



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년11월21일
(11) 등록번호 10-2047585
(24) 등록일자 2019년11월15일

(51) 국제특허분류(Int. Cl.)
H04L 12/26 (2006.01) H04L 12/841 (2013.01)
H04L 29/06 (2006.01) H04L 29/08 (2006.01)
(52) CPC특허분류
H04L 43/0852 (2013.01)
H04L 43/16 (2013.01)
(21) 출원번호 10-2016-7017704
(22) 출원일자(국제) 2015년01월07일
심사청구일자 2018년07월04일
(85) 번역문제출일자 2016년07월01일
(65) 공개번호 10-2016-0106062
(43) 공개일자 2016년09월09일
(86) 국제출원번호 PCT/US2015/010434
(87) 국제공개번호 WO 2015/105842
국제공개일자 2015년07월16일
(30) 우선권주장
201410008844.0 2014년01월08일 중국(CN)
(56) 선행기술조사문헌
US20060098586 A1*
US20060203808 A1
US20070192845 A1*
US20090144408 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
알리바바 그룹 홀딩 리미티드
케이만군도, 그랜드 케이만, 피오박스 847, 원 캐
피탈 플레이스 4층
(72) 발명자
후알 미안
중국 311121 항조우 유 항 디스트릭트 웨스트 웨
위 로드 넘버 969 빌딩 3 5/에프 알리바바 그룹
리갈 디파트먼트
(74) 대리인
제일특허법인(유)

전체 청구항 수 : 총 20 항

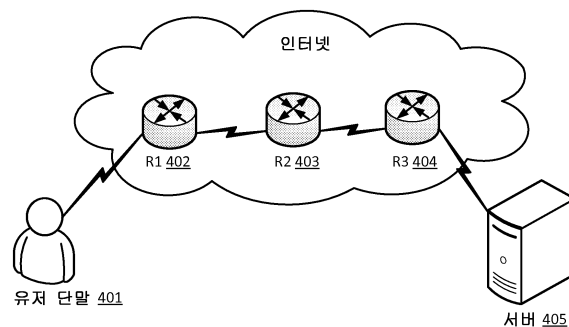
심사관 : 전용해

(54) 발명의 명칭 프록시 IP 어드레스를 식별하는 방법 및 장치

(57) 요약

프록시 IP 어드레스를 식별하는 방법 및 장치. 그 방법은: IP 어드레스를 유저 IP 어드레스로서 사용하여 서버와의 TCP 연결을 확립하는 단말과 서버 사이의 제1 네트워크 지연을 결정하는 것; IP 어드레스까지 한 홉 이전에 있는 라우터와 서버 사이의 제2 네트워크 지연을 결정하는 것; 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치보다 더 큰지 여부를 결정하는 것; 및 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치보다 더 큰 경우 IP 어드레스를 프록시 IP 어드레스로서 식별하는 것을 포함한다. 본 개시의 기술적 솔루션을 사용하여, IP 어드레스가 프록시 IP 어드레스인지의 여부를 식별하는 것은 빠르고 정확하게 이루어질 수 있다.

대표도 - 도4a



(52) CPC특허분류

H04L 47/286 (2013.01)

H04L 67/16 (2013.01)

H04L 69/16 (2013.01)

명세서

청구범위

청구항 1

하나 이상의 컴퓨팅 디바이스에 의해 구현되는 방법으로서,

인터넷 프로토콜(Internet Protocol; IP) 어드레스를 유저 IP 어드레스로서 사용하여 서버와의 전송 제어 프로토콜(Transmission Control Protocol; TCP) 연결을 확립하는 단말과 상기 서버 사이의 제1 네트워크 지연을 결정하는 단계와,

상기 TCP 연결을 확립하기 위하여 상기 서버에서 수신된 상기 유저 IP 어드레스를 사용하여, 상기 서버에서 수신된 상기 유저 IP 어드레스까지 하나의 홉 이전에 있는 라우터와 상기 서버 사이의 제2 네트워크 지연을 결정하는 단계 - 상기 TCP 연결을 확립하기 위하여 상기 서버에서 수신된 상기 유저 IP 어드레스는 상기 서버로부터 구축되어 전송되는 증분적(incremental) 수명 시간(TTL)을 구비하는 일련의 검출 패킷에서 목표 어드레스로 사용됨 - 와,

상기 제1 네트워크 지연과 상기 제2 네트워크 지연 사이의 비율이 임계치보다 더 큰지 여부를 결정하는 단계와,

상기 제1 네트워크 지연과 상기 제2 네트워크 지연 사이의 비율이 상기 임계치보다 더 큰지 여부의 결정의 결과에 기초하여 상기 유저 IP 어드레스를 프록시 IP 어드레스 또는 비프록시 IP 어드레스로서 식별하는 단계를 포함하는

방법.

청구항 2

제 1 항에 있어서,

상기 제1 네트워크 지연과 상기 제2 네트워크 지연 사이의 비율이 상기 임계치보다 더 크다는 결정에 응답하여 상기 유저 IP 어드레스를 상기 프록시 IP 어드레스로서 식별하는 단계를 더 포함하는

방법.

청구항 3

제 1 항에 있어서,

상기 제1 네트워크 지연과 상기 제2 네트워크 지연 사이의 비율이 상기 임계치 이하라는 결정에 응답하여 상기 유저 IP 어드레스를 상기 비프록시 IP 어드레스로서 식별하는 단계를 더 포함하는

방법.

청구항 4

제 1 항에 있어서,

상기 제1 네트워크 지연을 결정하는 단계는, SYN-ACK 패킷을 상기 단말로 전송하는 시간과 상기 단말로부터 ACK 패킷을 수신하는 시간 사이의 시간차를 제1 네트워크 지연으로서 결정하는 단계를 포함하는

방법.

청구항 5

제 1 항에 있어서,

상기 제1 네트워크 지연을 결정하는 단계는,

 SYN-ACK 패킷을 상기 단말로 전송하는 제1 시점을 기록하는 단계와,

 상기 단말로부터 ACK 패킷을 수신하는 제2 시점을 기록하는 단계와,

 상기 제2 시점과 상기 제1 시점 사이의 시간차를 상기 제1 네트워크 지연으로서 결정하는 단계를 포함하는 방법.

청구항 6

제 1 항에 있어서,

상기 제2 네트워크 지연을 결정하는 단계는, 상기 유저 IP 어드레스까지 하나의 홉 이전에 있는 상기 라우터로부터 인터넷 제어 메시지 프로토콜(Internet control message protocol; ICMP) 에러 패킷을 수신하는 시간과 상기 ICMP 에러 패킷에 대응하는 검출 패킷을 전송하는 시간 사이의 시간차를 상기 제2 네트워크 지연으로서 결정하는 단계를 포함하는

방법.

청구항 7

제 6 항에 있어서,

상기 일련의 검출 패킷은 상기 ICMP 에러 패킷을 포함하는

방법.

