



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2015년08월26일

(11) 등록번호 10-1547771

(24) 등록일자 2015년08월20일

(51) 국제특허분류(Int. Cl.)

H04L 12/26 (2006.01) H04L 12/701 (2013.01)

(21) 출원번호 10-2014-0107608

(22) 출원일자 2014년08월19일

심사청구일자 2014년08월19일

(56) 선행기술조사문헌

KR101409758 B1*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

경희대학교 산학협력단

경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)

(72) 발명자

홍충선

경기도 용인시 수지구 상현로 30-10 상현마을 성원상떼빌 233동101호 (상현동, 상현마을성원상떼빌아파트)

조웅준

경기도 용인시 기흥구 서천동로 60 402-1101

(74) 대리인

김연권

전체 청구항 수 : 총 9 항

심사관 : 전용해

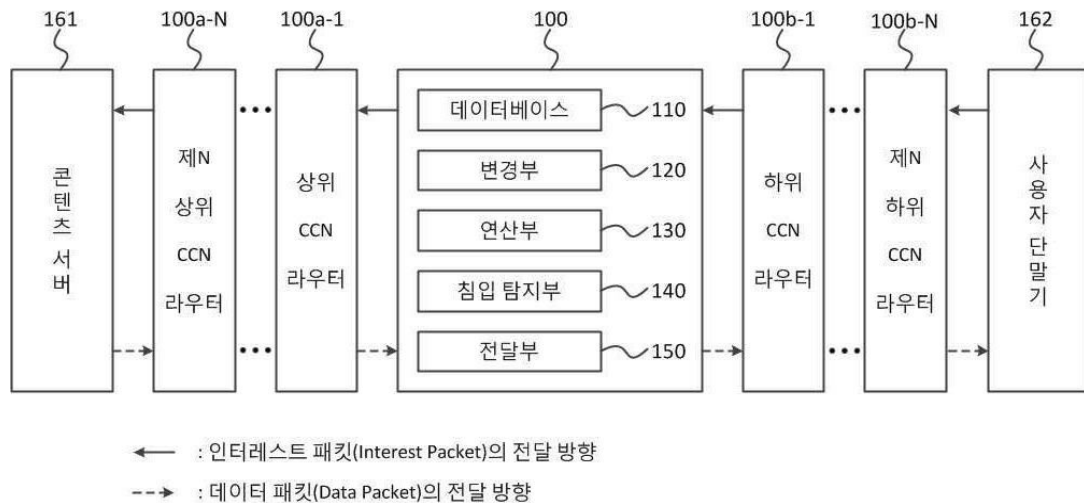
(54) 발명의 명칭 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템 및 방법

(57) 요약

본 발명은 콘텐츠 서버 및 상위 CCN(Content Centric Networking) 라우터 중 적어도 하나로부터 데이터 패킷(Data Packet)을 전달받는 CCN 라우터에 있어서, 상기 데이터 패킷의 악성코드 유무를 탐지하는 다중 분산 블룸필터 세트들, 하위 CCN 라우터로부터 전달 받은 인터레스트 패킷(Interest Packet)에 포함된 인터레스트 홉(Hop)

(뒷면에 계속)

대표도



카운터 수 및 상기 상위 라우터로부터 전달받은 데이터 패킷에 포함된 데이터 홉 카운터 수를 저장하는 데이터 베이스; 상기 인터레스트 홉 카운터 수와 상기 데이터 홉 카운터 수를 통하여 상기 다중 분산 블룸필터 세트들 중에서 블룸필터 세트를 선택하기 위한 연산과 상기 선택된 블룸필터 세트에서 블룸필터 배열을 선택하기 위한 연산을 수행하는 연산부; 상기 선택된 블룸필터 배열을 이용하여 상기 데이터 패킷의 상기 악성코드 유무를 탐지하는 침입 탐지부; 및 상기 탐지된 데이터 패킷에 대한 상기 악성코드가 없는 경우, 상기 탐지된 데이터 패킷을 상기 하위 CCN 라우터로 전달하는 전달부를 포함하는 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템 및 방법을 개시한다.

이 발명을 지원한 국가연구개발사업

과제고유번호	1711014131
부처명	미래창조과학부
연구관리전문기관	한국정보통신산업진흥원
연구사업명	대학ICT 연구센터육성 지원사업
연구과제명	실시간 모바일 클라우드 서비스 플랫폼 연구개발
기 여 율	1/1
주관기관	경희대학교 산학협력단
연구기간	2014.01.01 ~ 2014.12.31

특허청구의 범위

청구항 1

콘텐츠 서버 및 상위 CCN(Content Centric Networking) 라우터 중 적어도 하나로부터 데이터 패킷(Data Packet)을 전달받는 CCN 라우터에 있어서,

상기 데이터 패킷의 악성코드 유무를 탐지하는 다중 분산 블룸필터 세트들, 하위 CCN 라우터로부터 전달 받은 인터레스트 패킷(Interest Packet)에 포함된 인터레스트 홉(Hop) 카운터 수 및 상기 상위 라우터로부터 전달받은 데이터 패킷에 포함된 데이터 홉 카운터 수를 저장하는 데이터베이스;

상기 인터레스트 홉 카운터 수와 상기 데이터 홉 카운터 수를 통하여 상기 다중 분산 블룸필터 세트들 중에서 블룸필터 세트를 선택하기 위한 연산과 상기 선택된 블룸필터 세트에서 블룸필터 배열을 선택하기 위한 연산을 수행하는 연산부;

상기 선택된 블룸필터 배열을 이용하여 상기 데이터 패킷의 상기 악성코드 유무를 탐지하는 침입 탐지부; 및

상기 탐지된 데이터 패킷에 대한 상기 악성코드가 없는 경우, 상기 탐지된 데이터 패킷을 상기 하위 CCN 라우터로 전달하는 전달부

를 포함하고,

상기 연산부는

하기 [수식 1]을 이용하여 상기 블룸필터 세트를 선택하기 위한 연산을 수행하는 제1 연산부 및 하기 [수식 2]를 이용하여 상기 블룸필터 배열을 선택하기 위한 연산을 수행하는 제2 연산부를 포함하는 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템.

