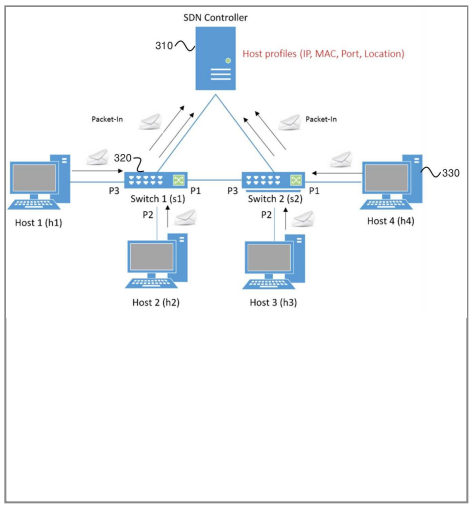
호스트 추적 서비스에 대한 공격을 방지할 수 있는 소프트웨어 정의 네트워크 및 이에 포함되는 컨트롤러

SDN to prevent an attack on the host tracking service and controller including the same

(51) Int. CL	H04L 29/06(2006.01.01) H04L 29/08(2006.01.01)
(52) CPC	H04L 63/1441(2013.01) H04L 63/166(2013.01) H04L 67/22(2013.01)
(21) Application No.(Date)	1020160139066 (2016.10.25)
(71) Applicant	Foundation of Soongsil University-Industry Cooperation
(11) Registration No.(Date)	1019148310000 (2018.10.29)
(65) Unex. Pub. No.(Date)	1020180045214 (2018.05.04)
(11) Publication No.(Date)	(2018.11.02)
(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(2016.10.25)
Number of examination claims	2



KPA (Korea Patent Abstract) Disclosed are a software defined network capable of preventing an attack against a host tracking service and a controller included therein. The software defined network comprises: a plurality of switches which are positioned on a data plane of the software defined network, and are connected to at least one host; and a controller which is positioned on a control plane of the software defined network, and controls the plurality of switches, and in which a host tracking system performing a position of at least one host connected to the plurality of switches is performed. In this

regard, switch A among the plurality of switches receives a packet from host A connected to switch A, and transmits an address information message of the host A to the controller based on the packet. The controller determines whether the host A is a host performing an attack against the host tracking system by using the address information message and previous address information of the host, which is stored in the controller.COPYRIGHT KIPO 2018

(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.
1	[Patent Application] Patent Application ([특허출원]특허출원서)	2016.10.25	Accepted (수리)	112016103614387
2	Request for Prior Art Search (선행기술조사의뢰서)	2018.04.09	Accepted (수리)	919999999999989
3	Report of Prior Art Search (선행기술조사보고서)	2018.06.08	Completion of Transmission (발송처리완료)	962018008503170
4	Notification of reason for refusal (의견제출통지서)	2018.07.16	Completion of Transmission (발송처리완료)	952018047859200
5	[Amendment to Description, etc.] Amendment ([명세서등 보정]보정서)	2018.08.31	Regarded as an acceptance of amendment (보정승인간주)	112018086688234
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)	2018.08.31	Accepted (수리)	112018086688199
7	Decision to grant (등록결정서)	2018.10.25	Completion of Transmission (발송처리완료)	952018072668880

Machine Translation

Claim

No.	Content

No.	Content
1	소프트웨어 정의 네트워크에 있어서, 상기 소프트웨어 정의 네트워크의 데이터 평면에 위치하며, 적어도 하나의 호스트(host)와 연결되는 복수의 스위치; 및 상기 소프트웨어 정의 네트워크의 컨트롤 평면에 위치하며, 상기 복수의 스위치를 제어하며, 상기 복수의 스위치와 각각 연결된 적어도 하나의 호스트의 위치를 인식하는 호스트 추적 서비스(Host Tracking Service)가 수행되며, 상기 복수의 스위치의 연결된 호스트들의 IP 주소 및 상기 호스트들이 연결된 스위치의 포트 주소를 포함하는 호스트 프로파일을 저장하는 컨트롤러;를 포함하되, 상기 복수의 스위치 중 스위치 A가 상기 스위치 A와 연결된 호스트 A로부터 패킷을 수신하고, 상기 수신된 패킷에 기초하여 상기 호스트 A의 IP 주소 및 상기 호스트 A가 연결된 상기 스위치 A의 포트 주소를 포함하는 상기 호스트 A의 주소 정보 메시지를 생성하며, 상기 생성된 주소 정보 메시지를 상기 컨트롤러로 전송하고, 상기 주소 정보 메시지에 포함된 상기 호스트 A의 IP 주소와 동일한 IP 주소를 사용하는 호스트 B가 상기 호스트 프로파일에 저장되어 있는 경우, 상기 컨트롤러는 상기 호스트 B가 연결된 스위치 B로 가용성 여부를 판단하기 위한 메시지인 검사 메시지를 전송하고, 상기 스위치 B는 상기 호스트 B가 연결된 포트 주소로 상기 검사 메시지를 상기 호스트 B로 전송하며, 상기 컨트롤러가 기 설정된 시간 내에 상기 검사 메시지의 응답인 응답 메시지를 상기 스위치 B를 통해 상기 호스트 B로부터 수신하는 경우, 정당한 호스트인 상기 호스트 B를 상기 호스트 A가 사칭하는 것으로 판단하여 상기 호스트 B를 상기 호스트 추적 서비스에 대한 공격을 수행한 호스트로 판단하고, 상기 컨트롤러가 상기 설정된 시간 내에 상기 응답 메시지를 상기 스위치 B를 통해 상기 호스트 B로부터 수신하지 않는 경우, 상기 호스트 A가 이전 위치에서 현재 위치로 마이그레이션한 것으로 판단하여 상기 호스트 A와 상기 호스트 B를 동일한 호스트로 판단하며, 상기 호스트 추적 서비스에 대한 공격이 수행되지 않는 것으로 판단하는 것을 특징으로 하는 소프트웨어 정의 네트워크.
2	삭제
3	삭제
4	삭제
5	소프트웨어 정의 네트워크의 컨트롤 평면에 위치하며, 상기 소프트웨어 정의 네트워크의 데이터 평면에 위치하는 호스트들의 위치를 인식하는 호스트 추적 서비스가 수행되는 컨트롤러에 있어서, 상기 데이터 평면에 위치하는 복수의 스위치 중에서 호스트 A와 연결되는 스위치 A로부터 상기 호스트 A의 주소 정보 메시지를 수신하고, 상기 주소 정보 메시지에서 상기 호스트 A의 IP 주소 및 상기 호스트 A에 대한 상기 스위치 A의 포트 주소를 추출하며, 상기 호스트들의 IP 주소 및 상기 호스트들이 연결된 스위치의 포트 주소를 포함하는 기 저장된 호스트 프로파일과 상기 호스트 A의 IP 주소를 비교하여 상기 호스트 A의 IP 주소와 동일한 IP 주소를 사용하는 호스트 B가 상기 호스트 프로파일에 저장되어 있는 경우, 상기 호스트 프로파일에서 상기 호스트 B가 연결된 스위치 B의 포트 주소를 검색하는 포트 매니저; 상기 스위치 B로 가용성 여부를 판단하기 위한 메시지인 검사 메시지를 전송하는 호스트 프로빙; 및 기 설정된 시간 내에 상기 검사 메시지의 응답인 응답 메시지가 상기 스위치 B를 통해 상기 호스트 B로부터 수신되는 경우, 정당한 호스트인 상기 호스트 B를 상기 호스트 A가 사칭하는 것으로 판단하여 상기 호스트 B를 상기 호스트 추적 서비스에 대한 공격을 수행한 호스트로 판단하고, 상기 설정된 시간 내에 상기 응답 메시지가 상기 스위치 B를 통해 상기 호스트 B로부터 수신되지 않는 경우 상기 호스트 A가 이전 위치에서 현재 위치로 마이그레이션한 것으로 판단하여 상기 호스트 A와 상기 호스트 B를 동일한 호스트로 판단하며, 상기 호스트 추적 서비스에 대한 공격이 수행되지 않는 것으로 판단하는 호스트 체커;를 포함하는 것을 특징으로 하는 컨트롤러.