청구항 8

제 1 항에 있어서,

상기 제2 네트워크 지연을 결정하는 단계는,

 충분적 수명 시간(TTL)을 가지며 목표 어드레스가 상기 유저 IP 어드레스인 일련의 검출 패킷에서의 각각의 검출 패킷을 전송하는 시간을 기록하는 단계와,

 상기 유저 IP 어드레스까지 하나의 홉 이전에 있는 상기 라우터로부터 인터넷 제어 메시지 프로토콜(ICMP) 에러 패킷을 수신하는 제4 시점을 기록하는 단계와,

 상기 ICMP 에러 패킷에 대응하는 검출 패킷을 전송하는 시간을 제3 시점으로서 정의하는 단계와,

 상기 제4 시점과 상기 제3 시점 사이의 시간차를 상기 제2 네트워크 지연으로서 결정하는 단계를 포함하는 방법.

청구항 9

프록시 IP 어드레스를 식별하는 장치로서,

하나 이상의 프로세서와,

메모리와,

인터넷 프로토콜(IP) 어드레스를 유저 IP 어드레스로서 사용하여 서버와의 전송 제어 프로토콜(TCP) 연결을 확립하는 단말과 상기 서버 사이의 제1 네트워크 지연을 결정하는, 상기 메모리에 저장되며 상기 하나 이상의 프로세서에 의해 실행가능한 제1 결정 모듈과,

상기 TCP 연결을 확립하기 위하여 상기 서버에서 수신된 상기 유저 IP 어드레스를 사용하여, 상기 서버에서 수신된 상기 유저 IP 어드레스까지 하나의 홉 이전에 있는 라우터와 상기 서버 사이의 제2 네트워크 지연을 결정하는, 상기 메모리에 저장되며 상기 하나 이상의 프로세서에 의해 실행가능한 제2 결정 모듈 - 상기 TCP 연결을 확립하기 위하여 상기 서버에서 수신된 상기 유저 IP 어드레스는 상기 서버로부터 구축되어 전송되는 증분적(incremental) 수명 시간(TTL)을 구비하는 일련의 검출 패킷에서 목표 어드레스로 사용됨 - 과,

상기 제1 네트워크 지연과 상기 제2 네트워크 지연 사이의 비율이 임계치보다 더 큰지 여부를 결정하는, 상기 메모리에 저장되며 상기 하나 이상의 프로세서에 의해 실행가능한 판정 모듈과,

상기 제1 네트워크 지연과 상기 제2 네트워크 지연 사이의 비율이 상기 임계치보다 더 큰지 여부의 결정의 결과에 기초하여 상기 유저 IP 어드레스를 프록시 IP 어드레스 또는 비프록시 IP 어드레스로서 식별하는, 상기 메모리에 저장되며 상기 하나 이상의 프로세서에 의해 실행가능한 식별 모듈을 포함하는

장치.

청구항 10

제 9 항에 있어서,

상기 식별 모듈은, 상기 제1 네트워크 지연과 상기 제2 네트워크 지연 사이의 비율이 상기 임계치보다 더 크다는 결정에 응답하여 상기 유저 IP 어드레스를 상기 프록시 IP 어드레스로서 식별하는

장치.

청구항 11

제 9 항에 있어서,

상기 식별 모듈은, 상기 제1 네트워크 지연과 상기 제2 네트워크 지연 사이의 비율이 상기 임계치 이하라는 결정에 응답하여 상기 유저 IP 어드레스를 상기 비프록시 IP 어드레스로서 식별하는

장치.

청구항 12

제 9 항에 있어서,

상기 제1 결정 모듈은 또한, SYN-ACK 패킷을 상기 단말로 전송하는 시간과 상기 단말로부터 ACK 패킷을 수신하는 시간 사이의 시간차를 제1 네트워크 지연으로서 결정하는

장치.

청구항 13

제 9 항에 있어서,

상기 제1 결정 모듈은,

SYN-ACK 패킷을 상기 단말로 전송하는 제1 시점을 기록하는 제1 기록 서브 모듈과,

상기 단말로부터 ACK 패킷을 수신하는 제2 시점을 기록하는 제2 기록 서브 모듈과,

상기 제2 시점과 상기 제1 시점 사이의 시간차를 상기 제1 네트워크 지연으로서 결정하는 제1 결정 서브 모듈을 더 포함하는 장치.

청구항 14

제 9 항에 있어서,

상기 제2 결정 모듈은 또한, 상기 IP 어드레스까지 하나의 홉 이전에 있는 상기 라우터로부터 인터넷 제어 메시지 프로토콜(ICMP) 에러 패킷을 수신하는 시간과 일련의 검출 패킷에서 상기 ICMP 에러 패킷에 대응하는 검출 패킷을 전송하는 시간 사이의 시간차를, 상기 IP 어드레스까지 하나의 홉 이전에 있는 상기 라우터와 상기 서버 사이의 상기 제2 네트워크 지연으로서 결정하는

장치.

청구항 15

제 9 항에 있어서,

상기 제2 결정 모듈은,

일련의 검출 패킷에서의 각각의 검출 패킷을 전송하는 시간을 기록하는 제3 기록 서브 모듈과,

상기 IP 어드레스까지 하나의 홉 이전에 있는 상기 라우터로부터 인터넷 제어 메시지 프로토콜(ICMP) 에러 패킷을 수신하는 제4 시점을 기록하는 제4 기록 서브 모듈과,

상기 일련의 검출 패킷에서 상기 ICMP 에러 패킷에 대응하는 상기 검출 패킷을 전송하는 시간을 제3 시점으로서 정의하는 제1 정의 서브 모듈과,

상기 제4 시점과 상기 제3 시점 사이의 시간차를 상기 제2 네트워크 지연으로서 결정하는 제2 결정 서브 모듈을 더 포함하는

장치.

청구항 16

실행가능 명령어를 저장하는 하나 이상의 컴퓨터 판독가능 매체로서,

상기 실행가능 명령어는, 하나 이상의 프로세서에 의한 실행시, 상기 하나 이상의 프로세서로 하여금,

인터넷 프로토콜(Internet Protocol; IP) 어드레스를 유저 IP 어드레스로서 사용하여 서버와의 전송 제어 프로토콜(Transmission Control Protocol; TCP) 연결을 확립하는 단말과 서버 사이의 제1 네트워크 지연을 결정하는 것과,

상기 TCP 연결을 확립하기 위하여 상기 서버에서 수신된 상기 유저 IP 어드레스를 사용하여, 상기 서버에서 수신된 상기 유저 IP 어드레스까지 하나의 홉 이전에 있는 라우터와 상기 서버 사이의 제2 네트워크 지연을 결정하는 것 - 상기 TCP 연결을 확립하기 위하여 상기 서버에서 수신된 상기 유저 IP 어드레스는 상기 서버로부터 구축되어 전송되는 증분적(incremental) 수명 시간(TTL)을 구비하는 일련의 검출 패킷에서 목표 어드레스로 사용됨 - 과,

상기 제1 네트워크 지연과 상기 제2 네트워크 지연 사이의 비율이 임계치보다 더 큰지 여부를 결정하는 것과,

상기 제1 네트워크 지연과 상기 제2 네트워크 지연 사이의 비율이 상기 임계치보다 더 크다는 결정에

응답하여 상기 유저 IP 어드레스를 프록시 IP 어드레스로서 식별하는 것을 포함하는 동작을 수행하게 하는 컴퓨터 판독가능 매체.

