다. 이 때, 아래의 명령들은 컨트롤러(310)에서 스위치(320)로 전송된다.
- [0048] - 스위치에 포워딩을 활성화하는 명령: `ovs-ofctl add-flow s1 priority=10,action=normal`
- [0049] - 악의적인 호스트의 트래픽을 차단하는 명령: `ovs-ofctl add-flow s1 priority=11, dl_type=0x0800, nw_src=10.0.0.1, action=drop`

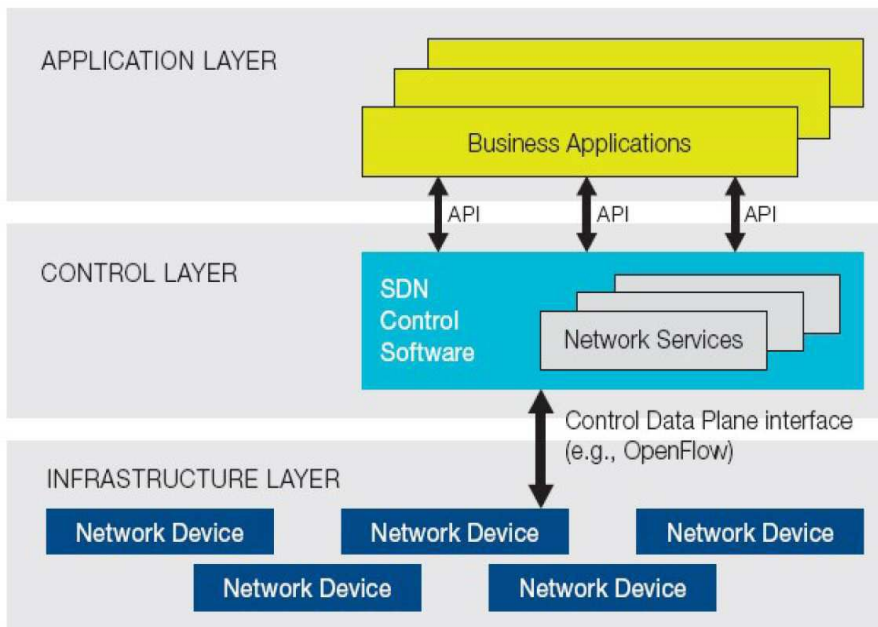
[0050] - 트래픽을 다시 복원하는 명령: `ovs-ofctl -strict del-flows s1 priority=11, dl_type=0x0800, nw_src=10.0.0.1`

[0051] 요컨대, 본 발명의 일 실시예에 따른 소프트웨어 정의 네트워크(300) 및 이에 포함되는 컨트롤러(310)는 인공지능인 역 전파 신경망을 이용하여 DDoS 공격을 정확하게 탐지할 수 있다.

[0052] 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 특허청구범위 뿐만 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

