



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0079086
(43) 공개일자 2017년07월10일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) H04L 29/12 (2006.01)
(52) CPC특허분류
H04L 63/0421 (2013.01)
H04L 61/2539 (2013.01)
(21) 출원번호 10-2015-0189268
(22) 출원일자 2015년12월30일
심사청구일자 2015년12월30일

(71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
리시
서울시 서대문구 이화여대7길 46,4층 영채리빙텔 207호 (대현동)
채기준
서울특별시 강남구 강남대로136길 34
도인실
인천광역시 연수구 센트럴로 194, 201동 2705호(송도동, 더샵 센트럴파크2)
(74) 대리인
특허법인(유한)아이시스

전체 청구항 수 : 총 9 항

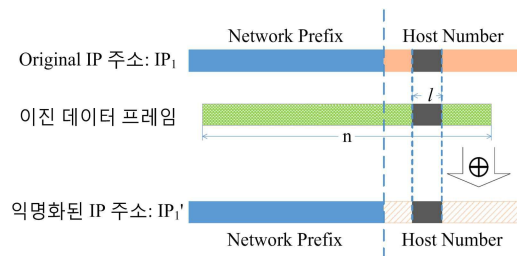
(54) 발명의 명칭 IP 기반 네트워크에서 IP 주소를 익명화하는 기법 및 IP 기반 네트워크에서 IP 주소를 익명화하여 패킷을 전송하는 방법

(57) 요약

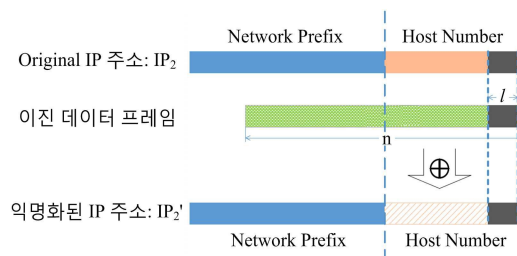
IP 기반 네트워크에서 IP 주소를 익명화하는 기법은 네트워크 인터페이스 장치가 자신이 관리하는 네트워크에 연결된 네트워크 객체로부터 상기 네트워크 객체의 소스 IP 주소를 포함하는 패킷을 수신하는 단계, 상기 네트워크 인터페이스 장치가 상기 소스 IP 주소의 호스트 번호 부분 중 기준 길이를 갖는 임의의 타겟 스트링을 선택하는

(뒷면에 계속)

대표도 - 도1



(a)



(b)

단계; , 상기 네트워크 인터페이스 장치가 이진 데이터 프레임에서 기준 위치를 시작으로 상기 타겟 스트링과 일치하는 부분을 찾고, 상기 이진 데이터 프레임을 상기 일치하는 부분을 기준으로 동일 선상에 배치하는 단계, 상기 네트워크 인터페이스 장치가 상기 타겟 스트링을 제외하고 상기 소스 IP 주소의 호스트 번호 부분을 상기 동일 선상에 배치된 상기 이진 데이터 프레임과 XOR 연산을 하는 단계 및 상기 네트워크 인터페이스 장치가 상기 소스 IP 주소의 네트워크 프리픽스에 상기 IP 주소의 호스트 번호 부분과 상기 이진 데이터 프레임이 XOR된 이진 스트링을 연결하는 단계를 포함한다.

(52) CPC특허분류

H04L 61/305 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 2013R1A1A2011788

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 기초연구사업(학술진흥)

연구과제명 CDN 환경에서의 안전하고 효율적인 서비스보안 기법

기 여 율 1/1

주관기관 이화여자대학교 산학협력단

연구기간 2015.06.01 ~ 2016.05.31

명세서

청구범위

청구항 1

네트워크 인터페이스 장치가 자신이 관리하는 네트워크에 연결된 네트워크 객체로부터 상기 네트워크 객체의 소스 IP 주소를 포함하는 패킷을 수신하는 단계;

상기 네트워크 인터페이스 장치가 상기 소스 IP 주소의 호스트 번호 부분 중 기준 길이(l)를 갖는 임의의 타겟 스트링을 선택하는 단계;

상기 네트워크 인터페이스 장치가 이진 데이터 프레임에서 기준 위치를 시작으로 상기 타겟 스트링과 일치하는 부분을 찾고, 상기 이진 데이터 프레임을 상기 일치하는 부분을 기준으로 동일 선상에 배치하는 단계;

상기 네트워크 인터페이스 장치가 상기 타겟 스트링을 제외하고 상기 소스 IP 주소의 호스트 번호 부분을 상기 동일 선상에 배치된 상기 이진 데이터 프레임과 XOR 연산을 하는 단계; 및

상기 네트워크 인터페이스 장치가 상기 소스 IP 주소의 네트워크 프리픽스에 상기 IP 주소의 호스트 번호 부분과 상기 이진 데이터 프레임이 XOR된 이진 스트링을 연결하는 단계를 포함하는 IP 기반 네트워크에서 IP 주소를 식별화하는 기법.