청구항 17

제 16 항에 있어서,

상기 제1 네트워크 지연을 결정하는 것은, SYN-ACK 패킷을 상기 단말로 전송하는 시간과 상기 단말로부터 ACK 패킷을 수신하는 시간 사이의 시간차를 제1 네트워크 지연으로서 결정하는 것을 포함하는

컴퓨터 판독가능 매체.

청구항 18

제 16 항에 있어서,

상기 제1 네트워크 지연을 결정하는 것은,

SYN-ACK 패킷을 상기 단말로 전송하는 제1 시점을 기록하는 것과,

상기 단말로부터 ACK 패킷을 수신하는 제2 시점을 기록하는 것과,

상기 제2 시점과 상기 제1 시점 사이의 시간차를 상기 제1 네트워크 지연으로서 결정하는 것을 포함하는

컴퓨터 판독가능 매체.

청구항 19

제 16 항에 있어서,

상기 제2 네트워크 지연을 결정하는 것은, 상기 유저 IP 어드레스까지 하나의 홉 이전에 있는 상기 라우터로부터 인터넷 제어 메시지 프로토콜(ICMP) 에러 패킷을 수신하는 시간과 상기 ICMP 에러 패킷에 대응하는 검출 패킷을 전송하는 시간 사이의 시간차를 상기 제2 네트워크 지연으로서 결정하는 것을 포함하고, 일련의 검출 패킷은 상기 ICMP 에러 패킷을 포함하는

컴퓨터 판독가능 매체.

청구항 20

제 16 항에 있어서,

상기 제2 네트워크 지연을 결정하는 것은,

증분적 수명 시간(TTL)을 가지며 목표 어드레스가 상기 유저 IP 어드레스인 일련의 검출 패킷에서의 각각의 검출 패킷을 전송하는 시간을 기록하는 것과,

상기 유저 IP 어드레스까지 하나의 홉 이전에 있는 상기 라우터로부터 인터넷 제어 메시지 프로토콜(ICMP) 에러 패킷을 수신하는 제4 시점을 기록하는 것과,

상기 ICMP 에러 패킷에 대응하는 검출 패킷을 전송하는 시간을 제3 시점으로서 정의하는 것과,

상기 제4 시점과 상기 제3 시점 사이의 시간차를 제2 네트워크 지연으로서 결정하는 것을 포함하는

컴퓨터 판독가능 매체.

발명의 설명

기술 분야

[0001] 관련 특허 출원에 대한 교차 참조

[0002] 본 출원은 2014년 1월 8일자로 출원된 발명의 명칭이 "Method and Apparatus Identifying Proxy IP Address"인 중국 특허 출원 제201410008844.0호에 대한 외국 우선권을 주장하는데, 상기 출원은 그 전체가 참조에 의해 통합된다.

[0003] 기술 분야

[0004] 본 개시는 인터넷 기술의 분야에 관한 것으로, 특히, 프록시 IP 어드레스를 식별하는 방법 및 장치에 관한 것이다.

배경 기술

[0005] 최근, 널리 사용되는 애플리케이션, 즉, IP(즉, 인터넷 프로토콜(Internet Protocol)) 어드레스 및 지리적 위치를 상호 질의하는 기술이 인터넷에서 존재한다. 이 기술은 인터넷의 다양한 분야에서 폭넓게 적용되며, 특히 위험 제어(risk control)의 분야에서 강한 위험 인자로서 사용된다. 다시 말하면, 위험 제어 분야의 솔루션에서 상호 질의하는 기술에 의해 사용되는 원칙은: 짧은 시간 기간 내에 상이한 지리적 위치에서 사용자가 로그인했는지의 여부를 결정하는 것, 및 긍정이면 고위험 동작으로 간주하는 것을 포함한다. 이 결정은, 유저의 IP가 진짜 IP인 경우에만 유효하다. 그러나, 프록시 서버 기술은 이 애플리케이션의 전체를 무너뜨린다. 다시 말하면, 베이징(Beijing)에 있는 유저가 프록시 서버를 통해 항저우(Hangzhou)에서 인터넷에 액세스할 수도 있으며, 서버가 봤을 때의 유저 IP 어드레스는 항저우 프록시 서버의 어드레스이다. 본 개시는 이러한 타입의 상황을 주로 식별하여, 유저가 프록시 서버를 사용하는지의 여부를 구별한다. 다시 말하면, IP 어드레스가 한 지리적 위치에 위치한 단말의 진짜 IP 어드레스인지 또는 프록시 서버의 IP 어드레스, 예를 들면, VPN(즉, 가상 사설 네트워크(Virtual Private Network)) 프록시 서버의 IP 어드레스인지의 여부에 관한 결정이 이루어진다.

[0006] 이 문제는 인터넷 분야에서 끊임없이 논의되어 왔고, 이 문제를 대상으로 한 몇몇 솔루션이 이 분야에서 존재한다. 그러나, 이들 솔루션은 주로 두 개의 방침에 초점을 맞춘다: 첫째, 인터넷에서 크롤러(crawler)에 의한 추출에 기초하여 또는 프록시 서버의 능동 스캐닝(active scanning)에 기초하여 수행되는 프록시 서버 리스트의 수집; 및 둘째, 기지의(known) 프록시 포트(들)가 개방되어 있는지의 여부를 결정하기 위해 현재 인터넷에 있는 모든 호스트를 역으로 스캔하는 역 검출. 첫 번째 아이디어의 솔루션은 크롤러에 의한 인터넷에서의 프록시 서버의 추출을 통해 프록시 서버를 수집한다. 그러나, 그 정보는, 많은 프록시 서버가 인터넷에서 공개되어 있지 않거나 해커에 의해 제어되는 익스플로잇(exploit)이기 때문에, 극도로 불완전하다. 두 번째 아이디어의 솔루션은, 몇몇 공통 프록시 포트가 개방되어 있는지의 여부를 결정하기 위해 모든 IP를 역 스캐닝하는 원칙을 갖는 역 검출에 기초한다. 그러나, 인터넷에서의 활성 호스트의 수가 아주 많고 프록시 서버의 서비스 포트가 고정되지 않기 때문에, 이 솔루션은 아주 긴 스캐닝 사이클을 갖는다.