[수식 1]

$$j = \text{Hop}_d - \text{Hop}_i$$

[수식 2]

$k = \text{Hop}_d \bmod j$ (여기서, Hop_d 는 상기 데이터 홉 카운터 수, Hop_i 는 상기 인터레스트 홉 카운터 수, j 는 상기 선택된 블룸필터 세트, k 는 상기 선택된 블룸필터 배열)

청구항 2

제1항에 있어서,

상기 데이터베이스는

사용자 단말기로부터 첫 번째 인터레스트 패킷을 전달받는 경우, 상기 인터레스트 홉 카운터 수를 1로 저장하는 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템.

청구항 3

제1항에 있어서,

상기 데이터베이스는

상기 콘텐츠 서버로부터 첫 번째 데이터 패킷을 전달받는 경우, 상기 인터레스트 홉 카운터 수에 2를 곱셈하여 상기 데이터 홉 카운터 수를 저장하는

CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템.

청구항 4

제1항에 있어서,

상기 데이터베이스는

복수의 인터레스트 홉 카운터 수가 존재하는 다중경로인 경우, 최소값을 갖는 인터레스트 홉 카운터 수를 선택하여 저장하는

CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템.

청구항 5

삭제

청구항 6

제1항에 있어서,

상기 전달부는

상기 인터레스트 홉 카운터 수에 1을 가산하고, 상기 1을 가산한 인터레스트 홉 카운터 수가 포함된 인터레스트 패킷을 상기 상위 CCN 라우터에게 전달하고,

상기 상위 CCN 라우터는

상기 1을 가산한 인터레스트 홉 카운터 수를 저장하는

CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템.

청구항 7

제1항에 있어서,

상기 전달부는

상기 데이터 홉 카운터 수에 1을 감산하고, 상기 1을 감산한 데이터 홉 카운터 수가 포함된 데이터 패킷을 상기 하위 CCN 라우터에게 전달하고,

상기 하위 CCN 라우터는

상기 1을 감산한 데이터 홉 카운터 수를 저장하는

CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템.

청구항 8

제1항에 있어서,

상기 인터레스트 홉 카운터 수에 2를 곱셈한 값이 상기 데이터 홉 카운터 수보다 클 경우, 상기 데이터 홉 카운터 수를 상기 인터레스트 홉 카운터 수에 2를 곱셈한 값으로 변경하는 변경부

를 더 포함하는 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템.

청구항 9

콘텐츠 서버 및 상위 CCN(Content Centric Networking) 라우터 중 적어도 하나로부터 데이터 패킷(Data Packet)을 전달받는 CCN 라우터에 있어서,

상기 데이터 패킷의 악성코드 유무를 탐지하는 다중 분산 블룸필터 세트들, 하위 CCN 라우터로부터 전달 받은 인터레스트 패킷(Interest Packet)에 포함된 인터레스트 홉(Hop) 카운터 수 및 상기 상위 라우터로부터 전달받은 데이터 패킷에 포함된 데이터 홉 카운터 수를 저장하는 단계;

상기 인터레스트 홉 카운터 수와 상기 데이터 홉 카운터 수를 통하여 상기 다중 분산 블룸필터 세트들 중에서 블룸필터 세트를 선택하기 위한 연산과 상기 선택된 블룸필터 세트에서 블룸필터 배열을 선택하기 위한 연산을 수행하는 단계;

상기 선택된 블룸필터 배열을 이용하여 상기 데이터 패킷의 상기 악성코드 유무를 탐지하는 단계; 및

상기 탐지된 데이터 패킷에 대한 상기 악성코드가 없는 경우, 상기 탐지된 데이터 패킷을 상기 하위 CCN 라우터로 전달하는 단계

를 포함하고,

상기 연산을 수행하는 단계는

하기 [수식 1]을 이용하여 상기 블룸필터 세트를 선택하기 위한 연산을 수행하는 단계 및 하기 [수식 2]를 이용하여 상기 블룸필터 배열을 선택하기 위한 연산을 수행하는 단계를 포함하는 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 방법.

[수식 1]

$$j = \text{Hop}_d - \text{Hop}_i$$

[수식 2]

$k = \text{Hop}_d \bmod j$ (여기서, Hop_d 는 상기 데이터 홉 카운터 수, Hop_i 는 상기 인터레스트 홉 카운터 수, j 는 상기 선택된 블룸필터 세트, k 는 상기 선택된 블룸필터 배열)

청구항 10

제9항의 방법을 실행하는 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

명세서

기술분야

[0001]

본 발명은 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템 및 방법에 관한 것으로, 보다 상세하게는 CCN 라우터에서 데이터 패킷의 악성코드 유무를 탐지하기 위한 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템 및 방법에 관한 것이다.

배경기술

[0002]

호스트 기반의 인터넷 구조는 확장성, 보안성 및 네트워크 유연성에 제약을 갖고 있다. 이를 극복하기 위해 최근에는 콘텐츠 중심 네트워크(CCN, Content Centric Networking)에 대한 연구가 활발히 진행되고 있다. 기존의 인터넷 전송 방법은 송수신 호스트의 IP(Internet Protocol) 주소를 이용하여 서비스를 제공하나, 동일한 데이터들이 사용자 수만큼 반복하여 전송되어 비효율적이다. 반면, CCN은 IP 주소 대신에 콘텐츠 이름을 사용하여 네트워크에서 데이터를 배포할 수 있으므로, 동일한 데이터의 반복 전송을 피하고, 동적으로 빠른 서비스를 제공할 수 있는 장점이 있다.