청구항 2

제1항에 있어서,

상기 이진 데이터 프레임은 $n = 2^l \times l$ 으로 연산되는 길이 n 을 갖는 IP 기반 네트워크에서 IP 주소를 식별화하는 기법.

청구항 3

제1항에 있어서,

상기 XOR 연산을 하는 단계에서 상기 호스트 번호 부분 중 XOR 연산할 상기 이진 데이터 프레임이 없는 부분은 XOR 연산하지 않고, 상기 인터페이스 장치가 상기 연결하는 단계에서 상기 없는 부분을 상기 호스트 번호 부분에 그대로 남기는 IP 기반 네트워크에서 IP 주소를 식별화하는 기법.

청구항 4

네트워크 인터페이스 장치가 자신이 관리하는 네트워크에 연결된 네트워크 객체로부터 상기 네트워크 객체의 소스 IP 주소를 포함하는 패킷을 수신하는 단계;

상기 네트워크 인터페이스 장치가 상기 소스 IP 주소의 호스트 번호 부분의 일부인 타겟 스트링을 기준으로 상기 호스트 번호 부분을 별도의 이진 데이터 프레임과 비트 연산하여 식별화된 IP 주소를 생성하는 단계;

상기 네트워크 인터페이스 장치가 상기 식별화된 IP 주소를 포함하는 패킷을 외부 네트워크에 전달하는 단계;

상기 네트워크 인터페이스 장치가 상기 외부 네트워크로부터 상기 식별화된 IP 주소를 포함하는 패킷에 대한 응답 패킷을 수신하는 단계;

상기 네트워크 인터페이스 장치가 상기 응답 패킷에 포함된 상기 식별화된 IP 주소를 상기 이진 데이터 프레임을 이용하여 상기 소스 IP 주소로 변환하는 단계; 및

상기 네트워크 인터페이스 장치가 상기 소스 IP 주소를 기반으로 상기 응답 패킷을 상기 네트워크 객체에 전달하는 단계를 포함하는 IP 기반 네트워크에서 IP 주소를 식별화하여 패킷을 전송하는 방법.

청구항 5

제4항에 있어서,

상기 익명화된 IP 주소를 생성하는 단계는

상기 네트워크 인터페이스 장치가 상기 소스 IP 주소의 호스트 번호 부분 중 기준 길이(l)를 갖는 임의의 타겟 스트링을 선택하는 단계;

상기 네트워크 인터페이스 장치가 이진 데이터 프레임에서 기준 위치를 시작으로 상기 타겟 스트링과 일치하는 부분을 찾고, 상기 이진 데이터 프레임을 상기 일치하는 부분을 기준으로 동일 선상에 배치하는 단계;

상기 네트워크 인터페이스 장치가 상기 타겟 스트링을 제외하고 상기 소스 IP 주소의 호스트 번호 부분을 상기 동일 선상에 배치된 상기 이진 데이터 프레임과 XOR 연산을 하는 단계; 및

상기 네트워크 인터페이스 장치가 상기 소스 IP 주소의 네트워크 프리픽스와 상기 IP 주소의 호스트 번호 부분과 상기 이진 데이터 프레임이 XOR된 이진 스트링을 연결하는 단계를 포함하는 IP 기반 네트워크에서 IP 주소를 익명화하여 패킷을 전송하는 방법.

청구항 6

제5항에 있어서,

상기 이진 데이터 프레임은 $n = 2^l \times l$ 으로 연산되는 길이 n 을 갖는 IP 기반 네트워크에서 IP 주소를 익명화하여 패킷을 전송하는 방법.

청구항 7

제5항에 있어서,

상기 XOR 연산을 하는 단계에서 상기 호스트 번호 부분 중 XOR 연산할 상기 이진 데이터 프레임이 없는 부분은 XOR 연산하지 않고, 상기 인터페이스 장치가 상기 연결하는 단계에서 상기 없는 부분을 상기 호스트 번호 부분에 그대로 남기는 IP 기반 네트워크에서 IP 주소를 익명화하여 패킷을 전송하는 방법.

청구항 8

제4항에 있어서,

상기 네트워크 인터페이스 장치는 상기 소스 IP 주소에서 익명화된 호스트 번호 부분과 상기 타겟 스트링을 맵핑하여 저장하는 단계를 더 포함하는 IP 기반 네트워크에서 IP 주소를 익명화하여 패킷을 전송하는 방법.