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	1020160002269 A	2016.01.07	SDN-based ARP Spoofing Detection apparatus and method therefor	H04L 29/06

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	US20180115581	US	United States of America	A1

DOCDB Family info.

Family Patents

No.	Family No.	Country(code)	Country	Type
1	US2018115581 DOCDB	US	United States of America	A1

(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년11월02일
(11) 등록번호 10-1914831
(24) 등록일자 2018년10월29일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)
(52) CPC특허분류
H04L 63/1441 (2013.01)
H04L 63/166 (2013.01)
(21) 출원번호 10-2016-0139066
(22) 출원일자 2016년10월25일
심사청구일자 2016년10월25일
(65) 공개번호 10-2018-0045214
(43) 공개일자 2018년05월04일
(56) 선행기술조사문헌
KR1020160002269 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

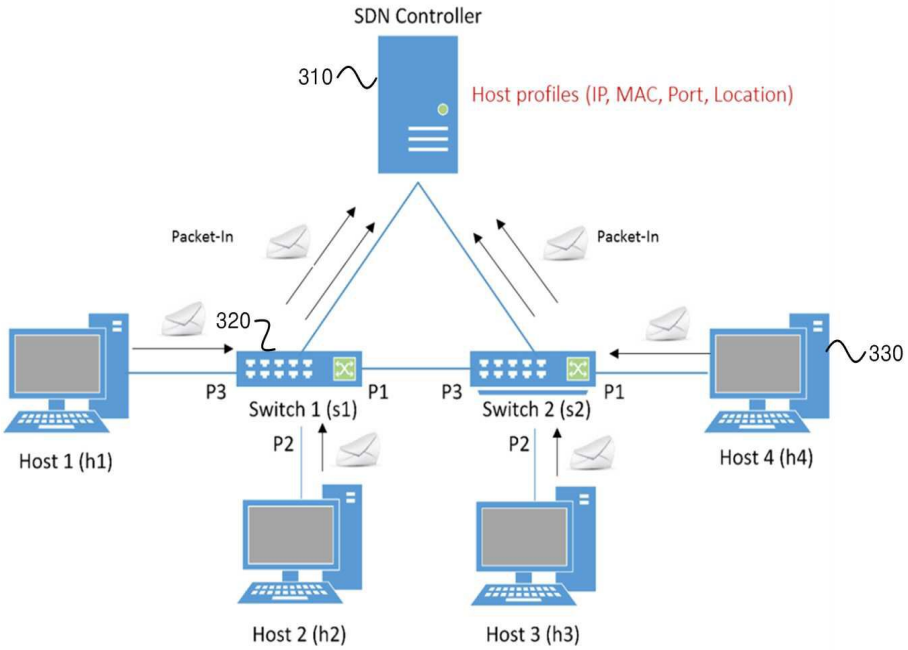
(54) 발명의 명칭 **호스트 추적 서비스에 대한 공격을 방지할 수 있는 소프트웨어 정의 네트워크 및 이에 포함되는 컨트롤러**

(57) 요 약

호스트 추적 서비스에 대한 공격을 방지할 수 있는 소프트웨어 정의 네트워크 및 이에 포함되는 컨트롤러가 개시된다. 개시된 소프트웨어 정의 네트워크는 상기 소프트웨어 정의 네트워크의 데이터 평면에 위치하며, 적어도 하나의 호스트(host)와 연결되는 복수의 스위치; 및 상기 소프트웨어 정의 네트워크의 컨트롤 평면에 위치하며,

(뒷면에 계속)

대 표 도 - 도3



상기 복수의 스위치를 제어하며, 상기 복수의 스위치와 각각 연결된 적어도 하나의 호스트의 위치를 인식하는 호스트 추적 시스템(Host Tracking Service)이 수행되는 컨트롤러;를 포함하되, 상기 복수의 스위치 중 스위치 A는 상기 스위치 A와 연결된 호스트 A로부터 패킷을 수신하고, 상기 패킷에 기초하여 상기 호스트 A의 주소 정보 메시지를 상기 컨트롤러로 전송하고, 상기 컨트롤러는 상기 주소 정보 메시지와 상기 컨트롤러에 저장된 상기 호스트의 이전 주소 정보를 이용하여 상기 호스트 A가 호스트 추적 시스템에 대한 공격을 수행하는 호스트인지 여부를 판단한다.

