(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0074342
(43) 공개일자 2016년06월28일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01)
(21) 출원번호 10-2014-0183589
(22) 출원일자 2014년12월18일
심사청구일자 2014년12월18일

(71) 출원인
광주과학기술원
광주광역시 북구 첨단과기로 123 (오룡동)
(72) 발명자
임혁
광주광역시 북구 첨단과기로 123(오룡동) 광주과학기술원 정보통신공학부
김종원
광주광역시 북구 첨단과기로 123(오룡동) 광주과학기술원 정보통신공학부
(뒷면에 계속)
(74) 대리인
김기문

전체 청구항 수 : 총 9 항

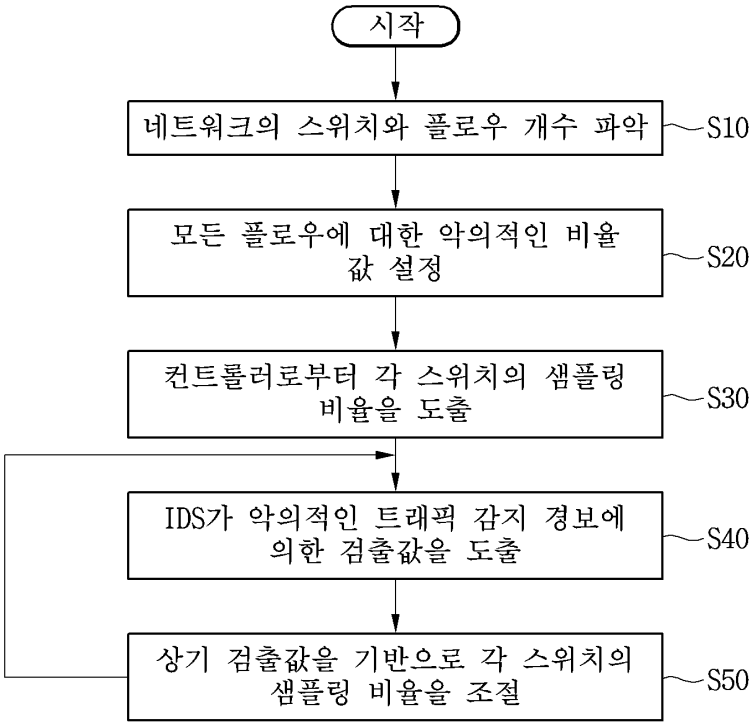
(54) 발명의 명칭 **네트워크에서의 침입 탐지 방법**

(57) 요 약

본 발명의 실시예는, 데이터를 송수신하는 복수개의 노드와, 상기 노드 간의 플로우 송수신을 중계하는 스위치로 구성된 네트워크와 IDS(Intrusion Detection System)가 결합된 시스템에서 공격 데이터를 탐지하는 방법으로서, 상기 네트워크 플로우 샘플링을 위한 SDN 지원 스위치를 설치하고 SDN 컨트롤러와 연동하는 단계, 상기 SDN 컨트

(뒷면에 계속)

대 표 도 - 도3



롤러를 통해 네트워크 플로우와 스위치의 갯수를 파악하는 단계, 상기 SDN 지원 스위치 각각의 샘플링 비율을 도출하는 단계, 상기 스위치가 샘플링 비율만큼의 패킷 정보를 상기 IDS로 전송하는 단계, 상기 IDS는 상기 패킷 정보에 따라 악의적인 데이터를 판별하고, 상기 각각의 SDN 지원 스위치에 대한 샘플링 비율을 갱신하는 단계를 포함할 수 있다. 따라서, 본 실시예는 기존의 네트워크에 SDN을 지원하는 스위치를 설치하고 SDN 컨트롤러와 연동함으로써, 특정 위치에 마련된 IDS에서 네트워크 전체 트래픽에 대해 공격 데이타의 유무를 검사할 수 있어 효율적으로 네트워크에 대한 감시를 수행할 수 있다.

(72) 발명자

자르갈사이흥 나랑토야

광주광역시 북구 첨단과기로123 광주과학기술원 생활관 4201호

하태진

광주광역시 북구 첨단과기로 123(오룡동) 광주과학기술원 정보기전공학부

정치욱

광주광역시 북구 첨단과기로 123(오룡동) 광주과학기술원 정보기전공학부

이 발명을 지원한 국가연구개발사업

과제고유번호 GM07140
부처명 산업통상자원부
연구관리전문기관 (주)넷비젼텔레콤
연구사업명 산업기술혁신사업
연구과제명 SDN 기반의 침입 대응을 위한 홈 게이트웨이 개발
기 여 율 1/2
주관기관 (주)넷비젼텔레콤
연구기간 2013.09.01 ~ 2014.12.31이 발명을 지원한 국가연구개발사업
과제고유번호 NN12680
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 중견연구자지원사업(핵심)
연구과제명 전이중 및 다중패킷 수신 차세대 무선랜을 위한 매체접근제어 기술 연구 및 Software Defined Radio (SDR) 기반 테스트베드 구축
기 여 율 1/2
주관기관 광주과학기술원
연구기간 2014.05.01 ~ 2015.04.30