청구항 9

제8항에 있어서,

상기 변환하는 단계는

상기 네트워크 인터페이스 장치는 상기 익명화된 IP 주소의 호스트 번호 부분 중 상기 타겟 스트링을 기준으로 상기 이진 데이터 프레임과 일치하는 부분을 찾고, 상기 이진 데이터 프레임을 상기 일치하는 부분을 기준으로 상기 호스트 번호 부분과 동일 선상에 배치하는 단계;

상기 네트워크 인터페이스 장치가 상기 타겟 스트링을 제외하고 상기 익명화된 IP 주소의 호스트 번호 부분을 상기 동일 선상에 배치된 상기 이진 데이터 프레임과 XOR 연산을 하는 단계; 및

상기 네트워크 인터페이스 장치가 상기 익명화된 IP 주소의 네트워크 프리픽스에 상기 IP 주소의 호스트 번호 부분과 상기 이진 데이터 프레임이 XOR된 이진 스트링을 연결하는 단계를 포함하는 IP 기반 네트워크에서 IP 주소를 익명화하여 패킷을 전송하는 방법.

발명의 설명

기술 분야

[0001] 이하 설명하는 기술은 IP 기반 네트워크에서 개인 정보를 보호하기 위한 기법에 관한 것이다.

배경 기술

[0002] 네트워크 통신 분야에서 타인에게 공개하지 않고 보호해야 할 정보는 크게 두 가지라고 할 수 있다. 하나는 개인 정보(personal information)이고 또 하나는 행동 정보(behavior information)라고 할 수 있다. 개인 정보는 이름, 이메일 주소, 전화 번호 등과 같은 정보를 의미한다. 행동 정보는 네트워크 상에서의 사용자의 활동에 대한 정보를 의미한다. 예컨대, 사용자가 어떤 웹 사이트를 주로 방문하고, 어떤 물건을 주문하는지 등과 같은 정보를 의미한다. 최근 데이터 마이닝 기법으로 개인의 활동 정보가 노출되는 문제가 제기되고 있기도 하다.

[0003] IP 기반 네트워크에서 사용자를 특정하는 정보는 특정 IP라고 할 수 있다. 즉 IP를 추적하면 개인의 행동 정보를 파악할 수 있는 것이다. IP를 일정하게 익명화(anonymization)하여 개인 정보를 보호하는 기법에 대한 연구가 있다.

선행기술문헌

비특허문헌

[0004] (비특허문헌 0001) J. Xu, J. Fan, M. H. Ammar, S. B. Moon, "Prefix-Preserving IP Address Anonymization: Measurement-based Security Evaluation and a New Cryptography-based Scheme," IEEE International Conference on Network Protocols (ICNP), 2002.

발명의 내용

해결하려는 과제

[0005] 이하 설명하는 기술은 IP 기반 네트워크에서 사용자의 IP를 그대로 노출하지 않고 일정하게 익명화하는 기법을 제공하고자 한다. 사용자 단의 네트워크에서 네트워크 내에서 사용자를 식별하는 부분만을 일정하게 변조하여 외부 네트워크와 정보를 주고 받는 기법을 제공하고자 한다.

과제의 해결 수단

[0006] IP 기반 네트워크에서 IP 주소를 익명화하는 기법은 네트워크 인터페이스 장치가 자신이 관리하는 네트워크에 연결된 네트워크 객체로부터 상기 네트워크 객체의 소스 IP 주소를 포함하는 패킷을 수신하는 단계, 상기 네트워크 인터페이스 장치가 상기 소스 IP 주소의 호스트 번호 부분 중 기준 길이를 갖는 임의의 타겟 스트링을 선택하는 단계, 상기 네트워크 인터페이스 장치가 이진 데이터 프레임에서 기준 위치를 시작으로 상기 타겟 스트링과 일치하는 부분을 찾고, 상기 이진 데이터 프레임을 상기 일치하는 부분을 기준으로 동일 선상에 배치하는 단계, 상기 네트워크 인터페이스 장치가 상기 타겟 스트링을 제외하고 상기 소스 IP 주소의 호스트 번호 부분을 상기 동일 선상에 배치된 상기 이진 데이터 프레임과 XOR 연산을 하는 단계 및 상기 네트워크 인터페이스 장치가 상기 소스 IP 주소의 네트워크 프리픽스에 상기 IP 주소의 호스트 번호 부분과 상기 이진 데이터 프레임이 XOR된 이진 스트링을 연결하는 단계를 포함한다.