(52) CPC특허분류
H04L 67/22 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 H8501-16-1008 / 1711035246
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 대학 ICT연구센터 육성 지원사업
연구과제명 클라우드 환경의 스마트 기기와 서비스 보안 기술 개발 및 연구 인력양성
기 여 율 1/1
주관기관 숭실대학교산학협력단
연구기간 2016.01.01 ~ 2016.12.31

명 세 서

청구범위

청구항 1

소프트웨어 정의 네트워크에 있어서,

상기 소프트웨어 정의 네트워크의 데이터 평면에 위치하며, 적어도 하나의 호스트(host)와 연결되는 복수의 스위치; 및

상기 소프트웨어 정의 네트워크의 컨트롤 평면에 위치하며, 상기 복수의 스위치를 제어하며, 상기 복수의 스위치와 각각 연결된 적어도 하나의 호스트의 위치를 인식하는 호스트 추적 서비스(Host Tracking Service)가 수행되며, 상기 복수의 스위치의 연결된 호스트들의 IP 주소 및 상기 호스트들이 연결된 스위치의 포트 주소를 포함하는 호스트 프로파일을 저장하는 컨트롤러;를 포함하되,

상기 복수의 스위치 중 스위치 A가 상기 스위치 A와 연결된 호스트 A로부터 패킷을 수신하고, 상기 수신된 패킷에 기초하여 상기 호스트 A의 IP 주소 및 상기 호스트 A가 연결된 상기 스위치 A의 포트 주소를 포함하는 상기 호스트 A의 주소 정보 메시지를 생성하며, 상기 생성된 주소 정보 메시지를 상기 컨트롤러로 전송하고,

상기 주소 정보 메시지에 포함된 상기 호스트 A의 IP 주소와 동일한 IP 주소를 사용하는 호스트 B가 상기 호스트 프로파일에 저장되어 있는 경우, 상기 컨트롤러는 상기 호스트 B가 연결된 스위치 B로 가용성 여부를 판단하기 위한 메시지인 검사 메시지를 전송하고, 상기 스위치 B는 상기 호스트 B가 연결된 포트 주소로 상기 검사 메시지를 상기 호스트 B로 전송하며,

상기 컨트롤러가 기 설정된 시간 내에 상기 검사 메시지의 응답인 응답 메시지를 상기 스위치 B를 통해 상기 호스트 B로부터 수신하는 경우, 정당한 호스트인 상기 호스트 B를 상기 호스트 A가 사칭하는 것으로 판단하여 상기 호스트 B를 상기 호스트 추적 서비스에 대한 공격을 수행한 호스트로 판단하고,

상기 컨트롤러가 상기 설정된 시간 내에 상기 응답 메시지를 상기 스위치 B를 통해 상기 호스트 B로부터 수신하지 않는 경우, 상기 호스트 A가 이전 위치에서 현재 위치로 마이그레이션한 것으로 판단하여 상기 호스트 A와 상기 호스트 B를 동일한 호스트로 판단하며, 상기 호스트 추적 서비스에 대한 공격이 수행되지 않는 것으로 판단하는 것을 특징으로 하는 소프트웨어 정의 네트워크.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

소프트웨어 정의 네트워크의 컨트롤 평면에 위치하며, 상기 소프트웨어 정의 네트워크의 데이터 평면에 위치하는 호스트들의 위치를 인식하는 호스트 추적 서비스가 수행되는 컨트롤러에 있어서,

상기 데이터 평면에 위치하는 복수의 스위치 중에서 호스트 A와 연결되는 스위치 A로부터 상기 호스트 A의 주소 정보 메시지를 수신하고, 상기 주소 정보 메시지에서 상기 호스트 A의 IP 주소 및 상기 호스트 A에 대한 상기 스위치 A의 포트 주소를 추출하며, 상기 호스트들의 IP 주소 및 상기 호스트들이 연결된 스위치의 포트 주소를 포함하는 기 저장된 호스트 프로파일과 상기 호스트 A의 IP 주소를 비교하여 상기 호스트 A의 IP 주소와 동일한 IP 주소를 사용하는 호스트 B가 상기 호스트 프로파일에 저장되어 있는 경우, 상기 호스트 프로파일에서 상기 호스트 B가 연결된 스위치 B의 포트 주소를 검색하는 포트 매니저;

상기 스위치 B로 가용성 여부를 판단하기 위한 메시지인 검사 메시지를 전송하는 호스트 프로빙; 및

기 설정된 시간 내에 상기 검사 메시지의 응답인 응답 메시지가 상기 스위치 B를 통해 상기 호스트 B로부터 수신되는 경우, 정당한 호스트인 상기 호스트 B를 상기 호스트 A가 사칭하는 것으로 판단하여 상기 호스트 B를 상기 호스트 추적 서비스에 대한 공격을 수행한 호스트로 판단하고, 상기 설정된 시간 내에 상기 응답 메시지가 상기 스위치 B를 통해 상기 호스트 B로부터 수신되지 않는 경우 상기 호스트 A가 이전 위치에서 현재 위치로 마이그레이션한 것으로 판단하여 상기 호스트 A와 상기 호스트 B를 동일한 호스트로 판단하며, 상기 호스트 추적 서비스에 대한 공격이 수행되지 않는 것으로 판단하는 호스트 체커;를 포함하는 것을 특징으로 하는 컨트롤러.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 호스트 추적 서비스에 대한 공격을 방지할 수 있는 소프트웨어 정의 네트워크(SDN: Software Defined Network) 및 이에 포함되는 컨트롤러(controller)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] 이와 관련하여, 호스트 추적 서비스(HTS: Host Tracking Service)는 소프트웨어 정의 네트워크 내에서 모든 호스트들의 위치는 인식 내지 추적할 수 있는 서비스이다. 그러나, 호스트 추적 서비스는 유효성 검사, 인증 또는 승인을 필요로 하지 않기 때문에, 공격자는 이 결함을 이용하여 소프트웨어 정의 네트워크 내의 컨트롤러에 의해 제어되는 스위치를 통하여 악성 메시지를 송신하여 공격을 실행할 수 있다. 즉, 공격자는 쉽게 타켓 호스트를 가장할 수 있으며, 호스트 추적 서비스가 호스트의 위치를 잘못 인식하게 할 수 있다. 이는 심각한 하이재킹을 유도할 수 있으며, 이 외에도 서비스 거부 공격 또는 중간자 공격을 유발할 수 있다.