명 세 서

청구범위

청구항 1

데이터를 송수신하는 복수개의 노드와, 상기 노드 간의 플로우 송수신을 중계하는 스위치로 구성된 네트워크와 IDS(Intrusion Detection System)가 결합된 시스템에서 공격 데이터를 탐지하는 방법으로서,

상기 네트워크에 플로우 샘플링을 위한 SDN 지원 스위치를 설치하고 SDN 컨트롤러와 연동하는 단계;

상기 SDN 컨트롤러를 통해 네트워크 플로우와 스위치의 갯수를 파악하는 단계;

상기 SDN 지원 스위치 각각의 샘플링 비율을 도출하는 단계;

상기 스위치가 샘플링 비율만큼의 패킷 정보를 상기 IDS로 전송하는 단계;

상기 IDS는 상기 패킷 정보에 따라 악의적인 데이터를 판별하고, 상기 각각의 SDN 지원 스위치에 대한 샘플링 비율을 갱신하는 단계;

를 포함하는 네트워크에서의 침입 탐지 방법.

청구항 2

제 1항에 있어서,

상기 SDN 지원 컨트롤러를 통해 네트워크 플로우와 스위치의 갯수를 파악하는 단계 이후에,

IDS의 처리량이 일정한 값으로 주어진 상태에서, 상기 네트워크 플로우의 전송률과 경로 정보를 도출하는 단계를 포함하는 네트워크에서의 침입 탐지 방법.

청구항 3

제 1항에 있어서,

상기 SDN 지원 스위치 각각의 샘플링 비율을 도출하는 단계는,

상기 각각의 네트워크 플로우에 대해 악의적인 공격이 일어날 비율의 초기값을 설정하는 단계를 포함하는 네트워크에서의 침입 탐지 방법.

청구항 4

제 3항에 있어서,

상기 각각의 네트워크 플로우에 대해 악의적인 공격이 일어날 비율의 초기값으로 상기 IDS에서 악의적인 공격에 대한 결손률의 최대값을 최소화하는 함수인 M(x)를 도출하는 단계를 더 포함하는 네트워크에서의 침입 탐지 방법.

청구항 5

제 4항에 있어서,

상기 함수인 M(x)를 통해서 초기 샘플링 비율값을 도출하여, 상기 SDN 컨트롤러로부터 상기 스위치로 플로우 테이블을 형성하여 각각의 스위치에 대한 샘플링 비율값을 도출하는 네트워크에서의 침입 탐지 방법.

청구항 6

제 5항에 있어서,

상기 각각의 스위치는 상기 플로우 테이블에 포함된 SDN 컨트롤러 갯수만큼 상기 IDS로 데이터 패킷을 전송하는 네트워크에서의 침입 탐지 방법.

청구항 7

제 1항에 있어서,

상기 IDS는 상기 패킷 정보에 따라 악의적인 데이터를 판별하고, 상기 각각의 SDN 지원 스위치에 대한 샘플링 비율을 갱신하는 단계는,

상기 IDS가 악의적인 트래픽을 감지하는 경우 이에 대한 감지 경보를 발생하여 악의적인 트래픽에 대해 악의적인 공격이 나타날 비율을 도출하는 단계를 포함하는 네트워크에서의 침입 탐지 방법.

청구항 8

제 7항에 있어서,

상기 IDS가 도출한 악의적인 공격이 나타날 비율을 통해, 각 플로우에서 악의적인 공격이 나타날 비율을 추정하는 단계를 포함하는 네트워크에서의 침입 탐지 방법.

청구항 9

제 8항에 있어서,

상기 각 플로우에서 악의적인 공격이 나타날 비율은 상기 IDS에 의해 반복적으로 추정되면서, 소정의 횟수만큼의 평균값으로 상기 플로우에 대한 악의적인 공격이 나타날 비율을 설정한 후에 각 스위치에 대한 샘플링 비율을 도출하는 네트워크에서의 침입 탐지 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 네트워크에서의 침입 탐지 방법에 관한 것으로, 보다 구체적으로는 기존 네트워크에 SDN 장비를 추가하고, 각 스위치에서의 샘플링 비율을 변경하여 네트워크 전체에 대한 검사를 수행할 수 있는 침입 탐지 방법에 관한 것이다.

배 경 기 술

[0002] 컴퓨터를 통한 소프트웨어 기반의 네트워크는 데이터 송신, 온라인 송금, 위치 추적 시스템과 같은 인터넷 서비스를 기반으로 급속도로 발전하고 있으며, 클라우드 데이터 시스템은 현재 많은 사람들에게 필수적인 부분이 되어가고 있다. 네트워크의 규모가 급속하게 방대해짐에 따라 사생활과 안전을 침해하는 보안 위협과 같은 네트워크 내의 공격 또한 나날이 증가하고 있어, 공격에 대한 침입 탐지가 더욱 복잡해지고 어려워지는 실정에 있다.