[0007] IP 기반 네트워크에서 IP 주소를 익명화하여 패킷을 전송하는 방법은 네트워크 인터페이스 장치가 자신이 관리하는 네트워크에 연결된 네트워크 객체로부터 상기 네트워크 객체의 소스 IP 주소를 포함하는 패킷을 수신하는 단계, 상기 네트워크 인터페이스 장치가 상기 소스 IP 주소의 호스트 번호 부분의 일부인 타겟 스트링을 기준으로 상기 호스트 번호 부분을 별도의 이진 데이터 프레임과 비트 연산하여 익명화된 IP 주소를 생성하는 단계, 상기 네트워크 인터페이스 장치가 상기 익명화된 IP 주소를 포함하는 패킷을 외부 네트워크에 전달하는 단계, 상기 네트워크 인터페이스 장치가 상기 외부 네트워크로부터 상기 익명화된 IP 주소를 포함하는 패킷에 대한 응답 패킷을 수신하는 단계, 상기 네트워크 인터페이스 장치가 상기 응답 패킷에 포함된 상기 익명화된 IP 주소를 상기 이진 데이터 프레임을 이용하여 상기 소스 IP 주소로 변환하는 단계 및 상기 네트워크 인터페이스 장치가 상기 소스 IP 주소를 기반으로 상기 응답 패킷을 상기 네트워크 객체에 전달하는 단계를 포함한다.

발명의 효과

[0008] 이하 설명하는 기술은 사용자 단의 네트워크의 게이트웨이 또는 라우터에서 손쉽게 사용자 IP를 변조하여 사용

자 IP를 외부에 노출하지 않으면서도 동시에 정확한 데이터 송수신을 가능하게 한다.

도면의 간단한 설명

도 1은 서버넷의 네트워크 인터페이스 장치가 IP 주소를 식명화하는 과정에 대한 예이다.

도 2는 네트워크 인터페이스 장치가 사용하는 이진 데이터 프레임에 대한 예이다.

도 3은 IP 네트워크에서 식명화를 이용한 패킷 라우팅 과정에 대한 절차 흐름도의 예이다.

도 4는 네트워크 인터페이스 장치가 식명화된 IP 주소를 원래의 IP주소로 변환하는 과정에 대한 예이다.

발명을 실시하기 위한 구체적인 내용

이하 설명하는 기술은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 이하 설명하는 기술을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 이하 설명하는 기술의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 해당 구성요소들은 상기 용어들에 의해 한정되지는 않으며, 단지 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 이하 설명하는 기술의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

본 명세서에서 사용되는 용어에서 단수의 표현은 문맥상 명백하게 다르게 해석되지 않는 한 복수의 표현을 포함하는 것으로 이해되어야 하고, "포함한다" 등의 용어는 실시된 특징, 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 의미하는 것이지, 하나 또는 그 이상의 다른 특징들이나 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 배제하지 않는 것으로 이해되어야 한다.

도면에 대한 상세한 설명을 하기에 앞서, 본 명세서에서의 구성부들에 대한 구분은 각 구성부가 담당하는 주기능 별로 구분한 것에 불과함을 명확히 하고자 한다. 즉, 이하에서 설명할 2개 이상의 구성부가 하나의 구성부로 합쳐지거나 또는 하나의 구성부가 보다 세분화된 기능별로 2개 이상으로 분화되어 구비될 수도 있다. 그리고 이하에서 설명할 구성부 각각은 자신이 담당하는 주기능 이외에도 다른 구성부가 담당하는 기능 중 일부 또는 전부의 기능을 추가적으로 수행할 수도 있으며, 구성부 각각이 담당하는 주기능 중 일부 기능이 다른 구성부에 의해 전담되어 수행될 수도 있음은 물론이다.

또, 방법 또는 동작 방법을 수행함에 있어서, 상기 방법을 이루는 각 과정들은 문맥상 명백하게 특정 순서를 기재하지 않은 이상 명기된 순서와 다르게 일어날 수 있다. 즉, 각 과정들은 명기된 순서와 동일하게 일어날 수도 있고 실질적으로 동시에 수행될 수도 있으며 반대의 순서대로 수행될 수도 있다.

이하 설명하는 기술은 IP 기반 네트워크에서 사용자의 IP를 그대로 노출하지 않고 일정하게 식명화하는 기법이다.

IP 기반 네트워크에서 사용되는 IP 주소는 현재 두 가지 종류가 있다. IPv4 주소와 IPv6 주소가 있다. IPv6는 주소를 나타내는 비트를 크게 늘려 많은 개수의 주소를 표현할 수 있다. 다만 IPv6 주소도 IPv4 주소와 공통된 구조를 갖고 있고, 이하 설명하는 기술은 공통된 구조를 이용하는 것이다. 따라서 설명의 편의를 위해 이하 IPv4 주소를 기반으로 설명하고자 한다. 물론 이하 설명하는 기술은 IPv6 주소에도 적용할 수 있다.

서브넷(subnet)은 IP 네트워크의 논리적 서브 영역(subdivision)에 해당한다. 동일한 서브넷에 연결된 기기는 그들의 IP 주소의 최상위 비트 부분이 공통된다. IP 주소는 두 개의 논리적 필드로 구분할 수 있다. IP 주소는 네트워크 프리픽스(또는 라우팅 프리픽스)와 호스트 식별자로 구분할 수 있다. 호스트 식별자는 특정 호스트(host) 또는 네트워크 인터페이스를 특정하는 식별 정보에 해당한다.