발명의 내용

해결하려는 과제

[0005] 상기한 바와 같은 종래기술의 문제점을 해결하기 위해, 본 발명에서는 호스트 추적 서비스에 대한 공격을 방지할 수 있는 소프트웨어 정의 네트워크(SDN: Software Defined Network) 및 이에 포함되는 컨트롤러(controller)를 제안하고자 한다.

[0006] 본 발명의 다른 목적들은 하기의 실시예를 통해 당업자에 의해 도출될 수 있을 것이다.

과제의 해결 수단

[0007] 상기한 목적을 달성하기 위해 본 발명의 바람직한 일 실시예에 따르면, 소프트웨어 정의 네트워크에 있어서, 상기 소프트웨어 정의 네트워크의 데이터 평면에 위치하며, 적어도 하나의 호스트(host)와 연결되는 복수의 스위치; 및 상기 소프트웨어 정의 네트워크의 컨트롤 평면에 위치하며, 상기 복수의 스위치를 제어하며, 상기 복수의 스위치와 각각 연결된 적어도 하나의 호스트의 위치를 인식하는 호스트 추적 시스템(Host Tracking Service)이 수행되는 컨트롤러;를 포함하되, 상기 복수의 스위치 중 스위치 A는 상기 스위치 A와 연결된 호스트 A로부터 패킷을 수신하고, 상기 패킷에 기초하여 상기 호스트 A의 주소 정보 메시지를 상기 컨트롤러로 전송하고, 상기 컨트롤러는 상기 주소 정보 메시지와 상기 컨트롤러에 저장된 상기 호스트의 이전 주소 정보를 이용하여 상기 호스트 A가 호스트 추적 시스템에 대한 공격을 수행하는 호스트인지 여부를 판단하는 것을 특징으로 하는 소

프트웨어 정의 네트워크가 제공된다.

[0008] 상기 수신된 주소 정보 메시지는 상기 호스트 A의 IP 주소 및 상기 호스트 A가 연결된 상기 스위치 A의 포트 주소 중 적어도 하나를 포함하고, 상기 컨트롤러는 호스트 프로파일을 저장하되, 상기 호스트 프로파일은 상기 복수의 스위치의 연결된 복수의 호스트 각각의 IP 주소 및 상기 호스트가 연결된 스위치의 포트 주소 중 적어도 하나를 포함할 수 있다.

[0009] 상기 컨트롤러는 상기 주소 정보 메시지에 포함된 상기 호스트 A의 IP 주소와 동일한 IP 주소를 사용하는 호스트 B가 상기 호스트 프로파일에 저장되어 있는 경우 상기 호스트 B가 연결된 스위치 B로 상기 검사 메시지를 전송하며, 상기 검사 메시지와 대응되는 응답 메시지가 상기 스위치 B를 통해 상기 호스트 B에서 수신되는 경우 상기 호스트 A가 상기 호스트 B를 사칭하는 것으로 판단할 수 있다.

[0010] 상기 검사 메시지는 상기 호스트 B의 가용성 여부를 판단하기 위한 메시지일 수 있다.

[0011] 또한, 본 발명의 다른 실시예에 따르면, 컨트롤 평면 및 데이터 평면을 포함하는 소프트웨어 정의 네트워크에서 상기 컨트롤 평면에 위치하며, 호스트 추적 시스템(Host Tracking Service)이 수행되는 컨트롤러에 있어서, 상기 데이터 평면에 위치하며 적어도 하나의 호스트(host)와 연결되는 복수의 스위치 중 스위치 A로부터 상기 스위치 A와 연결된 호스트 A의 주소 정보 메시지를 수신하고, 상기 주소 정보 메시지 내의 상기 호스트 A의 IP 주소 및 상기 호스트 A의 상기 스위치 A의 포트 주소를 추출하며, 상기 호스트 A의 IP 주소와 동일한 IP 주소를 사용하는 호스트 B가 기 저장된 호스트 프로파일에 저장되어 있는 경우, 상기 호스트 B가 연결된 스위치 B의 포트 주소를 검색하는 포트 매니저; 상기 호스트 B가 연결된 상기 스위치 B로 상기 검사 메시지를 전송하는 호스트 프로빙; 및 상기 검사 메시지와 대응되는 응답 메시지가 상기 스위치 B를 통해 상기 호스트 B에서 수신되는 경우 상기 호스트 A가 상기 호스트 B를 사칭하는 것으로 판단하는 호스트 체커;를 포함하는 것을 특징으로 하는 컨트롤러가 제공된다.

발명의 효과

[0012] 본 발명에 따른 소프트웨어 정의 네트워크는 컨트롤러에서 수행되는 호스트 추적 서비스에 대한 공격을 방지할 수 있는 장점이 있다.

도면의 간단한 설명

[0013] 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 호스트 추적 서비스에 대한 공격의 일례를 설명하기 위한 도면이다.

도 5는 본 발명의 일 실시예에 따른 컨트롤러의 개략적인 구성을 도시한 도면이다.

도 6은 본 발명의 일 실시예에 따른 호스트 추적 서비스에 대한 공격을 방지하는 컨트롤러의 동작의 흐름도를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0014] 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.

[0015] 이하, 본 발명의 대상이 되는 소프트웨어 정의 네트워크에 대해 간략하게 설명하기로 한다.