[0003]

그러나, 이러한 CCN상에 악성코드가 유포될 경우, 악성코드를 전달받은 CCN 라우터는 시스템 내부에 캐시되어 지속적으로 이웃하는 CCN 라우터에게 악성코드를 유포할 수 있다. 비록 각각의 CCN 라우터들은 자체적 보안 기술을 보유하고 있으나, 이 보안 기술은 콘텐츠 자체의 무결성만을 보장하고 있는 수준이다.

[0004]

또한, 각각의 CCN 라우터들은 하나의 분산 블룸필터만을 탑재하기 때문에 필연적으로 생성되는 경로에 따라 오탐지가 발생할 수 있고, 여러 CCN 라우터들이 중복적으로 동일한 블룸필터를 사용하는 단점이 존재한다.

선행기술문헌

특허문헌

[0005]

(특허문헌 0001) 대한민국 공개특허 제1020100088562호(2010.08.09), "콘텐츠-중심적인 네트워크에서 패킷의 전달을 용이하게 하기 위한 방법 및 시스템"

(특허문헌 0002) 대한민국 등록특허 제101355767호(2014.01.20), "콘텐츠 중심 네트워크 환경에서의 동등 계층 간 그룹 통신 방법"

발명의 내용

해결하려는 과제

- [0006] 본 발명의 일실시예는 사용자 단말기와 콘텐츠 서버 사이의 홉 수에 따라 동적으로 블룸필터 배열을 선택하여 악성코드를 탐지하는 소요 시간을 줄일 수 있는 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템 및 방법을 제공한다.
- [0007] 본 발명의 일실시예는 하나의 블룸필터 세트가 아닌 다중 분산 블룸필터 세트들을 사용하여 악성코드를 보다 효율적으로 탐지할 수 있는 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템 및 방법을 제공한다.

과제의 해결 수단

- [0008] 콘텐츠 서버 및 상위 CCN(Content Centric Networking) 라우터 중 적어도 하나로부터 데이터 패킷(Data Packet)을 전달받는 CCN 라우터에 있어서, 본 발명의 실시예에 따른 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템은 상기 데이터 패킷의 악성코드 유무를 탐지하는 다중 분산 블룸필터 세트들, 하위 CCN 라우터로부터 전달 받은 인터레스트 패킷(Interest Packet)에 포함된 인터레스트 홉(Hop) 카운터 수 및 상기 상위 라우터로부터 전달받은 데이터 패킷에 포함된 데이터 홉 카운터 수를 저장하는 데이터베이스; 상기 인터레스트 홉 카운터 수와 상기 데이터 홉 카운터 수를 통하여 상기 다중 분산 블룸필터 세트들 중에서 블룸필터 세트를 선택하기 위한 연산과 상기 선택된 블룸필터 세트에서 블룸필터 배열을 선택하기 위한 연산을 수행하는 연산부; 상기 선택된 블룸필터 배열을 이용하여 상기 데이터 패킷의 상기 악성코드 유무를 탐지하는 침입 탐지부; 및 상기 탐지된 데이터 패킷에 대한 상기 악성코드가 없는 경우, 상기 탐지된 데이터 패킷을 상기 하위 CCN 라우터로 전달하는 전달부를 포함한다.
- [0009] 상기 데이터베이스는 사용자 단말기로부터 첫 번째 인터레스트 패킷을 전달받는 경우, 상기 인터레스트 홉 카운터 수를 1로 저장할 수 있고, 상기 데이터베이스는 상기 콘텐츠 서버로부터 첫 번째 데이터 패킷을 전달받는 경우, 상기 인터레스트 홉 카운터 수에 2를 곱셈하여 상기 데이터 홉 카운터 수를 저장할 수 있으며, 상기 데이터베이스는 복수의 인터레스트 홉 카운터 수가 존재하는 다중경로인 경우, 최소값을 갖는 인터레스트 홉 카운터 수를 선택하여 저장할 수 있다.
- [0010] 상기 연산부는 하기 수식 (1)을 이용하여 상기 블룸필터 세트를 선택하기 위한 연산을 수행하는 제1 연산부; 및 하기 수식 (2)를 이용하여 상기 블룸필터 배열을 선택하기 위한 연산을 수행하는 제2 연산부를 포함할 수 있다.
- [0011] [수식 1]
- [0012]
$$j = \text{Hop}_d - \text{Hop}_i$$
- [0013] [수식 2]
- [0014]
$$k = \text{Hop}_d \bmod j$$
- [0015] 상기 전달부는 상기 인터레스트 홉 카운터 수에 1을 가산하고, 상기 1을 가산한 인터레스트 홉 카운터 수가 포함된 인터레스트 패킷을 상기 상위 CCN 라우터에게 전달하고, 상기 상위 CCN 라우터는 상기 1을 가산한 인터레스트 홉 카운터 수를 저장할 수 있다.
- [0016] 또한, 상기 전달부는 상기 데이터 홉 카운터 수에 1을 감산하고, 상기 1을 감산한 데이터 홉 카운터 수가 포함된 데이터 패킷을 상기 하위 CCN 라우터에게 전달하고, 상기 하위 CCN 라우터는 상기 1을 감산한 데이터 홉 카운터 수를 저장할 수 있다.
- [0017] 본 발명의 실시예에 따른 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템은 상기 인터레스트 홉 카운터 수에 2를 곱셈한 값이 상기 데이터 홉 카운터 수보다 클 경우, 상기 데이터 홉 카운터 수를 상기 인터레스트 홉 카운터 수에 2를 곱셈한 값으로 변경하는 변경부를 더 포함할 수 있다.
- [0018] 콘텐츠 서버 및 상위 CCN(Content Centric Networking) 라우터 중 적어도 하나로부터 데이터 패킷(Data Packet)을 전달받는 CCN 라우터에 있어서, 본 발명의 실시예에 따른 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 방법은 상기 데이터 패킷의 악성코드 유무를 탐지하는 다중 분산 블룸필터 세트들, 하위 CCN 라우터로부터 전달 받은 인터레스트 패킷(Interest Packet)에 포함된 인터레스트 홉(Hop) 카운터 수 및 상