[0003] 이에, 보안이 철처하고 사용자에게 신뢰성을 주는 네트워크를 구축하기 위해서, 네트워크 상에서 악의적인 트래픽을 감지하여 차단하는 시스템의 개발이 큰 이슈가 되고 있다. 침입 탐지 시스템(Intrusion Detection System, IDS)은 네트워크 상의 흐름을 파악하여, 데이터 패킷을 검사하여 악의적인 의도가 있는지에 대해 검사한다. 종래 IDS는 수동 모드와 직렬 모드의 두가지 모드로 수행되었는데, 수동 모드에서 IDS는 하나의 노드에 종속되어 네트워크에 연결되고 상기 노드로부터 데이터 패킷을 받아 검사한다. 반면에, 직렬 모드에서 IDS는 네트워크에서 노드의 한 부분에 배치되고, 임의 링크에 위치하게 되며 상기 링크를 통해 데이타의 흐름을 분석한다.

[0004] 그러나, 악의적인 트래픽의 경로를 예측하여 이에 해당하는 네트워크 트래픽에 IDS를 배치하는 것은 거의 불가능하기에, IDS는 통상적으로 네트워크가 많이 맞물려있는 노드에 배치된다. 그러나, 네트워크의 규모가 커짐에 따라 IDS를 배치할 위치를 결정하기가 매우 어려워지게 되며, 많은 양의 감시를 수행하기 위해 많은 IDS가 필요로 하게 되므로 이를 위해 네트워크 트래픽 샘플링 방법이 제안되었다.

[0005] 공격 감지를 위한 트래픽 샘플링은 네트워크 트래픽을 부분적으로 관찰하고 샘플된 트래픽에 대한 감시를 수행하는 방법이지만, 샘플링 과정에서 악의적인 패킷이 포함된 트래픽에 대한 감시가 건너뛰어질 가능성이 있기에 악의적인 트래픽을 효과적으로 감지하기 위한 네트워크 트래픽 샘플링 방법이 요구되고 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 상술한 문제점을 해결하기 위해 제안되는 것으로서, 네트워크에 구빈된 스위치에서의 샘플링 비율 변경을 통해 특정 위치에 있는 IDS로 보내줌으로써, 전체 네트워크에 대한 검사를 수행할 수 있는 네트워크 환경에서의 침입 탐지 방법을 제공하는 것을 목적으로 한다.

[0007] 본 발명은 악의적인 공격을 포함한 패킷이 스위치에서 IDS로 전송시 결손되는 것을 최소화하는 것을 목표로 하며, 기존 네트워크에 SDN 연동 가능한 장비를 추가하여 공격 탐지 기능이 향상된 네트워크의 침입 탐지 방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0008] 본 발명의 실시예는 데이터를 송수신하는 복수개의 노드와, 상기 노드 간의 플로우 송수신을 중계하는 스위치로 구성된 네트워크와 IDS(Intrusion Detection System)가 결합된 네트워크에서의 침입 탐지 방법으로서, 상기 네트워크에 플로우 샘플링을 위한 SDN 지원 스위치를 설치하고 SDN 컨트롤러와 연동하는 단계; 상기 SDN 컨트롤러를 통해 네트워크 플로우와 스위치의 갯수를 파악하는 단계; 상기 SDN 지원 스위치 각각의 샘플링 비율을 도출하는 단계; 상기 SDN 지원 스위치가 샘플링 비율만큼의 패킷 정보를 상기 IDS로 전송하는 단계; 상기 IDS는 상기 패킷 정보에 따라 악의적인 데이터를 판별하고, 상기 각각의 SDN 지원 스위치에 대한 샘플링 비율을 갱신하는 단계;를 포함할 수 있다.

발명의 효과

[0009] 본 발명의 실시예에 따르면, 기존 네트워크에 SDN이 지원 가능한 스위치 및 컨트롤러를 추가로 구성하여 이를 연동시킴으로써, 네트워크 전체에 대해 공격에 대한 탐지를 수행할 수 있어 네트워크 전체에 대한 모니터링을 수행할 수 있고 네트워크 보안을 더욱 강화시킬 수 있다.

[0010] 본 발명의 실시예에 따르면, 특정 위치에 마련된 IDS에서 네트워크 전체 트래픽에 대해 공격 데이타의 유무를 검사할 수 있어 보다 효율적으로 네트워크의 보안을 강화할 수 있다.

[0011] 본 발명의 실시예에 따르면, IDS에서 수행된 검사결과를 이용하여 의심되는 트래픽에 대해 집중적인 검사를 수행하도록 네트워크를 설정할 수 있다.

[0012] 본 발명의 실시예에 따르면, IDS 장비가 네트워크에 추가되어도 샘플링하는 알고리즘의 수정없이 그대로 검사를 실시할 수 있고, 기존의 네트워크에 SDN 장비를 추가함으로써 샘플링을 통한 네트워크 전체의 모니터링 및 공격 탐지가 가능해져 시스템의 크기를 크게 확장시키지 않고도 네트워크의 신뢰성을 확보할 수 있으며 시스템 설계 비용 또한 크게 감소시킬 수 있다.