[0016] 도 1은 소프트웨어 정의 네트워크(SDN: Software Defined Network)의 기본 구조를 도시한 도면이고, 도 2는 소프트웨어 정의 네트워크에 사용되는 OpenFlow의 구조를 도시한 도면이다.

[0017] 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.

[0018] 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.

[0019] 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.

[0020] 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.

[0021] 상기에서 설명된 내용을 참조하여 본 발명의 일 실시예에 따른 호스트 추적 서비스의 공격을 방지할 수 있는 소프트웨어 정의 네트워크를 상세하게 설명한다.

[0022] 도 3은 본 발명의 일 실시예에 따른 소프트웨어 정의 네트워크(SDN: Software Defined Network)의 개략적인 구조를 도시한 도면이다.

[0023] 도 3을 참조하면, 본 발명의 일 실시예에 따른 소프트웨어 정의 네트워크(300)는, 컨트롤러(310), 복수의 스위치(320) 및 복수의 호스트(330)를 포함한다.

[0024] 컨트롤러(310) 즉, SDN 컨트롤러는 컨트롤 평면에 위치하며, 네트워크의 모든 제어 명령, 데이터 트래픽의 전달을 수행하며, 전체 네트워크를 직접적으로 제어한다.

[0025] 복수의 스위치(320) 각각은 데이터 평면에 위치하며, 컨트롤러(310)에 의해 동작이 제어된다. 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. 일례로, 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.

[0026] 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.

[0027] 복수의 호스트(330) 각각은 스위치(320) 각각과 연결된다. 이 때, 호스트(330)는 주소 정보를 가지고 있으며, 주소 정보를 통해 패킷들을 송신 또는 수신한다. 본 발명의 일 실시예에 따르면, 호스트(330)의 주소 정보는 IP 주소 및 MAC 주소 및 호스트가 연결된 스위치 포트 주소 등을 포함할 수 있다.

[0028] 한편, 컨트롤러(310)에서는 소프트웨어 정의 네트워크(300) 내에서 모든 호스트들의 위치는 인식 내지 추적할 수 있는 서비스인 호스트 추적 서비스(HTS: Host Tracking Service)가 수행될 수 있다. 이에 대해 간략하게 설명하면 다음과 같다.

[0029] 소프트웨어 정의 네트워크(300)에서, 호스트(330)는 네트워크의 서로 다른 물리적 위치 사이에서 마이그레이션 할 수 있는데, 컨트롤러(310)에서 수행되는 호스트 추적 서비스는 이러한 호스트(330)의 위치를 추척할 수 있다. 호스트 추적 서비스는 패킷-인 메시지(Packet-In messages)를 동적으로 프로빙하고 호스트 프로파일(Host Profiles)을 업데이트함으로써 유연하게 네트워크의 이동성을 보장하는 쉬운 방법을 제공한다. 이 때, 호스트 프로파일은 컨트롤러(310)에 저장되는 것으로서, 모든 호스트(330)에 대한 IP 주소, MAC 주소, DPID(Diagnostic Provider ID), 각 호스트(330)과 연결된 스위치(320)에 대한 포트 번호, 최종 타임스탬프 등이 포함된다. 호스트 추적 서비스는 2가지의 관련 호스트 이벤트인 JOIN 이벤트 및 MOVE 이벤트를 처리한다.

[0030] 이 때, 상기에서 설명한 바와 같이, 호스트 추적 서비스는 유효성 검사, 인증 또는 승인을 필요로 하지 않기 때문에, 공격자는 이 결함을 이용하여 소프트웨어 정의 네트워크(300) 내의 컨트롤러(310)에 의해 제어되는 스위치(320)를 통하여 악성 메시지를 송신하여 공격을 실행할 수 있다.

[0031] 이하, 도 4를 참조하여 호스트 추적 서비스에 대한 공격의 일례를 설명하기로 한다.

[0032] 도 4를 참조하면, 하나의 스위치(320)에 대해 3개의 호스트(330)가 연결되어 있고, 호스트 1이 공격자인 호스트이고 호스트 3이 피해자인 호스트이다. 따라서, 호스트 1이 호스트 3을 사칭하는 것으로 가정한다. 호스트 추적 서비스에 대한 공격은 아래와 같은 3단계의 상태로 이루어진다.

[0033] 단계 1에서, 공격자인 호스트 1은 호스트 3의 IP 주소를 가장하여 가짜 ARP 요청을 스위치(330)로 전송하고, 스위치(330)는 이를 컨트롤러(320)로 전송한다. 이 때, 호스트 1의 실제 주소 정보는 [IP: 10.0.0.1, MAC: 00:00:00:00:00:00:01]이고, 호스트 3의 실제 주소 정보는 [IP: 10.0.0.3, MAC: 00:00:00:00:00:00:03]이며, 컨트롤러(310)의 입장에서 호스트 1의 주소 정보는 [IP: 10.0.0.3, MAC: 00:00:00:00:00:00:01]이다.

[0034] 단계 2에서, 컨트롤러(310)는 상기한 정보를 획득하고, 호스트 1의 IP 정보를 [10.0.0.1]에서 [10.0.0.3]으로 변경한다. 그리고, 컨트롤러(310)는 스위치(320)를 제어하기 위한 메시지를 전송한다.

[0035] 단계 3에서, 사용자는 호스트 3 대신 호스트 1로 연결된다. 따라서, 호스트 1이 호스트 3으로 전송되는 트래픽을 가로챌 수도 있다.

[0036] 도 5는 본 발명의 일 실시예에 따른 컨트롤러(320)의 개략적인 구성을 도시한 도면이다. 도 5를 참조하면, 본 발명의 일 실시예에 따른 컨트롤러(320)는 포트 매니저(311), 호스트 프로빙(host probing)(312) 및 호스트 체커(host checker)(313)를 포함한다. 그리고, 도 6은 본 발명의 일 실시예에 따른 호스트 추적 서비스에 대한 공격을 방지하는 컨트롤러(320)의 동작의 흐름도를 도시한 도면이다.