기 상위 라우터로부터 전달받은 데이터 패킷에 포함된 데이터 홉 카운터 수를 저장하는 단계; 상기 인터레스트 홉 카운터 수와 상기 데이터 홉 카운터 수를 통하여 상기 다중 분산 블룸필터 세트들 중에서 블룸필터 세트를 선택하기 위한 연산과 상기 선택된 블룸필터 세트에서 블룸필터 배열을 선택하기 위한 연산을 수행하는 단계; 상기 선택된 블룸필터 배열을 이용하여 상기 데이터 패킷의 상기 악성코드 유무를 탐지하는 단계; 및 상기 탐지된 데이터 패킷에 대한 상기 악성코드가 없는 경우, 상기 탐지된 데이터 패킷을 상기 하위 CCN 라우터로 전달하는 단계를 포함한다.

발명의 효과

[0019] 본 발명의 일실시예는 사용자 단말기와 콘텐츠 서버 사이의 홉 수에 따라 동적으로 블룸필터 배열을 선택하여 악성코드를 탐지하는 소요 시간을 줄일 수 있다.

[0020] 본 발명의 일실시예는 하나의 블룸필터 세트가 아닌 다중 분산 블룸필터 세트들을 사용하여 악성코드를 보다 효율적으로 탐지할 수 있다.

도면의 간단한 설명

[0021] 도 1은 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템을 도시한 블록도이다.

도 2는 다중 분산 블룸필터 세트들을 도시한 예이다.

도 3은 콘텐츠 서버와 사용자 단말기 사이에 위치하는 3개 각각의 CCN 라우터에 침입 탐지 시스템이 구비되는 예를 도시한 도면이다.

도 4는 다중경로가 발생하는 예를 도시한 도면이다.

도 5는 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 방법을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하 첨부 도면들 및 첨부 도면들에 기재된 내용들을 참조하여 본 발명의 실시예를 상세하게 설명하지만, 본 발명이 실시예에 의해 제한되거나 한정되는 것은 아니다.

[0023] 한편, 본 발명을 설명함에 있어서, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는, 그 상세한 설명을 생략할 것이다. 그리고, 본 명세서에서 사용되는 용어(terminology)들은 본 발명의 실시예를 적절히 표현하기 위해 사용된 용어들로서, 이는 사용자, 운용자의 의도 또는 본 발명이 속하는 분야의 관례 등에 따라 달라질 수 있다. 따라서, 본 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0024] 도 1은 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템을 도시한 블록도이다.

[0025] 도 1을 참조하면, 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템(100)은 콘텐츠 서버(161)와 사용자 단말기(162) 사이에 존재하는 각각의 라우터들(100, 100a-1, 100a-N, 100b-1 및 100b-N)에서 사용될 수 있고, 각각의 라우터들(100, 100a-1, 100a-N, 100b-1 및 100b-N)의 개수는 네트워크 환경에 따라 다양할 수 있다.

[0026] CCN 기술은 라우터상의 콘텐츠 저장소(CS, Content Store)에 한 번 전송한 데이터를 캐쉬하고, 사용자 단말기(162)가 캐시된 데이터를 요청시, 해당 데이터를 콘텐츠 서버(161)가 아닌 라우터에서 데이터를 바로 전송할 수 있는 기술이다.

[0027] 콘텐츠 서버(161) 및 상위 CCN(Content Centric Networking) 라우터(100a-1) 중 적어도 하나로부터 데이터 패킷(Data Packet)을 전달받는 CCN 라우터에 있어서, CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템(100)은 데이터베이스(110), 연산부(130), 침입 탐지부(140) 및 전달부(150)를 포함한다.

[0028] 데이터베이스(110)는 데이터 패킷의 악성코드 유무를 탐지하는 다중 분산 블룸필터 세트들, 하위 CCN 라우터(100b-1)로부터 전달 받은 인터레스트 패킷(Interest Packet)에 포함된 인터레스트 홉 카운터 수 및 상위 라우터(100a-1)로부터 전달받은 데이터 패킷에 포함된 데이터 홉 카운터 수를 저장한다.

[0029] 인터레스트 패킷은 데이터(예를 들어, 콘텐츠 등) 요청에 사용되는 패킷이고, 인터레스트 패킷은 FIB(Forwarding Information Base)를 참조하여 콘텐츠 서버 방향(상위 방향)으로 전송하는데 사용될 수 있으며,

데이터 패킷은 실제 데이터 전송에 사용되는 패킷일 수 있다. FIB는 콘텐츠 이름으로부터 인터레스트 패킷을 전달하는 인터페이스를 결정하는 라우팅 테이블(Routing Table)일 수 있다.