도면의 간단한 설명

[0013] 도 1은 SDN의 구조와 오픈플로우(Openflow)를 나타낸 개념도

도 2는 본 발명의 실시예에 따라 트래픽 샘플링을 실시하기 위한 SDN 기반 네트워크에 IDS가 마련된 시스템의 예시를 나타낸 도면

도 3은 본 발명의 실시예에 따라 트래픽 샘플링을 실시하는 방법을 나타내는 흐름도

도 4는 종래와 본 발명의 네트워크에서의 결손 비율을 비교한 그래프

발명을 실시하기 위한 구체적인 내용

[0014] 이하 첨부된 도면들을 참조하여 본 발명의 실시예들을 상세하게 설명하지만, 본 발명의 실시예에 의해 제한되거나 한정되는 것은 아니다. 본 발명을 설명함에 있어서, 공지된 기능 혹은 구성에 대해 구체적인 설명은 본 발명의 요지를 명료하게 하기 위해 생략될 수 있다.

[0015] 본 발명은 네트워크의 특정 위치에 마련된 IDS에서 트래픽 샘플링을 수행하여 네트워크 전체에 대한 공격을 감지하기 위해 SDN(Software Defined Networking) 구조를 접목하였다. SDN은 네트워크 장비, 즉 하드웨어 기능을

소프트웨어로 구현할 수 있는 일종의 가상화 기술을 말한다.

[0016] 도 1은 SDN의 구조와 오픈플로우(Openflow)를 나타낸 블록도이다. 도 1을 참조하면, 네트워크를 어플리케이션과 네트워크 운영체제로 하여 소프트웨어 계층을 하나 구성하고, 레이어와 하드웨어를 하나의 하드웨어 계층으로 보았을 때, 이 전체를 SDN이라 하며 하드웨어 레이어와의 접합 지점에 위치하는 것이 오픈플로우(Openflow)라 할 수 있다.

[0017] 오픈플로우 기반의 SDN 시스템은 복수개의 오픈플로우 스위치와 이를 제어하기 위한 오픈플로우 컨트롤러로 구성된다. 오픈플로우 컨트롤러는 수신 패킷을 처리하기 위한 플로우 제어 정보(출력 포트, QoS 등)를 제공하며, 오픈플로우 스위치는 오픈플로우 컨트롤러에서 제공되는 플로우 제어 정보에 따라 패킷을 처리한다.

[0018] 일반적으로 오픈플로우(OpenFlow) 스위치는 플로우 제어 정보를 저장하기 위해서 오픈플로우(OpenFlow) 테이블을 가지고 있다. 오픈플로우(OpenFolw) 스위치는 오픈플로우(Openfolw) 테이블에 등록되어 있는 플로우에 해당하는 패킷을 수신하면, 플로우 제어 정보에 따라 패킷을 처리한다.

[0019] 한편, 오픈플로우(OpenFlow) 스위치는 오픈플로우(OpenFlow) 테이블에 등록되어 있지 않는 플로우에 해당하는 패킷을 수신하는 경우에는 플로우 제어 정보가 없기 때문에 오픈플로우(OpenFlow) 컨트롤러로 전달한다. 오픈플로우(OpenFlow) 컨트롤러는 패킷을 분석하여 플로우 제어 정보를 생성하고 패킷과 함께 오픈플로우(OpenFlow) 스위치로 전달하며, 오픈플로우(OpenFlow) 스위치는 전달받은 플로우 제어 정보를 오픈플로우(OpenFlow) 테이블에 저장하고 패킷을 처리한다.

[0020] 도 2는 본 발명의 실시예에 따라 네트워크 상에서 트래픽 샘플링을 실시하기 시스템을 나타낸 도면이다.

[0021] 도 2를 참조하면, 실시예의 네트워크 시스템은 SDN 컨트롤러(20), Openflow(OF) 가능한 스위치(30) 및 IDS(Intrusion Detection System, 10)가 접목된 SDN을 기반으로 한 구조의 네트워크 시스템이다. 본 발명은 SDN 기반의 시스템에서 수행되는 것이지만, 기존의 네트워크에 SDN 장비를 일부 설치하여 이를 기존의 스위치 및 컨트롤러와 연동하여 수행될 수 있다. 하기에서 언급되는 스위치는 SDN과 연동된 SDN 지원 스위치인 것으로 해석될 수 있다.

[0022] SDN 컨트롤러(20)는 제어 영역에 오픈플로우 가능한 스위치(30)를 구비하여, 각각의 스위치(30)에서 데이터 흐름을 감지할 수 있다. 그리고, 상기 SDN 컨트롤러(20)에는 샘플링 비율을 결정하기 위한 알고리즘이 내장된다. 오픈플로우는 상기 SDN 컨트롤러(20)가 상기 스위치(30)에 배당되는 테이블에 엑세스할 수 있도록 상호소통하는 네트워킹 프로토콜이다.

[0023] 각각의 오픈플로우 가능한 스위치(30)는 SDN 컨트롤러(20)에 의해 결정된 샘플링 비율에 따라 데이터 패킷을 전송한다. 그리고, 상기 IDS(10)는 상기 스위치(30)에서 전송된 모든 데이터 패킷에 대한 감시를 수행하고, 의심스러운 패킷 또는 공격이 감지된 경우에 알람을 발생시키며, 이는 SDN 컨트롤러(20)에 의해 접근될 수 있다.