종래 연구 중 IP 주소를 일정하게 식명화하는 기법이 있었다. 다만 종래 연구는 모두 IP 주소의 프리픽스(prefix) 부분을 식명화하는 기법이었다. 그러나 종래 기법은 특정한 네트워크 서비스에는 적절하지 못하다. 예컨대, 종래 식명화 기법은 대표적으로 CDNI(Content Delivery NetworkInterconnection)에 적용하기 어렵다.

CDNi는 콘텐츠를 요청한 사용자에게 가장 가까운 CDN(또는 에지 서버)로부터 콘텐츠를 전달하기 때문이다. 즉, CDNi를 구성하는 개별 CDN은 프리픽스 부분이 상이할 수 있는 별도의 독립적인 네트워크이다. 따라서 개별 CDN을 특정하는 IP 주소의 프리픽스 부분이 식별화되면 CDNi가 정상적으로 동작하기 어렵다. 이하 설명하는 기술은 IP 주소의 프리픽스 부분이 아닌 호스트 식별자 부분을 식별화하는 기법에 해당한다. 따라서 이하 설명하는 기술은 CDNi 등에도 적용 가능하다.

[0021] 이하 설명하는 기술은 사용자고 속한 네트워크 단에서 수행된다. 예컨대, 사용자가 속한 네트워크(가정이나 회사 등)에서 외부 네트워크와 연결을 담당하는 게이트웨이 또는 라우터와 같은 장치가 IP 주소 식별화를 담당할 수 있다. 이하 식별화를 담당하는 장치를 네트워크 인터페이스 장치라고 명명한다.

[0023] IP 주소는 인터넷에 연결된 각 기기(예컨대, PC, 프린터, 스마트폰 등)에 할당된 고유한 숫자 정보로 표현될 수 있다. IP 주소의 프리픽스 부분은 CIDR(Classless Inter-Domain Routing)에 기반하여 서브넷 사이의 주소 할당(allocation) 및 라우팅 용도로 사용될 수 있다.

[0024] 서브넷에서 IP 주소는 두 개의 부분으로 구분된다. IP 주소는 네트워크 프리픽스 부분(network prefix part)과 호스트 번호 부분(host number part)으로 구분된다. 네트워크 프리픽스 부분은 서브넷의 위치를 파악하고 데이터를 라우팅하는데 사용된다. 호스트 번호 부분은 서브넷 상에 연결된 개별 기기를 식별한다. 호스트 번호 부분은 서브넷 내에서 특정 기기를 식별하는데 사용된다. 결국 서브넷 내부에서 네트워크 인터페이스 장치는 호스트 번호 부분으로 기기를 식별하여 패킷을 전송한다. 이하 설명하는 기술은 프리픽스 부분은 그대로 두고, 호스트 번호 부분을 식별화한다.

[0026] 도 1은 서브넷의 네트워크 인터페이스 장치가 IP 주소를 식별화하는 과정에 대한 예이다. 기본적으로 네트워크 인터페이스 장치는 IP 주소 식별화를 위한 이진 데이터 프레임을 갖는다. 데이터 프레임은 길이가 n 인 이진수 스트링(binary string)이다. 네트워크 인터페이스 장치는 임의의 이진 데이터 프레임을 생성할 수 있다. 경우에 따라서 네트워크 인터페이스 장치는 이진 데이터 프레임을 주기적으로 업데이트 할 수도 있다. 데이터 프레임의 길이는 $n = 2^l \times l$ 으로 나타낼 수 있다. 여기서 l 은 IP 주소에서 호스트 번호 부분 중 일부 길이에 해당한다. l 은 호스트 번호 부분 중 변조하고자 하는 길이에 해당한다. 정확하게는 $1 < l < \text{호스트 번호 부분 전체의 길이}$ 라는 관계를 갖는다.

[0027] 네트워크 인터페이스 장치는 호스트 번호 부분 전체를 변조할 수도 있고, 4비트만을 변조할 수도 있다. 변조하고자 하는 길이가 커지면 연산이 오래 걸릴 수 있으므로 적절한 길이를 설정하는 것이 바람직하다.

[0028] 도 1에서는 $l = 2$ 인 경우이다. 호스트 번호 부분에서 두 자리 비트만 변경되어도 식별화는 충분하다고 볼 수 있다. 2^l 개의 이진 서브 스트링이 존재할 수 있으므로 길이가 2인 경우 $2^2 = 4$ 개의 이진 서브 스트링(00, 01, 10 및 11)이 존재한다. 네트워크 인터페이스 장치는 모든 가능한 이진 서브 스트링을 임의의 순서로 배열할 수 있다. 도 2는 네트워크 인터페이스 장치가 사용하는 이진 데이터 프레임에 대한 예이다. 도 2는 $l = 2$ 인 경우에 대한 이진 데이터 프레임의 한 예이다.