[0007] 따라서, 현재로서는, IP 어드레스가 프록시 IP 어드레스인지의 여부를 빠르고 정확하게 식별할 수 있는 방법이 바람직할 수도 있다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0008] 이 개요는 하기 상세한 설명에서 더 설명되는 엄선된 개념을 간소화된 형태로 소개하기 위해 제공된다. 이 개요는 청구된 주제의 주요한 피쳐(feature) 또는 본질적인 피쳐를 식별하도록 의도된 것도 아니고, 청구된 주제의 범위를 결정함에 있어서의 보조로서 단독으로 사용되도록 의도된 것도 아니다. 용어 "기술"은, 예를 들면, 본 개시의 전체를 통해 그리고 상기의 맥락에 의해 허용되는 바와 같은 디바이스(들), 시스템(들), 방법(들) 및/또는 컴퓨터 판독가능 명령어를 가리킬 수도 있다.

[0009] 본 개시의 주요 목적은, 현존하는 기술에서의 상기 문제점을 해결하기 위해 IP 어드레스를 식별하는 방법을 제공하는 것이다.

[0010] 본 개시는 프록시 IP 어드레스를 식별하는 방법을 제공하는데, 그 방법은: IP 어드레스를 유저 IP 어드레스로서 사용하여 서버와의 TCP(즉, 전송 제어 프로토콜(Transmission Control Protocol)) 연결을 확립하는 단말과 서버 사이의 제1 네트워크 지연을 결정하는 것; IP 어드레스까지 한 홉 이전에 있는 라우터와 서버 사이의 제2 네트워크 지연을 결정하는 것; 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치보다 더 큰지 여부를 결정하는 것; 및 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치보다 더 큰 경우 IP 어드레스를 프록시 IP 어드레스로서 식별하는 것을 포함한다.

[0011] 본 개시의 다른 양태는 프록시 IP 어드레스를 식별하는 장치를 제공하는데, 그 장치는: IP 어드레스를 유저 IP 어드레스로서 사용하여 서버와의 TCP 연결을 확립하는 단말과 서버 사이의 제1 네트워크 지연을 결정하기 위해 사용되는 제1 결정 모듈; IP 어드레스까지 한 홉 이전에 있는 라우터와 서버 사이의 제2 네트워크 지연을 결정하기 위해 사용되는 제2 결정 모듈; 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치보다 더 큰지 여부를 결정하기 위해 사용되는 판정 모듈; 및 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치보다 더 큰 경우 IP 어드레스를 프록시 IP 어드레스로서 식별하기 위해 사용되는 식별 모듈을 포함한다.

[0012] 현존하는 기술과 비교하여, 본 개시의 기술적 솔루션에 따르면, 제1 네트워크 지연(이것은 IP 어드레스를 유저 IP 어드레스로서 사용하여 서버와의 TCT 연결을 확립하는 단말과 서버 사이에 있음)과 제2 네트워크 지연(이것은 IP 어드레스까지 한 홉 이전에 있는 라우터와 서버 사이에 있음) 사이의 비율이 임계치보다 더 크다는 것을 결정하는 것에 의해, IP 어드레스는 프록시 IP 어드레스로서 식별되고, 따라서 프록시 IP 어드레스를 빠르고 정확하게 식별하게 된다.

도면의 간단한 설명

[0013] 본원에서 설명되는 첨부 도면은, 본 개시의 추가적인 이해를 위해 사용되며 본 개시의 일부로서 취급된다. 그 예시적인 실시형태 및 설명은 본 개시를 설명하기 위해 사용되는 것이며 본 개시의 제한으로서 간주되어선 안된다. 첨부 도면에서:

도 1은, 본 개시의 한 실시형태에 따른, 프록시 IP 어드레스를 식별하는 방법을 예시하는 플로우차트이다.

도 2는, 본 개시의 한 실시형태에 따른, 프록시 IP 어드레스를 식별하는 방법에서 제1 네트워크 지연을 결정하는 플로우차트이다.

도 3은, 본 개시의 한 실시형태에 따른, 프록시 IP 어드레스를 식별하는 방법에서 제2 네트워크 지연을 결정하는 플로우차트이다.

도 4a는, 본 개시의 한 실시형태에 따른, 네트워크를 통해 서버에 직접 연결되는 단말을 예시하는 개략도이다.

도 4b는, 본 개시의 한 실시형태에 따른, 프록시를 통해 서버에 간접적으로 연결되는 단말을 예시하는 개략도이다.

도 5는, 본 개시의 한 실시형태에 따른, 프록시 IP 어드레스를 식별하는 장치를 예시하는 구조도이다.

도 6은, 도 5에서 설명되는 장치를 더 상세히 예시하는 구조도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 본 개시의 주요 아이디어는, IP 어드레스를 유저 IP 어드레스로서 사용하여 서버와의 TCP 연결을 확립하는 단말과 서버 사이의 제1 네트워크 지연을 결정하고, IP 어드레스까지 하나의 홉 이전에 있는 라우터와 서버 사이의 제2 네트워크 지연을 결정하는 것에 의해, 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치보다 더 큰지 여부에 관한 결정이 이루어진다는 것이다. 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치보다 더 크면, IP 어드레스는 프록시 IP 어드레스로서 식별된다.

[0015] 본 개시의 목적, 기술적 솔루션 및 이점을 더 명확하게 하기 위해, 본 개시의 기술적 솔루션은, 본 개시의 예시적인 실시형태 및 대응하는 첨부 도면을 사용하여 명확하고 포괄적인 방식으로 설명된다. 명백하게, 설명되는 실시형태는, 본 개시의 실시형태의 전체가 아니라 일부를 나타내는 것에 불과하다. 본 개시에서의 실시형태에 기초하여, 창조적 노력 없이 당업자에 의해 유도되는 모든 다른 실시형태는 본 개시의 보호 범위 안에 있을 것

이다.