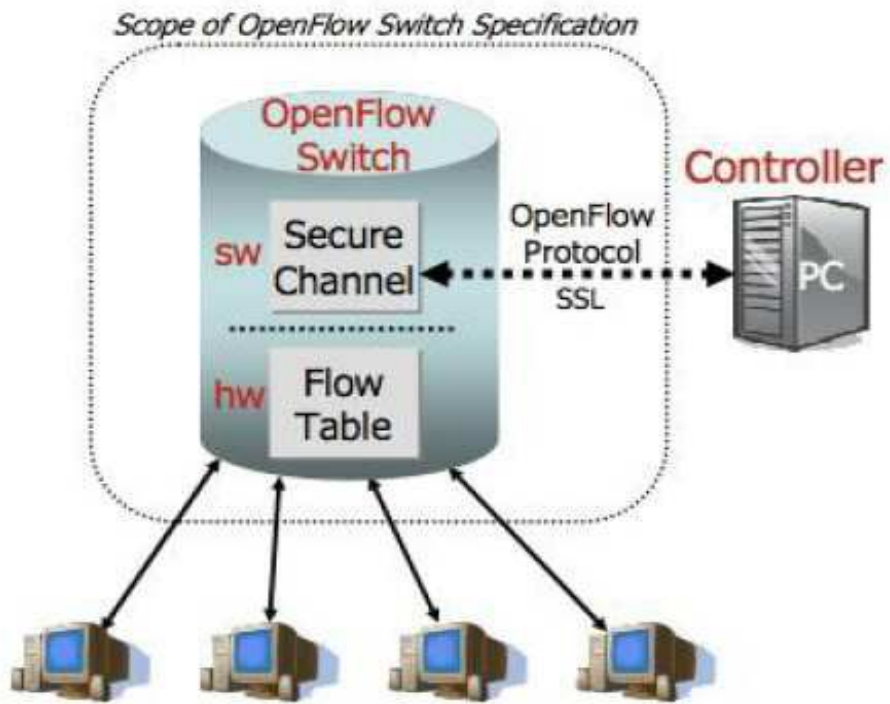
**도면**

**도면1**

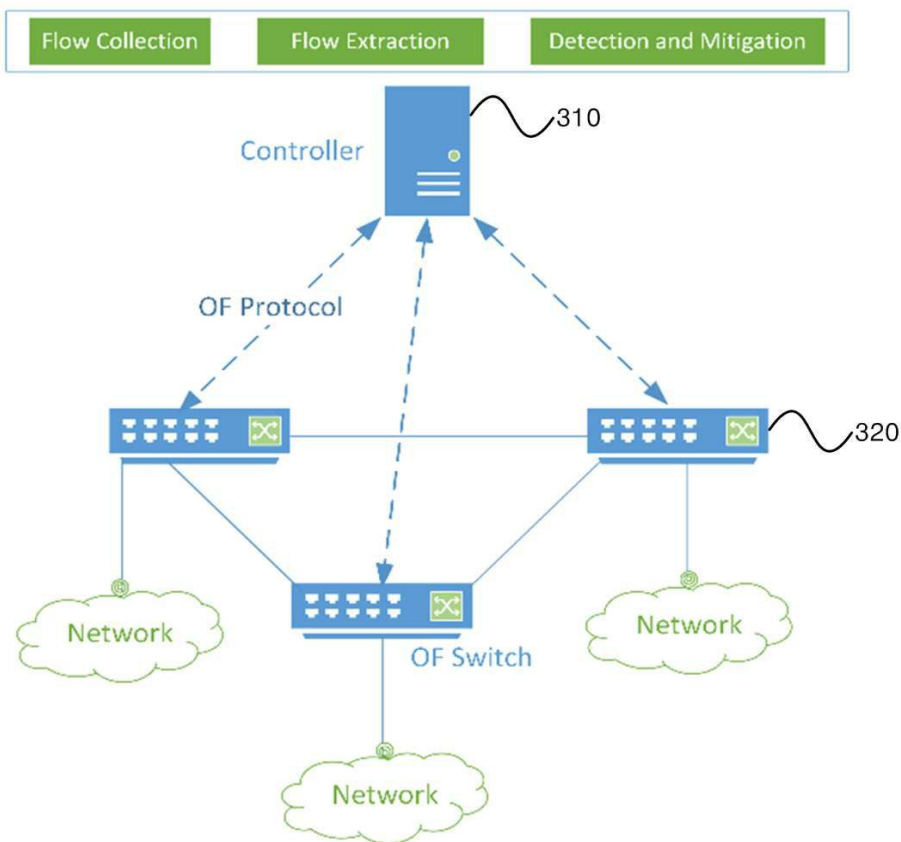




도면2

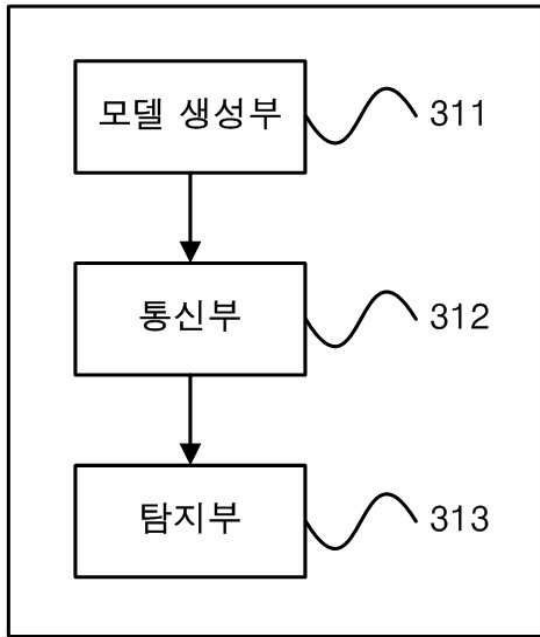


도면3



도면4

310



도면5