[0030] 네트워크 인터페이스 장치가 기기로부터 외부 네트워크로 나가는(outgoing) 패킷을 수신한다. 이때 기기의 IP 주소를 IP_1 이라고 가정한다. 도 1(a)는 IP_1 을 기준으로 네트워크 인터페이스 장치가 IP 주소를 식별화하는 과정에 대한 예이다. 네트워크 인터페이스 장치는 IP_1 의 호스트 번호 부분에서 임의로 길이 l 인 부분을 선택한다. 네트워크 인터페이스 장치가 IP_1 에서 선택한 길이 l 인 부분을 타겟 스트링이라고 명명한다.

[0031] 네트워크 인터페이스 장치는 사전에 마련한 이진 데이터 프레임에서 타겟 스트링과 일치하는 부분을 찾는다. l

의 길이에 따라 이진 데이터 프레임에서 다수의 영역이 타겟 스트링과 일치할 수 있다. 따라서 네트워크 인터페이스 장치는 기본적으로 이진 데이터 프레임의 처음부터 검색하여 타겟 스트링과 일치하는 최초의 지점을 찾을 수 있다. 나아가 네트워크 인터페이스 장치는 다른 기준으로 이진 데이터 프레임을 검색할 수도 있다. 예컨대, 네트워크 인터페이스 장치는 이진 데이터 프레임을 마지막 부분부터 역으로 검색할 수도 있고, 이진 데이터 프레임을 일정하게 분할하고 분할한 영역별(즉 복수의 세그먼트)로 검색할 수도 있다. 다만 설명의 편의를 위해 네트워크 인터페이스 장치는 이진 데이터 프레임의 처음부분부터 검색하여 타겟 스트링과 동일한 부분을 찾다고 가정한다. 네트워크 인터페이스 장치가 이진 데이터 프레임에서 타겟 스트링과 동일한 부분으로 선택한 부분을 기준 스트링이라고 명명한다.

[0032] 이제 도 1(a)와 같이 IP_1 과 이진 데이터 프레임 사이의 상대적인 위치가 고정된다. 즉 IP_1 과 이진 데이터 프레임이 나란히 놓인다. 이후 네트워크 인터페이스 장치는 기준 스트링을 제외한 IP_1 의 호스트 번호 부분과 타겟 스트링을 제외하고 호스트 번호 부분과 나란히 놓인 이진 데이터 프레임의 일부를 XOR 연산한다. 도 1(a)와 같이 기준 스트링을 제외하고도 호스트 번호 부분의 일부는 XOR 연산이 수행되지 않을 수 있다. IP_1 에 대한 이진 데이터 프레임의 상대적인 위치가 달라질 수 있기 때문이다. 네트워크 인터페이스 장치는 최종적으로 의 XOR 연산으로 생성된 이진열을 나머지 호스트 번호 부분에 연결(overwrite)한다. 네트워크 인터페이스 장치는 새로운 IP 주소인 IP_1' 를 생성하였다.

[0033] 도 1(b)는 IP_2 을 기준으로 네트워크 인터페이스 장치가 IP 주소를 식명화하는 과정에 대한 예이다. 네트워크 인터페이스 장치는 도 1(a)에서 설명한 과정과 동일한 과정을 IP_2 에 대해서 수행한다. 도 1(b)에서 IP_2 의 호스트 번호 부분과 이진 데이터 프레임의 상대적인 위치가 도 1(a)와는 상이하다.

[0034] 네트워크 인터페이스 장치는 IP 주소에 대한 식명화를 완료하면, 식명화된 IP 주소(IP_1' 및 IP_2') 및 길이 l 인 서브 스트링(기준 스트링)을 맵핑하여 저장한다.

[0035] 도 1은 사용자(기기)의 주소를 식명화하는 것을 예로 설명하였다. 그러나 도 1의 기법은 반드시 사용자 주소 외에도 다른 객체에 대한 주소를 식명화하는데 사용될 수 있다. 예컨대, 특정 서버의 주소도 식명화하는데 사용할 수 있다.

[0037] 도 3은 IP 네트워크에서 식명화를 이용한 패킷 라우팅 과정(200)에 대한 절차 흐름도의 예이다. 도 3은 CDNi에서 사용자가 콘텐츠를 요청하는 과정을 예로 도시하였다. 사용자(기기)는 콘텐츠를 요청하는 일정한 패킷을 자신의 서브넷에 속한 네트워크 인터페이스 장치에 전달한다(201). 네트워크 인터페이스 장치는 도 1에서 설명한 방법으로 사용자의 IP 주소를 식명화한다(211). 네트워크 인터페이스 장치는 식명화된 IP 주소인 IP' 를 포함하는 패킷을 오리진 서버(uCDN)에 전달한다(212). uCDN은 업스트림 CDN을 의미한다. uCDN은 IP' 를 기준으로 콘텐츠를 사용자에게 제공할 수 있는 dCDN을 검색한다(221). dCDN은 다운 스트림 CDN을 의미한다. uCDN은 가장 적절한 dCDN에 콘텐츠 요청을 전달(redirection)한다(222). dCDN은 IP' 를 기준으로 사용자에게 가장 가까운 에지 서버를 결정한다(231). dCDN은 결정한 에지 서버를 통해 콘텐츠를 네트워크 인터페이스 장치에 전달한다(241). 네트워크 인터페이스 장치는 식명화 과정에서 생성한 맵핑 테이블을 이용하여 식명화된 IP' 를 원래의 IP로 변환한다(251). 이후 네트워크 인터페이스 장치는 원래의 IP를 이용하여 사용자에게 콘텐츠를 전달한다(261).