- [0016] 본 개시의 한 실시형태에 따르면, 프록시 IP 어드레스를 식별하는 방법이 제공된다.
- [0017] 도 1을 참조하면, 도 1은, 본 개시의 한 실시형태에 따른, 프록시 IP 어드레스를 식별하는 방법을 예시하는 플로우차트이다. 도 1에서 도시되는 바와 같이, IP 어드레스를 유저 IP 어드레스로서 사용하여 서버와의 TCP 연결을 확립하는 단말과 서버 사이의 제1 네트워크 지연이 블록 S101에서 결정된다.
- [0018] 한 실시형태에서, IP 어드레스가 프록시 IP 어드레스인지의 여부를 식별하기 위해, IP 어드레스를 단말의 유저 IP 어드레스로서 사용하여 서버와의 TCP 연결을 확립하려고 시도하는 진짜 단말과 서버 사이의 제1 네트워크 지연이 먼저 획득될 필요가 있다.
- [0019] 도 2를 참조하여, 제1 네트워크 지연을 어떻게 획득하는지의 예시적인 방법을 예시하는 플로우차트가 이하 상세히 설명된다.
- [0020] 제1 네트워크 지연의 의미를 더 명확하게 이해하기 위해, 단말과 서버 사이에서 TCP 연결을 확립하기 위해 수행되는 3웨이 핸드셰이크(three-way handshake)의 프로세스가 먼저 소개된다. 3웨이 핸드셰이크는, 말하자면, TCP 연결을 확립할 때 클라이언트와 서버 사이에서 총 세 개의 패킷을 전송하는 필요성을 지칭한다. 3웨이 핸드셰이크의 목표는, 서버의 지정된 포트를 연결하는 것 및 TCP 연결을 확립하는 것이다. 제1 핸드셰이크에서, 단말은, SYN(Synchronize Sequence Numbers; 동기화 시퀀스 번호) 플래그를 포함하는 TCP 패킷을 서버로 전송한다. 이것은 3웨이 핸드셰이크의 프로세스에서 제1 패킷이며, 본 개시에서 SYN 패킷으로 칭해진다. 제2 핸드셰이크에서, 서버 단(server end)은 단말에 응답하고, SYN-ACK 패킷을 단말로 전송한다. 이것은 3웨이 핸드셰이크 프로세스에서의 제2 패킷이다. 이 패킷은 ACK 플래그 및 SYN 플래그를 동시에 포함하며, 따라서 클라이언트의 SYN 패킷에 대한 응답을 나타내고 또한 클라이언트가 데이터 통신을 행하기 위한 준비가 되어 있는지의 여부를 질의하기 위해 클라이언트에 대한 SYN을 마킹한다. 제3 핸드셰이크에서, 단말은 응답으로 ACK 패킷(즉, 3웨이 핸드셰이크의 확인응답(acknowledgement) 패킷)을 서버로 전송할 필요가 있다. 이것은, 단말이 데이터 통신을 행할 준비가 되었다는 것을 나타내는 제3 패킷이다. 이 3웨이 핸드셰이크를 통해, TCP 연결이 확립된다. 본 개시는, 서버에 의한 SYN-ACK의 전송과 단말로부터 리턴되는 ACK 패킷 사이의 제1 네트워크 지연을 획득하기 위해, 단말과 서버 사이에 TCP 연결을 확립하는 3웨이 핸드셰이크의 프로세스를 활용한다. 제1 네트워크 지연을 획득하는 방법의 상세가 이하 설명된다.
- [0021] 서버는 IP 어드레스를 유저 IP 어드레스로서 사용하는 단말로부터 SYN 패킷을 수신하고, 단말은 TCP 연결 확립을 요청한다. SYN 패킷을 수신한 이후, 서버는 SYN-ACK 패킷을 단말로 전송한다. 따라서, 도 2에서 도시되는 바와 같이, 블록 S201에서 서버는 SYN-ACK 패킷이 단말로 전송되는 때의 시간을 기록한다. 이 시간은, 예를 들면, 제1 시점으로서 정의될 수도 있다.
- [0022] 그 후, 서버는 단말로부터 ACK 패킷을 수신한다. 따라서, 블록 S202에서 서버는 단말로부터 ACK 패킷이 수신되는 때의 시간을 기록한다. 이 시간은, 예를 들면, 제2 시점으로서 정의될 수도 있다.
- [0023] 마지막으로, 블록 S203에서, SYN-ACK 패킷이 단말로 전송되는 때의 시간과 ACK 패킷이 단말로부터 수신되는 때의 시간 사이의 시간차가 제1 네트워크 지연으로서 결정된다. 다시 말하면, 제2 시점과 제1 시점 사이의 시간차가 제1 네트워크 지연으로서 정의된다.
- [0024] 상기 방법 블록을 통해, 서버와 단말 사이의 제1 네트워크 지연이 획득될 수도 있다.
- [0025] 다시 도 1을 참조하면, 제1 네트워크 지연의 결정시, IP 어드레스까지 하나의 홉 이전에 있는 라우터와 서버 사이의 제2 네트워크 지연이 블록 S102에서 결정된다.
- [0026] 제2 네트워크 지연은 다음의 원칙에 기초하여 획득된다.
- [0027] 서버 단은 유저 IP 어드레스를 ip1로서 기록할 수도 있고, 서버 단은 목표 IP를 ip1로서 갖는 1 내지 255인 수명 시간(time to live; ttl)을 각각 구비하는 일련의 검출 패킷(예를 들면, 255 개)을 구축할 수 있다. TCP/IP 프로토콜에 따르면, 이 일련의 검출 패킷이 라우터를 통과할 때마다, ttl은 1만큼 감소된다. ttl이 제로로 감소되는 경우에도 목표 어드레스가 도달되지 않으면, 그 라우터는 에러(error)를 보고하고, 인터넷 제어 메시지 프로토콜(Internet control message protocol; ICMP) 에러 패킷을 전송측(sender)으로 전송한다. 이와 같이, IP 어드레스까지 하나의 홉 이전의 라우터에 의해 전송되는 최종 ICMP 에러 패킷이 알려질 수도 있다. 따라서, 이 일련의 검출 패킷은, 분석을 통해 유저와 관련되는 이전 홉 라우터(previous-hop router)의 어드레스 및 네트워

크 지연을 획득하기 위해 사용될 수도 있다.