[0030] 데이터베이스(110)는 사용자 단말기(162)로부터 첫 번째 인터레스트 패킷을 전달받는 경우, 인터레스트 홉 카운터 수를 1로 저장할 수 있고, 콘텐츠 서버(130)로부터 첫 번째 데이터 패킷을 전달받는 경우, 인터레스트 홉 카운터 수에 2를 곱셈하여 데이터 홉 카운터 수를 저장할 수 있다.

[0031] 연산부(130)는 인터레스트 홉 카운터 수와 데이터 홉 카운터 수를 통하여 다중 분산 블룸필터 세트들 중에서 블룸필터 세트를 선택하기 위한 연산과 선택된 블룸필터 세트에서 블룸필터 배열을 선택하기 위한 연산을 수행한다.

[0032] 보다 상세하게는 연산부(130)는 하기 수식 (1)을 이용하여 블룸필터 세트를 선택하기 위한 연산을 수행하는 제1 연산부 및 하기 수식 (2)를 이용하여 블룸필터 배열을 선택하기 위한 연산을 수행하는 제2 연산부를 포함할 수 있다.

[0033] [수식 1]

[0034] $j = \text{Hop}_d - \text{Hop}_i$

[0035] [수식 2]

[0036] $k = \text{Hop}_d \bmod j$

[0037] 여기서, Hop_d 는 데이터 홉 카운터 수, Hop_i 는 인터레스트 홉 카운터 수, j 는 선택된 블룸필터 세트, k 는 선택된 블룸필터 배열 및 $\text{Hop}_d \bmod j$ 는 Hop_d 를 j 로 나눴을 때의 나머지를 나타낸다.

[0038] 도 2는 다중 분산 블룸필터 세트들을 도시한 예이다. 도 2를 참조하면, 다중 분산 블룸필터 세트들(200)은 적어도 하나의 블룸필터 세트(201, 202, 203 및 204)를 포함할 수 있다.

[0039] 연산부(130)는 다중 분산 블룸필터 세트들(200) 중에서 위에 전술한 수식 (1)을 통하여 블룸필터 세트를 선택할 수 있고, 선택된 블룸필터 세트 중에서 위에 전술한 수식 (2)를 통하여 블룸필터 배열을 선택할 수 있다.

[0040] 본 발명의 일측에 따르면, CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템(100)은 이웃하는 CCN 라우터 홉 수에 따라 다중 분산 블룸필터 세트들(201, 202, 203 및 204)의 개수를 다양하게 설정할 수 있다.

[0041] 다시 도 1을 참조하면, 침입 탐지부(140)는 선택된 블룸필터 배열을 이용하여 데이터 패킷의 악성코드 유무를 탐지한다. 보다 상세하게는, 침입 탐지부(130)는 선택된 블룸필터 배열 위치에 저장되어 있는 공격 패턴 데이터를 이용하여 데이터 패킷의 악성코드 유무를 탐지할 수 있다.

[0042] 본 발명의 일측에 따르면, CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템(100)은 CCN 환경, CDN(Content Delivery Networking) 환경, CBN(Content Based Networking) 환경, NDN(Named Data Networking) 환경, DON(Data Oriented Networking) 환경, ICN(Information Centric Networking) 환경 및 애드혹(Ad-hoc) 형태의 네트워킹 환경 중 적어도 하나에 적용하여 데이터 패킷의 악성코드 유무를 탐지할 수 있다.

[0043] 전달부(150)는 탐지된 데이터 패킷에 대한 악성코드가 없는 경우, 탐지된 데이터 패킷을 하위 CCN 라우터로 전달한다.

[0044] 본 발명의 일측에 따르면, 전달부(140)는 인터레스트 홉 카운터 수에 1을 가산하고, 1을 가산한 인터레스트 홉 카운터 수가 포함된 인터레스트 패킷을 상위 CCN 라우터에게 전달할 수 있고, 상위 CCN 라우터는 1을 가산한 인터레스트 홉 카운터 수를 저장할 수 있다.

[0045] 본 발명의 다른 일측에 따르면, 전달부(150)는 데이터 홉 카운터 수에 1을 감산하고, 1을 감산한 데이터 홉 카운터 수가 포함된 데이터 패킷을 하위 CCN 라우터에게 전달할 수 있고, 하위 CCN 라우터는 1을 감산한 데이터 홉 카운터 수를 저장할 수 있다. 이하, 도 3을 참조하여 각각의 CCN 라우터에 침입 탐지 시스템이 구비되는 예를 설명하기로 한다.