[0037] 이하, 도 3, 도 5 및 도 6를 참조하여 상기에서 설명한 호스트 추적 서비스에 대한 공격을 방지할 수 있는 소프트웨어 정의 네트워크(300) 및 컨트롤러(320)를 상세하게 설명하기로 한다.

[0038] 먼저, 단계(610)에서, 포트 매니저(311)는 복수의 스위치 중 스위치 A로부터 스위치 A와 연결된 호스트 A의 주소 정보 메시지를 수신한다.

[0039] 즉, 호스트 A는 스위치 A와 연결되어 있으며, 호스트 A는 스위치 A로 패킷을 전송하며, 스위치 A는 상기 수신된 패킷에 기초하여 호스트 A의 주소 정보 메시지, 즉 패킷-인 메시지를 생성하여 컨트롤러(320)로 전송한다.

[0040] 여기서, 주소 정보 메시지에는 호스트 A의 IP 주소, 호스트 A의 MAC 주소, 및 호스트 A가 연결된 스위치 A의 포트 주소 중 적어도 하나를 포함할 수 있다. 한편, 상기에서 설명한 바와 같이 호스트 프로파일이 저장될 수 있으며, 호스트 프로파일에는 IP 주소, MAC 주소, DPID(Diagnostic Provider ID), 각 호스트(330)과 연결된 스위치(320)에 대한 포트 번호, 최종 타임스탬프 등이 포함된다.

[0041] 다음으로, 단계(620)에서, 포트 매니저(311)는 주소 정보 메시지 내의 주소 정보 및 호스트 프로파일에 저장된 이전 주소 정보를 추출한다.

[0042] 즉, 포트 매니저(311)는 주소 정보 메시지 내의 호스트 A의 IP 주소 및 호스트 A의 스위치 A의 포트 주소를 추출하며, 호스트 A의 IP 주소와 동일한 IP 주소를 사용하는 호스트 B가 호스트 프로파일에 저장되어 있는 경우 호스트 B가 연결된 스위치 B의 포트 주소를 검색한다.

[0043] 계속하여, 단계(630)에서, 호스트 프로빙(312)는 호스트 B가 연결된 스위치 B로 검사 메시지를 전송하고 검사 메시지와 대응되는 응답 메시지가 기 설정된 시간 내에 수신되는지 여부를 판단한다.

[0044] 즉, 호스트 프로빙(312)는 호스트 A의 이전 주소 정보인 호스트 B의 주소로 검사 메시지를 전송하고, 호스트 B로부터 응답 메시지가 수신되는지 여부를 판단한다. 검사 메시지는 호스트 B의 가용성 여부(네트워크에 연결되어 어떤 동작을 수행하는지 여부)를 판단하기 위한 메시지일 수 있으며, 예를 들어, ICMP Echo Request일 수 있다.

[0045] 그 후, 단계(640)에서, 호스트 체커(313)는 응답 메시지가 기 설정된 시간 내에 스위치 B를 통해 호스트 B에서 수신되는 경우 호스트 A가 호스트 B를 사칭하는 것으로 판단한다.

[0046] 즉, 응답 메시지가 기 설정된 시간 내에 수신되지 않는 경우, 호스트 B는 소프트웨어 정의 네트워크(300)에서 연결이 끊어진 호스트일 수 있다. 따라서, 호스트 B은 호스트 A와 동일한 호스트일 수 있으며(일례로, 호스트 B가 호스트 A의 위치로 이동함), 이 경우 호스트 추적 서비스에 대한 공격이 수행되지 않을 수 있다.

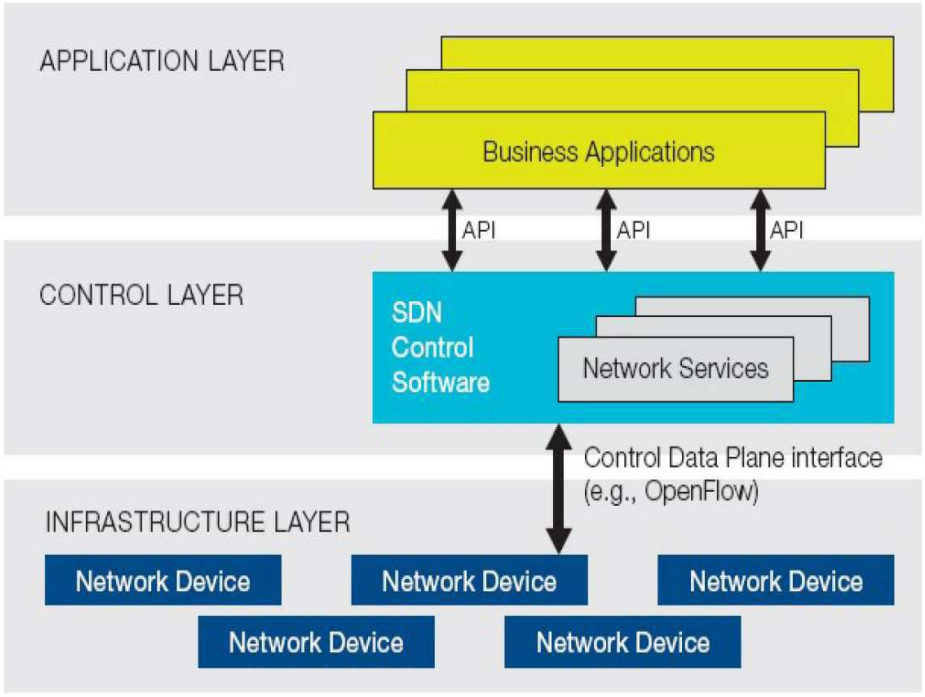
[0047] 반대로, 응답 메시지가 기 설정된 시간 내에 수신되는 경우, 호스트 B는 소프트웨어 정의 네트워크(300)에서 연결된 호스트이며, 따라서 동일한 IP 주소를 가지는 2개의 호스트(호스트 A, 호스트 B)가 소프트웨어 정의 네트워크(300) 상에 존재한다. 따라서, 이전 주소에 위치한 호스트 B가 정당한 호스트이고, 새로운 주소에 위치한 호스트 A가 공격자의 호스트일 수 있다. 이에 따라, 컨트롤러(320)는 악의적인 호스트 A에 대한 소프트웨어 정의 네트워크(300)의 연결을 차단할 수 있으며, 호스트 추적 서비스에 대한 공격을 방지할 수 있다.