- [0028] 도 3을 참조하여, 제2 네트워크 지연을 어떻게 획득하는지의 예시적인 방법을 예시하는 플로우차트가 상세히 설명된다.
- [0029] 상기에서 설명된 바와 같이, 서버는, 목표 어드레스를 유저 IP 어드레스로서 갖는 증분적(incremental) 수명 시간(TTL)을 구비하는 일련의 검출 패킷을 구축하여 전송한다. 예를 들면, 상기에서 설명된 바와 같이, 목표 IP를 유저 IP 어드레스로서 갖는 1 내지 255인 증분적 수명 시간(TTL)을 구비하는 일련의 255개의 검출 패킷이 구축되어 전송될 수도 있다. 따라서, 도 3에서 도시되는 바와 같이, 일련의 검출 패킷의 각각의 검출 패킷을 전송하는 각각의 시간이 블록 S301에서 기록될 수도 있다.
- [0030] 후속하여, IP 어드레스까지 하나의 홉 이전에 있는 라우터에 의해 서버로 전송되는 ICMP 에러 패킷이 일련의 검출 패킷에 기초하여 획득된다. 상기에서 설명된 바와 같이, 예를 들면, 이 일련의 검출 패킷에서 수명 시간을 1로 구비하는 검출 패킷이 제1 라우터에 도달하는 경우, IP 어드레스가 도달되지 않았기 때문에 제1 ICMP 에러 패킷이 생성되어 전송된다. 제1 ICMP 에러 패킷은 서버에 의해 수신되고, 제1 에러 패킷을 수신하는 시간이 기록된다. 동일한 토큰에 의해, 예를 들면, 이 일련의 검출 패킷에서 수명 시간을 n 으로 구비하는 패킷이 제 n 라우터에 도달하는 경우, IP 어드레스가 도달되지 않았기 때문에 제 n ICMP 에러 패킷이 생성되어 전송된다. 제 n ICMP 에러 패킷은 서버에 의해 수신되고, 제 n 에러 패킷을 수신하는 시간이 기록된다. 이 일련의 검출 패킷에서 수명 시간을 $n+1$ 로 구비하는 패킷이 IP 어드레스에 도달하면, 어떠한 ICMP 에러 패킷도 생성되지 않는다. 따라서, 서버는, 제 n 라우터가 IP 어드레스까지 하나의 홉 이전에 있는 라우터이라는 것을 알게 되고, 따라서 제 n 에러 패킷을 수신하는 시간을, IP 어드레스까지 하나의 홉 이전에 있는 라우터로부터 서버로 전송되는 ICMP 에러 패킷을 수신하는 시간으로서 기록하게 된다. 다시 말하면, 블록 S302에서, IP 어드레스까지 하나의 홉 이전에 있는 라우터로부터 서버로 전송되는 ICMP 에러 패킷을 수신하는 시간이 기록된다. 예를 들면, 이 시간은 제4 시점으로서 정의될 수도 있다.
- [0031] 블록 S303에서, 일련의 검출 패킷에서 ICMP 에러 패킷에 대응하는 검출 패킷을 전송하는 시간은 제3 시점으로서 기록된다. 한 실시형태에서, ICMP 에러 패킷에 대응하는 검출 패킷이 발견될 수도 있고, 그 결과 이 대응하는 검출 패킷을 전송하는 시간이 알려지게 되고, 그 검출 패킷을 전송하는 시간이 제3 시점으로서 정의된다.
- [0032] 블록 304에서, IP 어드레스까지 하나의 홉 이전에 있는 라우터로부터 ICMP 에러 패킷을 수신하는 시간과 일련의 검출 패킷에서 ICMP 에러 패킷에 대응하는 검출 패킷을 전송하는 시간 사이의 시간차가, IP 어드레스까지 하나의 홉 이전에 있는 라우터와 서버 사이의 제2 네트워크 지연으로서 결정된다.
- [0033] 다시 말하면, 제4 시점과 제3 시점 사이의 시간차가 제2 네트워크 지연으로서 설정된다.
- [0034] 도 1을 다시 참조하면, 제1 네트워크 지연 및 제2 네트워크 지연을 결정하는 것에 응답하여, 블록 S103에서, 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치보다 더 큰지 여부에 관한 결정이 이루어진다.
- [0035] 정상 상황 하에서, 프록시 IP 어드레스를 사용하는 대신 단말의 유저 IP 어드레스를 사용하여 단말이 서버에 직접 연결되면, 단말과 서버 사이의 제1 네트워크 지연(T1)의 값은, 유저 IP 어드레스(즉, 단말의 IP 어드레스)의 이전 홉 라우터(R1)와 서버 사이의 제2 네트워크 지연(T2)의 값은 거의 동일하다. 따라서, T1 및 T2의 비율은 거의 1과 동일하다.
- [0036] 그러나, 유저가 임의의 프록시 서버를 사용하면, 서버에 의해 검출되는 소위 "유저 IP 어드레스"는 프록시 서버의 프록시 IP 어드레스이다. 따라서, 결정된 제2 네트워크 지연은, 소위 "유저 IP 어드레스"(이것은 프록시 서버의 실제 프록시 IP 어드레스임)의 이전 홉 라우터와 서버 사이의 시간 지연(T2')이다. T2'와 T1 사이의 차이는 크며, 그 결과 T1과 T2' 사이의 비율은, 임계치, 예를 들면 2이도록 설정되는 임계치보다 일반적으로 더 크다. 실제 필요에 따라 적절한 임계치가 설정될 수도 있다는 것을 유의해야 한다.
- [0037] 블록 S104에서, 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치보다 더 크면, IP 어드레스는 프록시 IP 어드레스로서 식별된다.
- [0038] 다시 말하면, 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치보다 더 크면, 두 지연 사이의 큰 차이 때문에, IP 어드레스는 단말의 IP 어드레스이라는 결정이 이루어질 수 있다. 단말은 프록시 서버의 프록시 IP 어드레스를 사용하여 서버에 액세스했고, 따라서 IP 어드레스는 프록시 IP 어드레스로서 식별된다. 옵션적으로, 프록시 서버는 VPN 프록시 서버일 수도 있고, 프록시 IP 어드레스는 본 개시에서 VPN 프록시 IP 어드레스일 수도 있다.