- [0046] 도 3은 콘텐츠 서버와 사용자 단말기 사이에 위치하는 3개 각각의 CCN 라우터에 침입 탐지 시스템이 구비되는 예를 도시한 도면이다.
- [0047] 도 3을 참조하면, 각각의 침입 탐지 시스템은 인터레스트 홉 카운터 수 및 데이터 홉 카운터 수를 저장할 수 있다.
- [0048] 본 발명의 일측에 따르면, 침입 탐지 시스템은 사용자 단말기로부터 첫 번째 인터레스트 패킷을 전달받는 경우, 인터레스트 홉 카운터 수를 1로 저장할 수 있고, 콘텐츠 서버로부터 첫 번째 데이터 패킷을 전달받는 경우, 인터레스트 홉 카운터 수에 2를 곱셈하여 데이터 홉 카운터 수를 저장할 수 있다.
- [0049] 또한, 각각의 침입 탐지 시스템들은 인터레스트 홉 카운터 수에 1을 가산하고, 1을 가산한 인터레스트 홉 카운터 수가 포함된 인터레스트 패킷을 상위 CCN 라우터에게 전달할 수 있다.
- [0050] 또한, 각각의 침입 탐지 시스템들은 데이터 홉 카운터 수에 1을 감산하고, 1을 감산한 데이터 홉 카운터 수가 포함된 데이터 패킷을 하위 CCN 라우터에게 전달할 수 있다.
- [0051] 또한, 각각의 침입 탐지 시스템들은 인터레스트 홉 카운터 수와 데이터 홉 카운터 수를 통하여 다중 분산 블룸필터 세트들 중에서 블룸필터 세트를 선택하기 위한 연산과 선택된 블룸필터 세트에서 블룸필터 배열을 선택하기 위한 연산을 수행할 수 있다.
- [0052] 보다 상세하게는, 각각의 침입 탐지 시스템들은 위에 기술한 수식 (1) 및 수식 (2)를 이용하여 블룸필터 세트 및 블룸필터 배열을 선택할 수 있다.
- [0053] 다시 도 1을 참조하면, 데이터베이스(110)는 복수의 인터레스트 홉 카운터 수가 존재하는 다중경로인 경우, 최소값을 갖는 인터레스트 홉 카운터 수를 선택하여 저장할 수 있다.
- [0054] 본 발명의 실시예에 따른 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 시스템(100)은 인터레스트 홉 카운터 수에 2를 곱셈한 값이 데이터 홉 카운터 수보다 클 경우, 데이터 홉 카운터 수를 인터레스트 홉 카운터 수에 2를 곱셈한 값으로 변경하는 변경부(120)를 더 포함할 수 있다. 이하, 다중경로가 발생하는 예를 설명하기로 한다.
- [0055] 도 4는 다중경로가 발생하는 예를 도시한 도면이다.
- [0056] 도 4를 참조하면, 다중경로는 복수의 사용자 단말기의 경로에 따라 복수의 인터레스트 패킷을 수신하는 CCN 라우터(410)의 경로일 수 있다. 따라서, 침입 탐지 시스템(100)은 복수의 인터레스트 홉 카운터 수가 존재하는 다중경로인 경우, 최소값을 갖는 인터레스트 홉 카운터 수를 선택하여 저장할 수 있다. 예를 들어, 다중경로를 겪는 CCN 라우터(410)는 도 4에 도시된 바와 같이, 최소값을 갖는 인터레스트 홉 카운터 수 2를 선택하여 저장할 수 있다.
- [0057] 침입 탐지 시스템(100)은 인터레스트 홉 카운터 수에 2를 곱셈한 값이 데이터 홉 카운터 수보다 클 경우, 데이터 홉 카운터 수를 인터레스트 홉 카운터 수에 2를 곱셈한 값으로 변경할 수 있다.
- [0058] 예를 들어, 데이터 홉 카운터 수 3과 인터레스트 홉 카운터 수 5를 갖는 CCN 라우터(420)는 도 4에 도시된 바와 같이, 식별번호 430의 순서도에 따라 데이터 홉 카운터 수를 유지 또는 변경할 수 있다. 보다 상세하게는, CCN 라우터(420)는 인터레스트 홉 카운터 수에 2를 곱셈한 값이 데이터 홉 카운터 수보다 크기 때문에, 데이터 홉 카운터 수를 인터레스트 홉 카운터 수에 2를 곱셈한 10으로 변경할 수 있다.
- [0059] 또한, CCN 라우터(420)는 도 4에 도시된 바와 같이 데이터 홉 카운터 수 10에서 1을 감산하고, 1을 감산한 데이터 홉 카운터 수 9가 포함된 데이터 패킷을 하위 CCN 라우터에게 전달할 수 있다.
- [0060] 침입 탐지 시스템(100)은 인터레스트 홉 카운터 수에 2를 곱셈한 값이 데이터 홉 카운터 수보다 같거나 작을 경우, 현재 데이터 홉 카운터 수를 유지할 수 있다. 예를 들어, 도 4에 도시된 식별번호 420번의 CCN 라우터를 제외한 CCN 라우터들은 인터레스트 홉 카운터 수에 2를 곱셈한 값이 데이터 홉 카운터 수보다 같거나 작은 경우이다.
- [0061] 도 5는 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 방법을 도시한 흐름도이다.