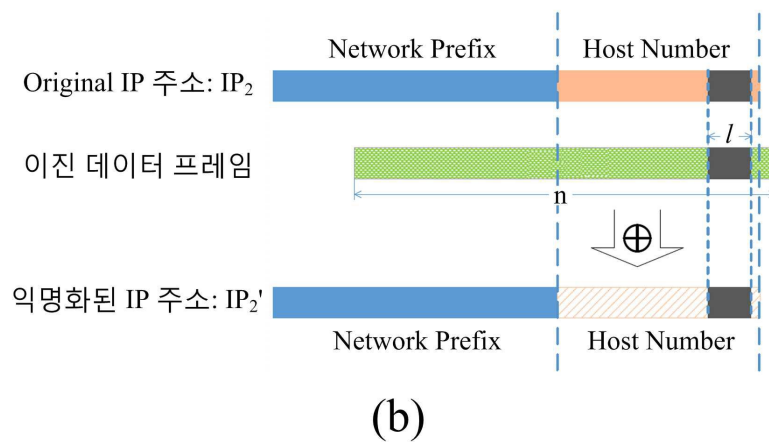
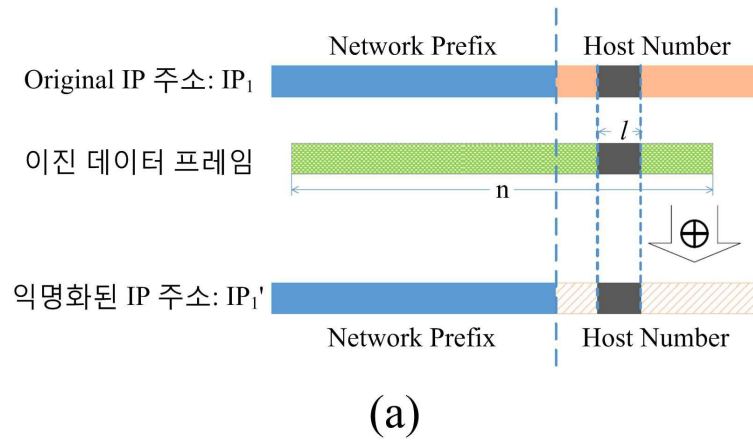
[0039] 도 4는 네트워크 인터페이스 장치가 식명화된 IP 주소를 원래의 IP주소로 변환하는 과정에 대한 예이다. 도 4는 네트워크 인터페이스 장치는 식명화된 주소 IP_1' 를 포함하는 패킷을 수신한 예이다. 네트워크 인터페이스 장치는 IP_1' 의 호스트 번호 부분을 기준으로 매칭되는 l 길이의 서브 스트링(기준 스트링)을 찾는다. 이제 네트워크 인터페이스 장치는 기준 스트링을 기준으로 이진 데이터 프레임에서 최초로 기준 스트링과 일치하는 부분(타겟 스트링)을 찾는다. 도 4를 살펴보면 도 1(a)와 유사하게 IP_1' 과 이진 데이터 프레임이 나란히 놓인 것을 알 수 있다. 즉, IP_1' 과의 관계에서 이진 데이터 프레임은 고정된 위치에 배치된 것이다. 이제 네트워크 인터페이스 장치는 IP_1' 의 호스트 번호 부분에서 기준 스트링 부분을 제외하고 나머지 부분을 이진 데이터 프레임과 XOR 연산한다. 최종적으로 IP_1' 은 원래의 IP 주소인 IP_1 으로 변환되었다.