[0048] 요컨대, 본 발명의 일 실시예에 따른 컨트롤러(320)는 특정 호스트에서 수신된 주소 정보 메시지와 컨트롤러(320)에 저장된 호스트의 이전 주소 정보를 이용하여 특정 호스트가 호스트 추적 시스템에 대한 공격을 수행하는 호스트인지 여부를 판단할 수 있다.

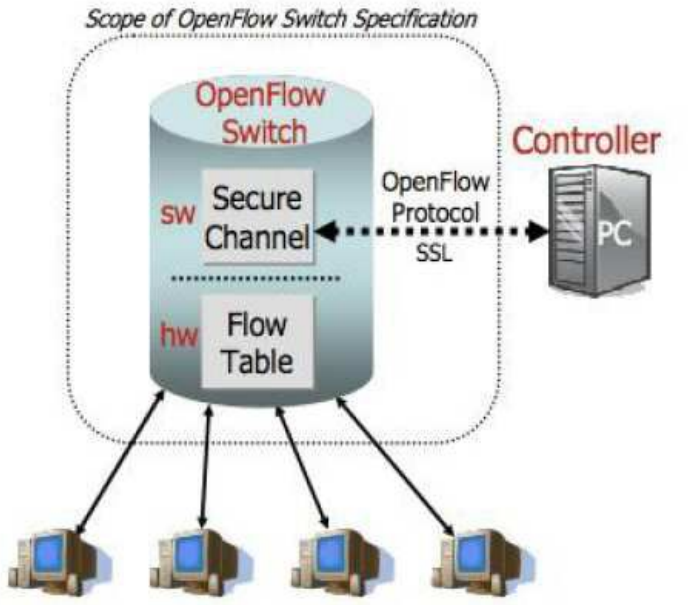
[0049] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