- [0062] 도 5를 참조하면, 콘텐츠 서버 및 상위 CCN 라우터 중 적어도 하나로부터 데이터 패킷을 전달받는 CCN 라우터에 있어서, CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 방법은 단계 510에서, 데이터 패킷의 악성코드 유무를 탐지하는 다중 분산 블룸필터 세트들, 하위 CCN 라우터로부터 전달받은 인터레스트 패킷에 포함된 인터레스트 홉 카운터 수 및 상위 라우터로부터 전달 받은 데이터 패킷에 포함된 데이터 홉 카운터 수를 저장한다.
- [0063] 또한, 단계 510은 사용자 단말기로부터 첫 번째 인터레스트 패킷을 전달받는 경우, 인터레스트 홉 카운터 수를 1로 저장할 수 있고, 콘텐츠 서버로부터 첫 번째 데이터 패킷을 전달받는 경우, 인터레스트 홉 카운터 수에 2를 곱셈하여 데이터 홉 카운터 수를 저장할 수 있다.
- [0064] CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 방법은 단계 520에서, 인터레스트 홉 카운터 수와 데이터 홉 카운터 수를 통하여 다중 분산 블룸필터 세트들 중에서 블룸필터 세트를 선택하기 위한 연산과 선택된 블룸필터 세트에서 블룸필터 배열을 선택하기 위한 연산을 수행한다.
- [0065] 보다 상세하게는, 단계 520은 위에 기술한 수식 (1)을 이용하여 블룸필터 세트를 선택하기 위한 연산을 수행하는 단계 및 위에 기술한 수식 (2)를 이용하여 블룸필터 배열을 선택하기 위한 연산을 수행하는 단계를 포함할 수 있다.
- [0066] CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 방법은 단계 530에서, 선택된 블룸필터 배열을 이용하여 데이터 패킷의 악성코드 유무를 탐지하고, 단계 540에서, 탐지된 데이터 패킷에 대한 악성코드가 없는 경우, 탐지된 데이터 패킷을 하위 CCN 라우터로 전달한다.
- [0067] 단계 540은 인터레스트 홉 카운터 수에 1을 가산하고, 1을 가산한 인터레스트 홉 카운터 수가 포함된 인터레스트 패킷을 상위 CCN 라우터에게 전달할 수 있고, 상위 CCN 라우터는 1을 가산한 인터레스트 홉 카운터 수를 저장할 수 있다.
- [0068] 또한, 단계 540은 데이터 홉 카운터 수에 1을 감산하고, 1을 감산한 데이터 홉 카운터 수가 포함된 데이터 패킷을 하위 CCN 라우터에게 전달할 수 있고, 하위 CCN 라우터는 1을 감산한 데이터 홉 카운터 수를 저장할 수 있다.
- [0069] 본 발명의 일측에 따르면, 단계 510은 복수의 인터레스트 홉 카운터 수가 존재하는 다중경로인 경우, 최소값을 갖는 인터레스트 홉 카운터 수를 선택하여 저장할 수 있다.
- [0070] 본 발명의 실시예에 따른 CCN 라우터에서 다중 분산 블룸필터 세트들을 이용하는 침입 탐지 방법은 인터레스트 홉 카운터 수에 2를 곱셈한 값이 데이터 홉 카운터 수보다 클 경우, 데이터 홉 카운터 수를 인터레스트 홉 카운터 수에 2를 곱셈한 값으로 변경하는 단계를 더 포함할 수 있다.
- [0071] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0072]
- [0073] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될

수 있다.

[0074]

[0075]

그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

부호의 설명

[0076]