[0041]

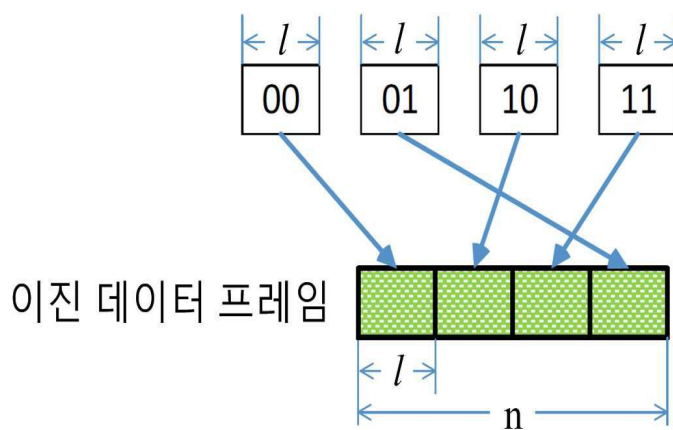
본 실시예 및 본 명세서에 첨부된 도면은 전술한 기술에 포함되는 기술적 사상의 일부를 명확하게 나타내고 있는 것에 불과하며, 전술한 기술의 명세서 및 도면에 포함된 기술적 사상의 범위 내에서 당업자가 용이하게 유추할 수 있는 변형 예와 구체적인 실시예는 모두 전술한 기술의 권리범위에 포함되는 것이 자명하다고 할 것이다.

도면

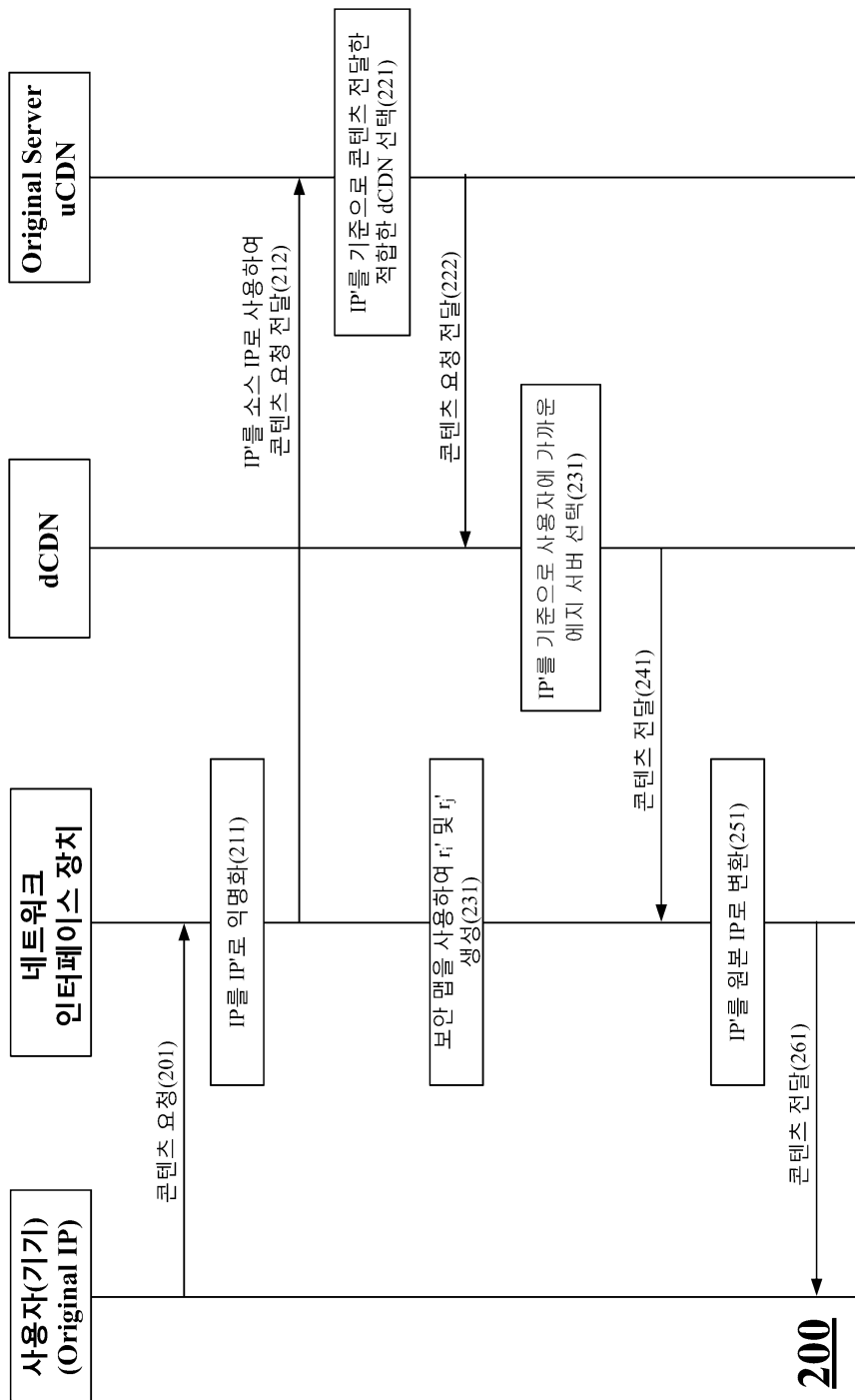
도면1



도면2



도면3



도면4