도면

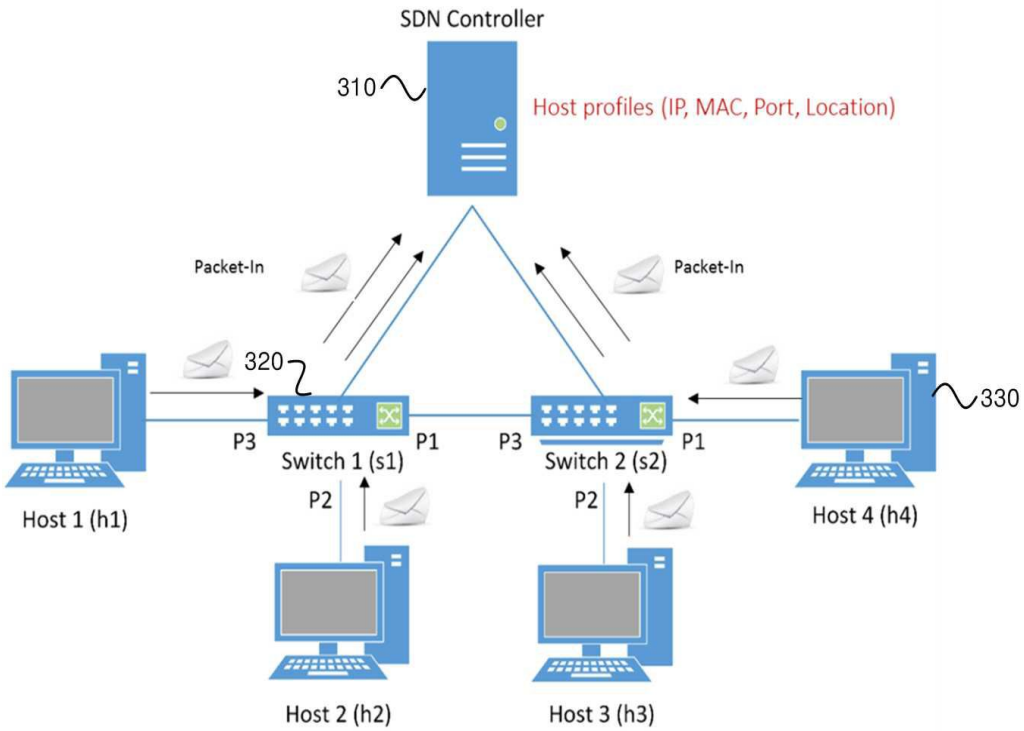
도면1



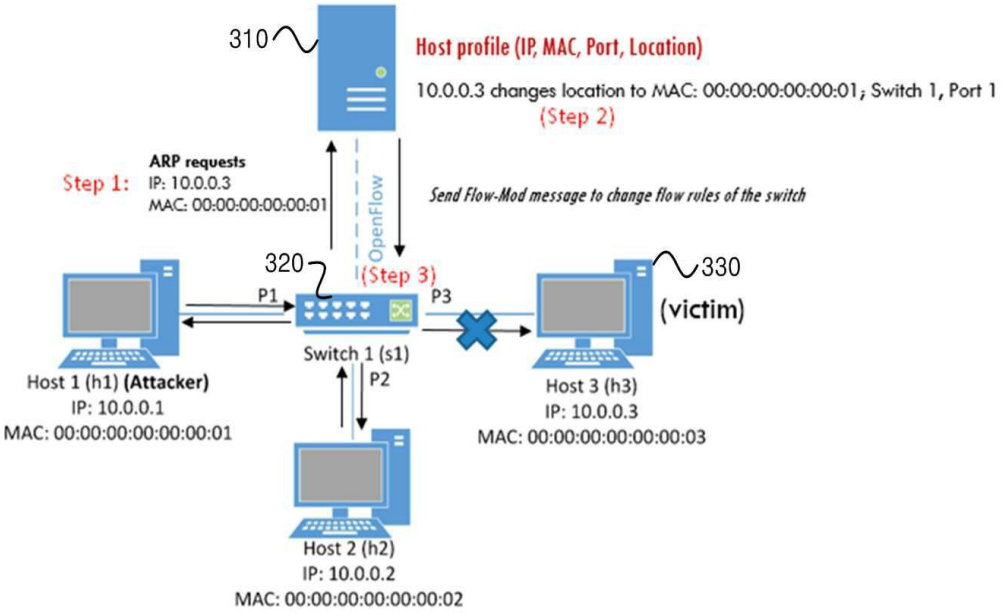
도면2


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

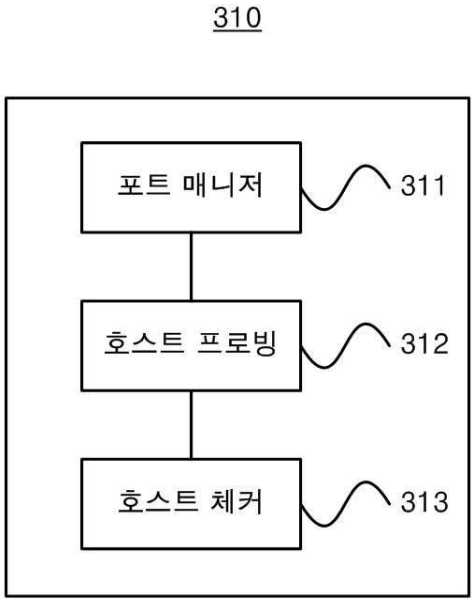
도면3


SDN Controller
310
Host profiles (IP, MAC, Port, Location)
Packet-In
Packet-In
320
330
P3
P1
Switch 1 (s1)
P3
P1
Switch 2 (s2)
P2
P2
Host 1 (h1)
Host 4 (h4)
Host 2 (h2)
Host 3 (h3)

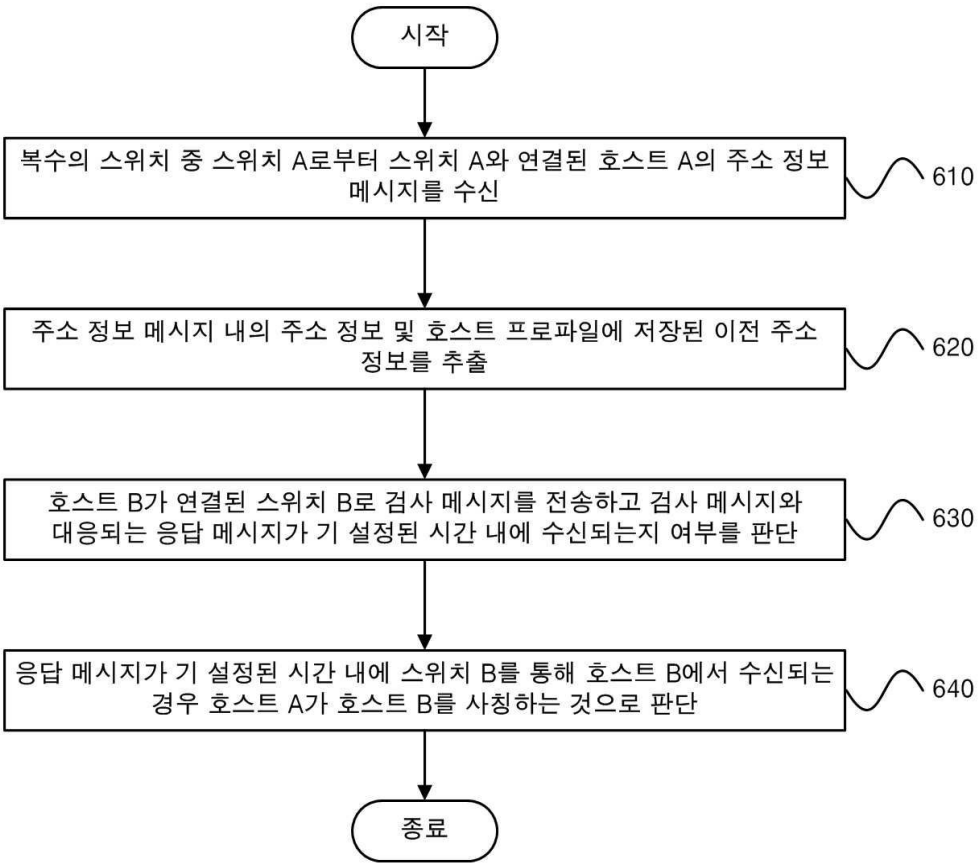
도면4


310
Host profile (IP, MAC, Port, Location)
10.0.0.3 changes location to MAC: 00:00:00:00:00:01; Switch 1, Port 1
(Step 2)
ARP requests
Step 1: IP: 10.0.0.3
MAC: 00:00:00:00:00:01
OpenFlow
Send Flow-Mod message to change flow rules of the switch
320
(Step 3)
P1
P3
P2
Switch 1 (s1)
330
(victim)
Host 1 (h1) (Attacker)
IP: 10.0.0.1
MAC: 00:00:00:00:00:00:01
Host 3 (h3)
IP: 10.0.0.3
MAC: 00:00:00:00:00:00:03
Host 2 (h2)
IP: 10.0.0.2
MAC: 00:00:00:00:00:00:02

도면5


310
포트 매니저
311
호스트 프로빙
312
호스트 체커
313

도면6


시작
복수의 스위치 중 스위치 A로부터 스위치 A와 연결된 호스트 A의 주소 정보 메시지를 수신
610
주소 정보 메시지 내의 주소 정보 및 호스트 프로파일에 저장된 이전 주소 정보를 추출
620
호스트 B가 연결된 스위치 B로 검사 메시지를 전송하고 검사 메시지와 대응되는 응답 메시지가 기 설정된 시간 내에 수신되는지 여부를 판단
630
응답 메시지가 기 설정된 시간 내에 스위치 B를 통해 호스트 B에서 수신되는 경우 호스트 A가 호스트 B를 사칭하는 것으로 판단
640
종료