- [0039] 블록 105에서, 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치 이하이면, IP 어드레스는 비프록시(non-proxy) IP 어드레스로서 식별된다.
- [0040] 다시 말하면, 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치 이하이면, 두 지연 사이의 작은 차이 때문에 IP 어드레스는 단말의 IP 어드레스이며, 단말이 프록시 IP 어드레스를 사용하지 않고 서버에 액세스했다는 결정이 이루어질 수 있다. 따라서, IP 어드레스는 비프록시 IP 어드레스로서 식별된다.
- [0041] 본 개시의 실시형태의 기술적 솔루션을 명확하게 설명하기 위해, 도 4a 및 도 4b를 참조로 더 상세한 설명이 이하 이루어진다.
- [0042] 예를 들면, 도 4a에서 도시되는 바와 같이, 소정의 위치(A)에 위치한 단말(401)(제1 단말)이 SYN 패킷을 전송한다. SYN 패킷은, 예를 들면, 유저 단말의 셀을 통해 라우터(R1)(402)에 진입하고, 위치(A)의 백본 네트워크 익스포트(backbone network export), 예를 들면, 라우터(R2)(403)를 통과하고, 위치(B)의 백본 네트워크 익스포트, 예를 들면, 라우터(R3)(404)를 통과하고, 마지막으로 서버(405)에 도달하고, 서버는 SYN 패킷을 수신한다. 다시 말하면, 서버는, 제1 IP 어드레스를 유저 IP 어드레스로 사용하며 서버와의 TCP 연결 확립을 시도하는 제1 단말로부터 SYN 패킷을 수신한다. 서버는 제1 단말로 SYN-ACK 패킷을 전송하고, SYN-ACK 패킷을 제1 단말로 전송하는 제1 시간(시간1)을 기록한다. 그 후, 서버는 제1 단말로부터 ACK 패킷을 수신하고, 서버는 제1 단말로부터 ACK 패킷을 수신하는 제2 시간(시간2)을 기록한다. 따라서, 제1 네트워크 지연이 $T1 = \text{시간2} - \text{시간1}$ 인 것으로 결정된다. 도 4a로부터 알 수 있는 바와 같이, 네트워크 지연($T1$)은 서버와 라우터(R3) 사이의 지연, 라우터(R3과 R2) 사이의 지연, 라우터(R2와 R1) 사이의 지연, 및 라우터(R1)와 제1 단말 사이의 지연을 포함한다.
- [0043] 또한, 서버는, 예를 들면, 각각 1 내지 255인 수명 시간(tt1) 및 목표 IP 어드레스를 제1 IP 어드레스로서 갖는 일련의 255개의 검출 패킷을 구축하여 전송할 수도 있다. 따라서, 서버는 일련의 검출 패킷에서의 각각의 검출 패킷의 전송 시간을 기록할 수도 있다. 위에서 설명된 바와 같이, 서버는 또한, 제1 IP 어드레스(제1 단말의 IP 어드레스)의 이전 홉 라우터에 의해 전송되는 ICMP 에러 패킷을 수신하는 제4 시점(시간4)을 기록할 수도 있다. 또한, 이 ICMP 에러 패킷에 기초하여, 대응하는 검출 패킷의 전송 시간을 알기 위해, 대응하는 검출 패킷이 발견될 수도 있다. 다시 말하면, 일련의 검출 패킷에서 ICMP 에러 패킷에 대응하는 검출 패킷의 전송 시간은, 예를 들면, 제3 시점(시간3)으로서 정의된다. 따라서, 제2 네트워크 지연이 $T2 = \text{시간4} - \text{시간3}$ 인 것으로 결정된다. 도 4a로부터 알 수 있는 바와 같이, 네트워크 지연($T2$)은, 서버와 라우터(R3) 사이의 지연, 라우터(R3과 R2) 사이의 지연, 및 라우터(R2와 R1) 사이의 지연을 포함한다. 다시 말하면, $T1$ 과 $T2$ 사이의 차이는, 라우터와 제1 단말 사이의 지연에 불과하고, 그 차이는 상대적으로 작다.
- [0044] 도면으로부터 알 수 있는 바와 같이, 제1 IP 어드레스가 제1 단말의 진짜 어드레스이기 때문에, 획득된 $T1$ 및 $T2$ 의 결정된 값은 서로 비슷하며, $T1$ 과 $T2$ 사이의 비율은 임계치보다 더 크지 않다. 따라서, 제1 IP 어드레스가 프록시 IP 어드레스가 아니라는 결정이 이루어질 수도 있다. 본 개시의 기술적 솔루션으로부터 알 수 있는 바와 같이, 식별 결과는 실제 결과에 일치한다.
- [0045] 마찬가지로, 도 4b에서 도시되는 바와 같이, 제1 단말이 프록시에 의해 서버에 연결되면, 소정의 위치(A)에 위치되는 유저 단말(406)(제1 단말)이 SYN 패킷을 전송한다. SYN 패킷은, 예를 들면, 유저 단말(406)을 통해 라우터(R1)(407)에 진입하고, 위치(A)의 백본 네트워크 익스포트, 예를 들면, 라우터(R2)(408)를 통과하고, 소정의 위치(B)의 백본 네트워크 익스포트, 예를 들면, 라우터(R3)(409)를 통과하고, 프록시(410)를 통과하고, 예를 들면, 프록시(410)의 셀을 통해 라우터(R4)(411)에 진입하고, 그 다음, 소정의 위치(C)의 백본 네트워크 익스포트, 예를 들면, 라우터(R5)(412)를 통과하고, 소정의 위치(D)의 백본 네트워크 익스포트, 예를 들면, 라우터(R6)(413)를 통과하고, 최종적으로 서버(414)에 도달한다. 서버는 SYN 패킷을 수신한다. 다시 말하면, 서버는, 제2 IP 어드레스(프록시 IP 어드레스)를 유저 IP 어드레스로 사용하며 서버와의 TCP 연결 확립을 시도하는 제1 단말로부터 SYN 패킷을 수신한다. 서버는 제1 단말로 SYN-ACK 패킷을 전송하고, SYN-ACK 패킷을 제1 단말로 전송하는 제1 시간(시간1')을 기록한다. 그 후, 서버는 제1 단말로부터 ACK 패킷을 수신한다. 서버는 제1 단말로부터 ACK 패킷을 수신하는 제2 시점(시간2')을 기록한다. 따라서, 제1 네트워크 지연이 $T1' = \text{시간2}' - \text{시간1}'$ 이라는 결정이 이루어진다. 도 4b로부터 알 수 있는 바와 같이, 프록시의 사용으로 인해, 네트워크 지연($T1'$)은, 서버와 라우터(R6) 사이의 지연, 라우터(R6과 R5) 사이의 지연, 라우터(R5와 R4) 사이의 지연, 라우터(R4)와 프록시 사이의 지연, 프록시와 라우터(R3) 사이의 지연, 라우터(R3와 R2) 사이의 지연, 라우터(R2와 R1) 사이의 지연, 및 라우터(R1)와 제1 단말 사이의 지연을 포함한다.
- [0046] 또한, 서버는, 예를 들면, 각각 1 내지 255인 수명 시간(tt1) 및 목표 IP 어드레스를 제2 IP 어드레스로서 갖는 일련의 255개의 검출 패킷을 구축하여 전송할 수도 있고, 그 결과 서버는 일련의 검출 패킷에서의 각각의 검출

패킷의 전송 시간을 기록할 수도 있다. 위에서 설명된 바와 같이, 서버는 또한, 제2 IP 어드레스(제2 단말 대신 프록시 서버의 IP 어드레스)의 이전 홉 라우터로부터 전송되는 ICMP 에러 패킷을 수신하는 제4 시점(시간4')을 기록할 수도 있다. 또한, ICMP 에러 패킷에 기초하여, 대응하는 검출 패킷이 발견될 수도 있고, 따라서 대응하는 검출 패킷의 전송 시간을 알 수 있다. 다시 말하면, 일련의 검출 패킷에서 ICMP 에러 패킷에 대응하는 검출 패킷의 전송 시간은, 예를 들면, 제3 시점(시간3')으로서 정의된다. 이와 같이, 제2 네트워크 지연이 T2=시간 4'-시간3'인 것으로 결정된다. 도 4b로부터 알 수 있는 바와 같이, 프록시의 사용으로 인해, 제2 IP 어드레스(프록시 IP 어드레스)의 이전 홉 라우터는 더 이상 라우터(R1)가 아니고 대신 라우터(R4)로 변경된다. 따라서, 네트워크 지연(T2')은, 서버와 라우터(R6) 사이의 지연, 라우터(R6과 R5) 사이의 지연, 및 라우터(R5와 R4) 사이의 지연을 포함한다. 다시 말하면, T1'과 T2' 사이의 차이는, 라우터(R4)와 프록시 사이의 지연, 프록시와 라우터(R3) 사이의 지연, 라우터(R3와 R2) 사이의 지연, 라우터(R2와 R1) 사이의 지연, 및 라우터(R1)와 제1 단말 사이의 지연을 포함하고, 차이는 크다.