[0024] IDS(10)와 각 스위치(30)의 현재 상태의 감시 결과에 따라 조사된 데이터를 기초로, SDN 컨트롤러(20)는 각각의 스위치(30)에 대해 최적의 샘플링 비율을 도출한다. 상기 스위치(30)의 샘플링 비율을 결정하는 알고리즘은 의심되는 트래픽의 감지가 결손되는 비율을 최소화하면서, 전체 샘플링된 플로우의 양이 IDS(10)의 최대 감시 용량보다 낮도록 유지된다.

[0025] 실시예에 따른 네트워크에서의 침입 탐지 시스템은 SDN을 기반으로 한 네트워크이거나 기존의 네트워크에 SDN 호환이 가능한 스위치(라우터) 등을 설치한 네트워크에서 활용될 수 있다. 즉, 종래 모든 스위치에서 동일한 값으로 샘플링을 실시한 점에 비해서, 본 발명에서는 SDN 컨트롤러를 통해 네트워크 상에 배치된 각각의 스위치(30)에 대한 샘플링 비율을 도출한다. 따라서, IDS가 임의의 위치에 배치되어 있는 경우에도 네트워크 전체 트래픽에 대한 검사를 실시할 수 있다.

[0026] 도 3은 본 발명의 실시예에 따라 트래픽 샘플링을 실시하는 방법을 나타내는 흐름도이다. 도 3을 참조하여, 구체적으로 본 발명의 샘플링 비율을 설정하는 방법을 살펴보기로 한다.

[0027] 우선 본 발명은 데이터를 송수신하는 복수개의 노드와, 상기 노드 간의 플로우 송수신을 중계하는 스위치로 구성된 네트워크와 IDS가 결합된 시스템에서 수행될 수 있다. 실시예에서는 상기 네트워크에 플로우 샘플링을 위해 SDN 지원 스위치를 설치하고 이를 SDN 컨트롤러와 연동하는 단계가 선행될 수 있다.

[0028] 실시예에 따른 트래픽 샘플링을 수행하는 방법은 우선, 네트워크에 배치된 스위치와 플로우의 개수를 파악하는 단계를 수행한다(S10).

[0029] 구체적으로, 네트워크 상에 f개의 플로우와 n개의 스위치가 있다고 가정한다. i와 j를 상기 플로우와 스위치를 나타내는 문자로 정의하면, i={1,..f}, j={1,..n}으로 나타내어진다. 이 때, λ를 악의적인 공격이 나타나는 비율로 정의하면, 각각의 플로우는 특정한 악의적인 공격 비율을 가진다고 가정한다. 만약 어떤 플로우가 악의적인 패킷을 포함하고 있지 않다면, 악의적인 공격 비율은 0이 된다. 플로우의 전송률은 전송 비율 벡터 $s=\{s_1,...s_f\}$로 정의되고, 악의적인 플로우의 비율은 $\lambda=\{\lambda_1,...\lambda_f\}$로 정의된다. 플로우의 전송 비율과 악의적인 공격 비율의 단위는 초당 패킷의 수(pps)로 계산될 수 있다.

[0030] 상술한 바와 같이, 각 스위치의 플로우 위치는 SDN 컨트롤러에 의해서 파악할 수 있다. 이 정보를 통해서 기존 네트워크의 루팅 테이블과 같은 플로우 경로 정보인 매트릭스 A를 도출할 수 있다. 플로우 경로 정보 매트릭스 A는 f행과 n열을 갖는 매트릭스이며, 구성인자인 $a_{i,j}$ 는 i번째 플로우가 j번째 스위치를 통과할 때만 1을 나타내고, 나머지는 0을 나타낸다. 상기 플로우의 전송율 s와 각 플로우의 경로 정보 매트릭스 A를 통해서, 스위치의 전송률인 $b = s \cdot A$ 와 같이 나타내어지며, b_j는 j번째 스위치의 전송률을 나타낸다.

[0031] 패킷의 샘플링은 각 스위치의 샘플링 비율에 따라 상기 스위치들에서 수행될 수 있다. 샘플링 비율 벡터는 x로 표현되며, 인자인 x_j는 j번째 스위치의 샘플링 비율을 나타낸다. $x=\{x_1,...x_n\}$, $0 \le x_j \le 1$ 여기서, 만약 x_j가 1이라면, j번째 스위치를 지나는 모든 패킷은 샘플링되어 IDS로 전송된다.

[0032] 이어서, 모든 플로우에 대한 악의적인 공격이 나타나는 비율값을 설정하는 단계(S20)를 수행한다.

[0033] 통상적으로 위험 감지를 위한 단어로, 부정 오류율(false negative rate)이 두루 쓰이고 있다. 부정 오류는 IDS가 공격이 발생함에도 불구하고 어떠한 의심스런 공격을 감지하지 못하는 것을 의미한다. 부정 오류율은 간단히 말해서, 결손률이라 해석될 수 있으며, IDS의 관점에서 결손의 의미는 공격의 존재를 알지 못하는 것으로 이해될 수 있다. 데이터 패킷의 조사과정에서 의심스러운 패킷이 샘플링되지 않는다면, IDS가 공격의 존재를 누락한 것으로 생각될 수 있다. 즉, IDS의 성능은 상기 결손률에 의해 나타내어질 수 있다.