100: 침입 탐지 시스템

110: 데이터베이스

120: 변경부

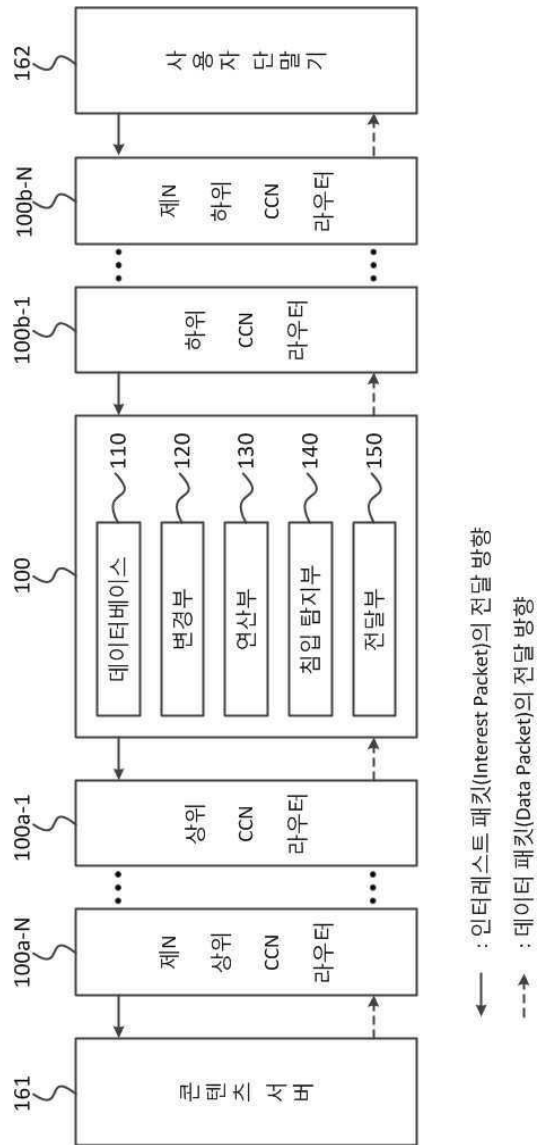
130: 연산부

140: 침입 탐지부

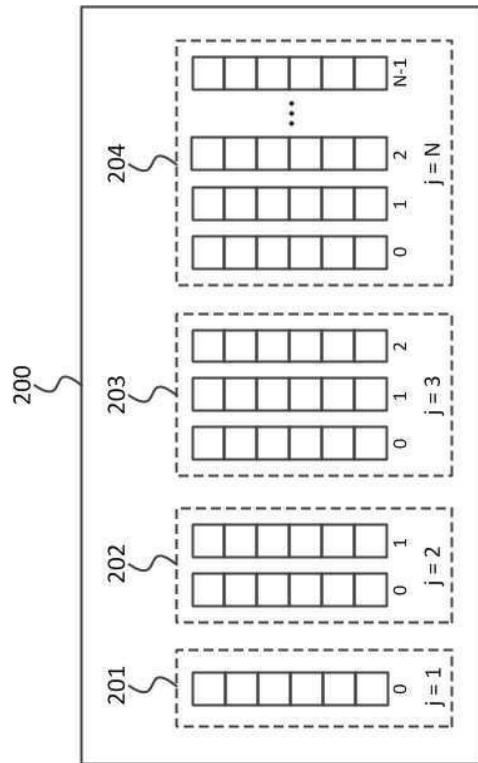
150: 전달부

도면

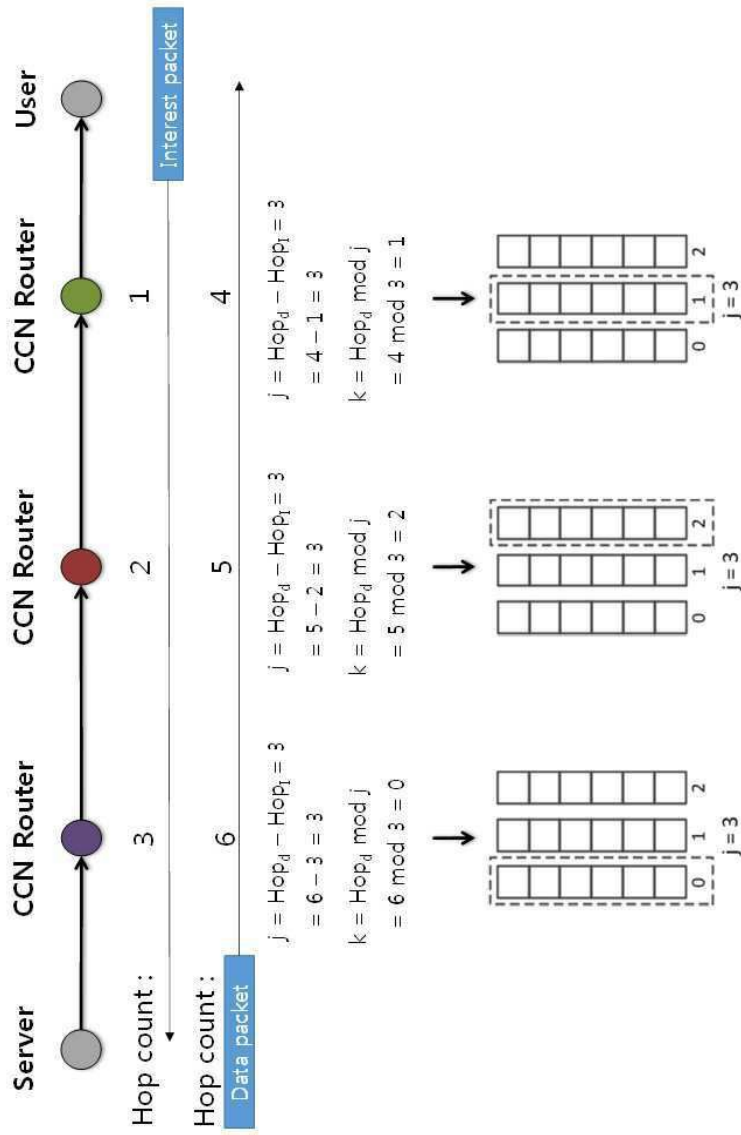
도면1



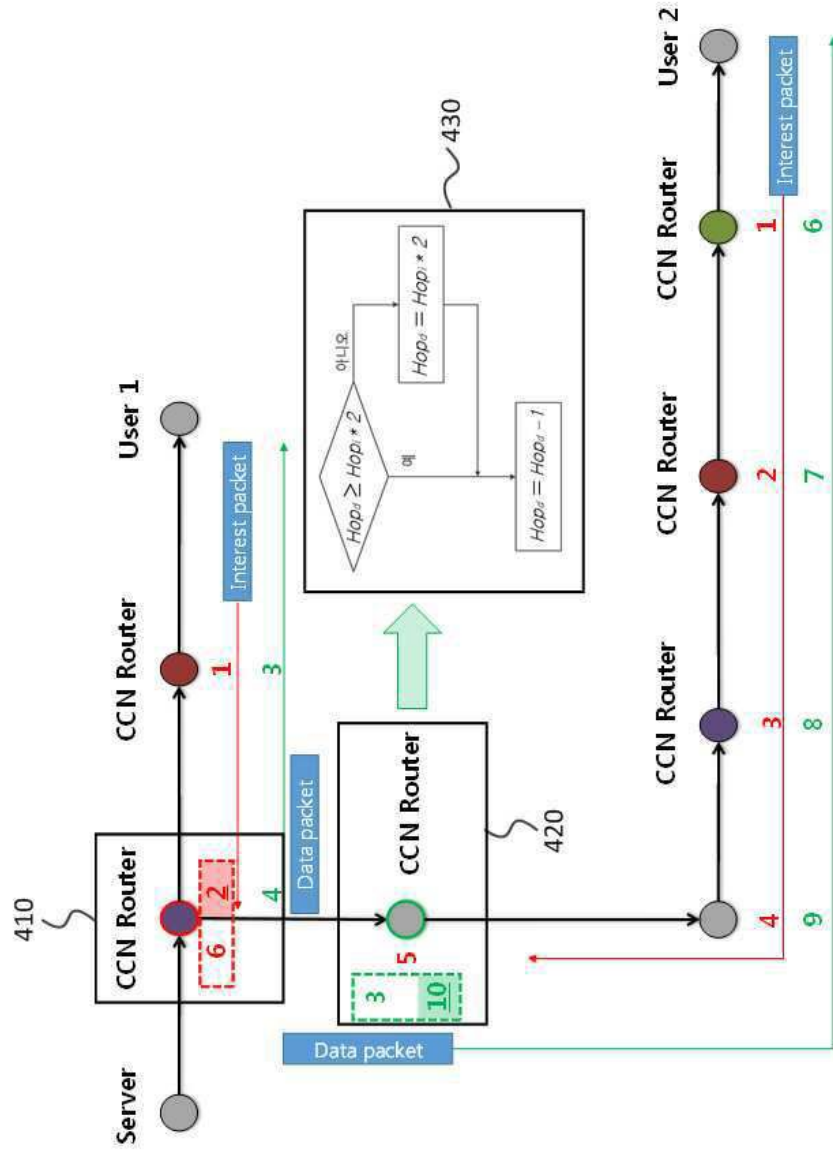
도면2



도면3



도면4



도면5