[0034] 각 플로우는 공격 존재율을 가지며 모든 플로우는 잠재적으로 악의적인 플로우를 내포하고 있다고 생각할 수 있다. 하나의 플로우는 목적지에 도착하기 위해 여러개의 스위치를 거쳐간다. 만약, IDS에서 악의적인 목적의 패킷이 감지되지 않는다면, 모든 스위치에서 악의적인 패킷이 포함된 플로우가 샘플링되지 않아야 한다. 따라서, 모든 플로우에 대해서 악의적인 공격 비율을 나타내는 벡터를 λ으로 설정한다. $\lambda=\{\lambda_1,\lambda_2,...\lambda_f\}$ 이며, i번째 벡터는 $\lambda_i=\eta$ 으로 표현된다. 상기 λ의 초기값은 모든 플로우에서 동일할 수 있다.

[0035] 이어서, 컨트롤러로부터 각 스위치의 샘플링 비율을 도출하는 단계(S30)를 수행한다. 상술한 바와 같은 플로우의 악의적인 공격 비율을 사용하여, 악의적인 공격에 대한 결손률의 최대값을 최소화하는 함수인 M(x)와 초기 샘플링 비율 벡터 x를 도출할 수 있다.

[0036] 공격 탐지의 시스템의 성능은 IDS에서 얼마나 많은 악의적인 의도가 담긴 데이터를 감지할 수 있는지에 달려있다. IDS로 전송되는 모든 악의적인 패킷들이 감지된다고 가정하면, 악의적인 공격이 포함된 트래픽의 결손율을 최소화하도록 샘플링 비율을 설정함으로써 공격 탐지 시스템의 성능을 강화시킬 수 있다. 따라서, SDN 컨트롤러로부터 스위치에 플로우 테이블을 배당하여 각각의 스위치에 대해 샘플링 비율을 설정할 수 있다.

[0037] S10 내지 S30 단계에서는 SDN 컨트롤러로부터 각각의 스위치에 대해 샘플링 비율을 설정하는 방법에 대해 설명하였다. 그러나, 플로우에 대해서 악의적인 공격 비율을 나타내는 벡터인 λ의 초기값은 모든 플로우에서 동일하게 설정되므로 이 값을 악의적인 공격이 발생하는 비율에 따라 최적화해줄 필요가 있다.

[0038] 따라서, S40 단계에서는 IDS가 악의적인 트래픽을 감지하는 경우에 경보를 발생하고, 감지 경보에 의한 검출값을 도출한다. 이 단계에서는, 각각의 악의적인 공격이 포함된 트래픽에 대해 악의적인 공격이 나타나는 비율을 계산한다. 각 플로우에 대해 IDS로 전송된 데이터 패킷을 계산하고, 임의의 플로우에서 감지된 악의적인 패킷의 양을 비교하여 악의적인 공격이 발생하는 비율을 계산하여 검출값을 업데이트한다. 그러나, 상기 검출값은 특정한 지점에서 악의적인 공격이 발생시의 초기값일 수 있어 신뢰도가 낮으므로, 임의의 값인 k번째까지의 평균값을 도출하여 악의적인 공격이 나타나는 비율을 최적화시킨다.

[0039] 이어서, 상기 검출값의 평균값을 기반으로 각 스위치의 샘플링 비율을 조절하는 단계(S50)을 수행한다. 상기 평균값에 의해 악의적인 공격이 나타나는 비율값이 재설정되면 악의적인 공격에 대한 결손률의 최대값을 최소화하는 함수인 M(x)를 재계산하고, 이에 대한 샘플링 비율 벡터인 x값을 계산할 수 있고, 샘플링 비율을 새롭게 설정할 수 있다. 상술한 바와 같이 악의적인 공격이 나타나는 비율의 재설정을 반복함에 따라서, 악의적인 공격이

나타나는 비율 벡터는 더욱 실제값과 유사하게 설정될 수 있다.

[0040] 즉, 상술한 바와 같이 본 실시예에서는 SDN 기반의 네트워크 상에서 SDN 컨트롤러를 사용하여 모든 지점의 트래픽을 샘플링할 수 있고 IDS로 전송할 수 있다. 즉, SDN 기반에서 IDS는 네트워크상에서 흐르는 모든 패킷에 대해 검사가 가능하다. 이에, 실시예는 각각의 스위치에 대한 샘플링 비율을 설정함으로써, 악의적인 공격에 대한 감지를 효과적으로 수행할 수 있다.

[0041] 도 4는 종래와 본 발명의 네트워크에서의 악의적인 공격의 결손률을 나타낸 그래프이며, (a)는 IDS의 처리량에 따른 결손율을 나타낸 것이고 (b)는 악의적인 트래픽의 비율에 따른 결손률을 나타낸 것이다.

[0042] 도 4의 (a)를 참조하면, 200개의 스위치로 구성된 네트워크에서 모든 스위치에 대해 동일하게 샘플링을 수행한 경우와, 각각의 스위치에 대해 본 발명의 실시예와 같이 샘플링 비율을 변경한 경우를 나타낸다. 모든 스위치에서 동일하게 샘플링(Fixed sampling)을 수행한 경우에는 결손률(missing rate)이 1에 근접하게 나타나며 0.7 이상의 값을 가짐을 알 수 있다. 이는 네트워크에 악의적인 공격이 발생했음에도 불구하고, 스위치에서 샘플링된 데이터 패킷이 악의적인 공격에 대한 패킷을 결손함으로써 IDS에서 공격에 대한 감지가 거의 이루어지지 않았음을 의미한다.

[0043] 그러나, 실시예와 같이 각각의 스위치에 대해 샘플링 비율을 변경(Proposed sampling)한 경우에는 악의적인 공격의 트래픽이 IDS로 전달될 확률이 높아짐에 따라서 악의적인 공격에 대한 결손률이 점차 0으로 수렴하는 것을 알 수 있다.

[0044] 도 4의 (b)를 참조하면, 종래와 같이 모든 스위치에서 동일하게 샘플링(Fixed sampling)을 수행한 경우에는 악의적인 트래픽의 비율이 증가함에 따라서 결손률이 서서히 감소하는 경향을 보이지만, 실시예와 같이 각 스위치에 대해 샘플링 비율을 변경(Proposed sampling)한 경우에는 결손율이 초기부터 0에 근접함을 확인할 수 있다.

[0045] 따라서, 도 4의 그래프를 토대로 실시예는 악의적인 공격에 대한 결손률을 최소화함으로써, 최대한 많은 수의 공격에 대한 감지를 수행할 수 있고 공격에 대한 탐지 성능이 기존의 시스템에 비해 우월함을 알 수 있다.

[0046] 상술한 바와 같이 본 발명은 모든 스위치의 샘플링 비율을 변경함으로써, 악의적인 패킷이 IDS로 전달될 확률을 높여 악의적인 공격에 대한 탐지 기능을 기존의 시스템에 비해 향상시킬 수 있다. 이는 기존의 네트워크 장비에 SDN을 지원하는 스위치 및 컨트롤러 등의 SDN 장비를 설치하여 연동시키는 일련의 과정을 통해서 용이하게 수행될 수 있다.

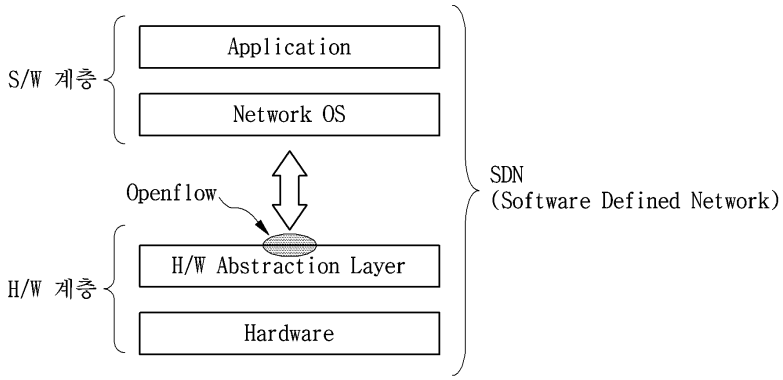
[0047] 따라서, 본 발명은 IDS의 갯수를 네트워크의 크기에 비례해서 증가시키지 않고도 특정 위치에 마련된 IDS에서 네트워크 전체 트래픽에 대해 공격 데이타의 유무를 검사할 수 있어 보다 효율적으로 네트워크에 대한 감시를 수행할 수 있다. 또한, IDS에서 수행된 검사결과를 이용하여 의심되는 트래픽에 대해 집중적인 검사를 수행하도록 네트워크를 설정할 수 있다.

[0048] 본 발명은 IDS 장비가 네트워크에 추가되어도 샘플링하는 알고리즘의 수정없이 그대로 검사를 실시할 수 있고, 기존의 네트워크에 SDN 장비를 추가함으로써 샘플링을 통한 네트워크 전체의 모니터링 및 공격 탐지가 가능해져 시스템의 크기를 크게 확장시키지 않고도 네트워크의 신뢰성을 확보할 수 있으며 시스템 설계 비용 또한 크게 감소시킬 수 있다.

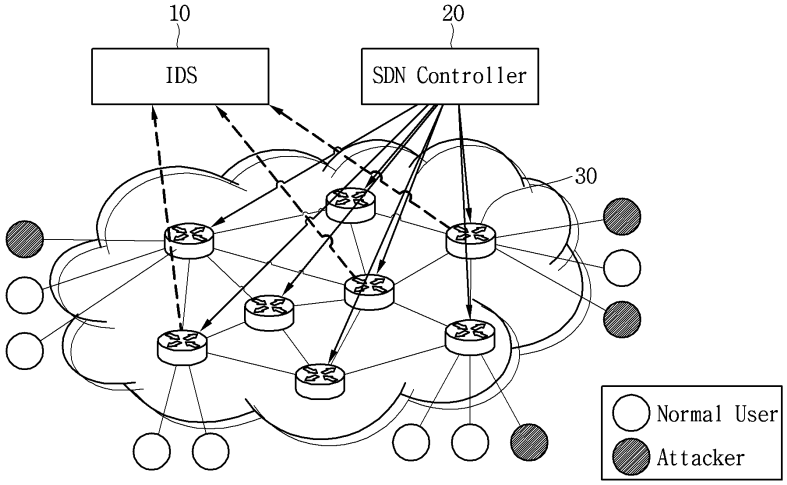
[0049] 이상에서 본 발명에 대하여 그 바람직한 실시예를 중심으로 설명하였으나 이는 단지 예시일 뿐 본 발명을 한정하는 것이 아니며, 본 발명이 속하는 분야의 통상의 지식을 가진 자라면 본 발명의 본질적인 특성을 벗어나지 않는 범위에서 이상에 예시되지 않은 여러 가지의 변형과 응용이 가능함을 알 수 있을 것이다. 예를 들어, 본 발명의 실시예에 구체적으로 나타난 각 구성 요소는 변형하여 실시할 수 있는 것이다. 그리고 이러한 변형과 응용에 관계된 차이점들은 첨부된 청구 범위에서 규정하는 본 발명의 범위에 포함되는 것으로 해석되어야 할 것이다.

도면

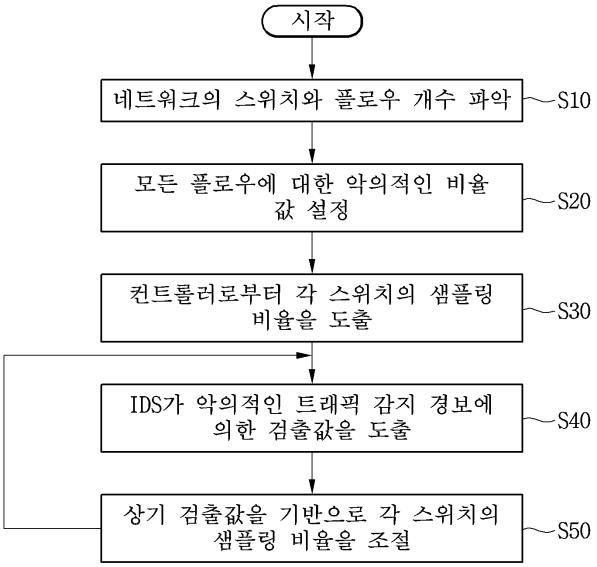
도면1



도면2

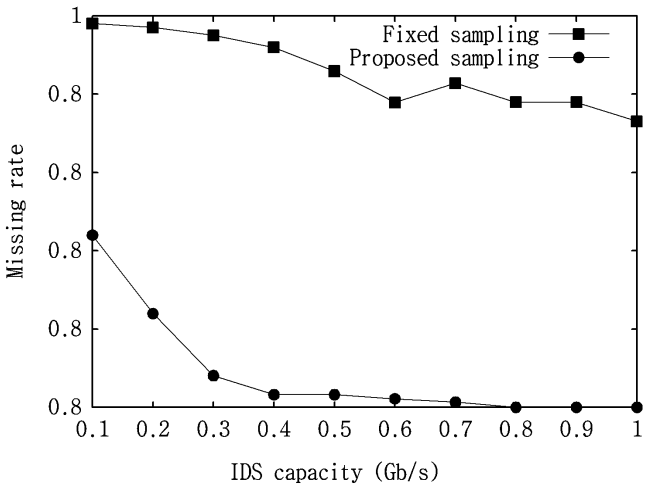


도면3

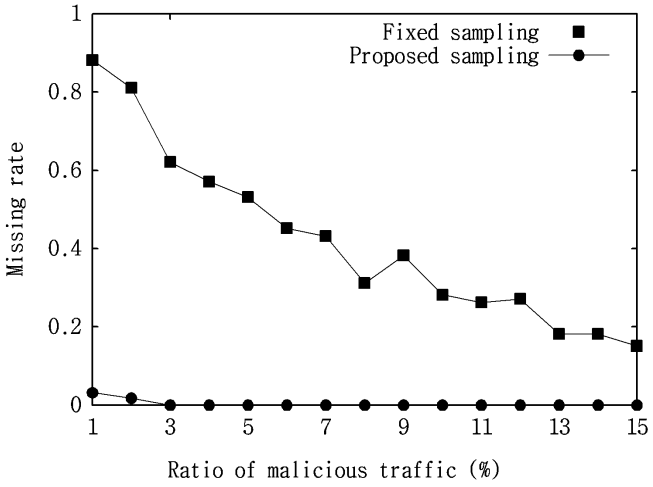


도면4

(a)


Fixed sampling
Proposed sampling
Missing rate
IDS capacity (Gb/s)
1
0.8
0.8
0.8
0.8
0.8
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

(b)


Fixed sampling
Proposed sampling
Missing rate
Ratio of malicious traffic (%)
1
0.8
0.6
0.4
0.2
0
1
3
5
7
9
11
13
15