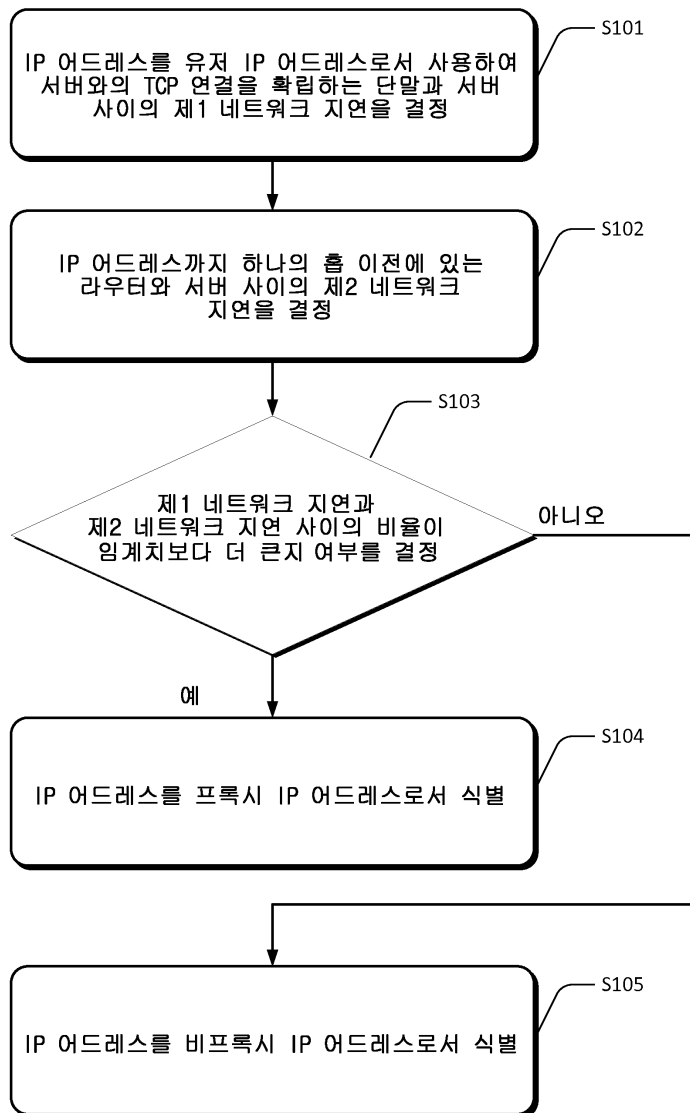
- [0047] 도 4b로부터 알 수 있는 바와 같이, 제2 IP 어드레스는 제1 단말의 진짜 어드레스가 아니며, 제1 네트워크 지연(T1')은 T2'보다 훨씬 더 크다. 따라서, T1'과 T2' 사이의 비율은 임계치보다 더 크다. 이와 같이, 제2 IP 어드레스는 프록시 IP 어드레스이며 제1 단말의 IP 어드레스가 아니라는 결정이 이루어질 수도 있다. 본 개시의 기술적 솔루션을 사용하여, 식별 결과가 실제 결과에 일치한다는 것을 알 수 있다.
- [0048] 본 개시의 실시형태에 따른 프록시 IP 어드레스를 식별하는 방법은, 상기의 도 1 내지 도 4b를 통해 설명되었다.
- [0049] 본 개시는 또한, 프록시 IP 어드레스를 식별하는 장치를 제공한다.
- [0050] 도 5는, 본 개시의 한 실시형태에 따른, 프록시 IP 어드레스를 식별하는 장치(500)의 구조도를 개략적으로 도시한다. 본 개시의 한 실시형태에 따르면, 장치(500)는: 제1 결정 모듈(501), 제2 결정 모듈(502), 판정 모듈(503) 및 식별 모듈(504)을 포함할 수도 있다.
- [0051] 본 개시의 실시형태에 따르면, 제1 결정 모듈(501)은, IP 어드레스를 유저 IP 어드레스로서 사용하여 서버와의 TCP 연결을 확립하는 단말과 서버 사이의 제1 네트워크 지연을 결정하도록 구성될 수도 있다.
- [0052] 제2 결정 모듈(502)은, IP 어드레스의 이전 홉 라우터와 서버 사이의 제2 네트워크 지연을 결정하도록 구성될 수도 있다.
- [0053] 판정 모듈(503)은, 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치보다 더 큰지 여부를 결정하도록 구성될 수도 있다.
- [0054] 결정 모듈(504)은, 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치보다 더 큰 경우 IP 어드레스가 프록시 IP 어드레스인다는 것을 식별하도록 구성될 수도 있다.
- [0055] 결정 모듈(504)은, 제1 네트워크 지연과 제2 네트워크 지연 사이의 비율이 임계치 이하인 경우 IP 어드레스가 비프록시 IP 어드레스인다는 것을 식별하도록 구성될 수도 있다.
- [0056] 본 개시의 실시형태에 따르면, 제1 결정 모듈(501)은 또한, SYN-ACK 패킷을 단말로 전송하는 시간과 단말로부터 ACK 패킷을 수신하는 시간 사이의 시간차를 제1 네트워크 지연으로서 결정하도록 구성될 수도 있다.
- [0057] 한 실시형태에서, 제1 결정 모듈(501)은 또한: SYN-ACK 패킷이 단말로 전송되는 때의 제1 시점을 기록하도록 구성되는 제1 기록 서브 모듈; ACK 패킷이 단말로부터 수신되는 제2 시점을 기록하도록 구성되는 제2 기록 서브 모듈; 및 제2 시점과 제1 시점 사이의 시간차를 제1 네트워크 지연으로서 결정하도록 구성되는 제1 결정 서브 모듈을 포함할 수도 있다.
- [0058] 본 개시의 실시형태에 따르면, 제2 결정 모듈(502)은 또한: IP 어드레스의 이전 홉 라우터로부터 ICMP 에러 패킷을 수신하는 시간과 일련의 검출 패킷에서 ICMP 에러 패킷에 대응하는 검출 패킷을 전송하는 시간 사이의 시간차를, 서버와 IP 어드레스의 이전 홉 라우터 사이의 제2 네트워크 지연으로서 결정하도록 구성되고, 일련의 검출 패킷은 증분적 수명 시간을 가지며, 그 목표 어드레스는 유저 IP 어드레스이다.
- [0059] 한 실시형태에서, 제2 결정 모듈은 또한: 일련의 검출 패킷에서의 각각의 검출 패킷의 전송 시간을 기록하도록 구성되는 제3 기록 서브 모듈; IP 어드레스의 이전 홉 라우터로부터 ICMP 에러 패킷이 수신되는 제4 시점을 기록하도록 구성되는 제4 기록 서브 모듈; 일련의 검출 패킷에서 ICMP 에러 패킷에 대응하는 검출 패킷의 전송 시간을 제3 시점으로서 정의하도록 구성되는 제1 정의 서브 모듈; 및 제4 시점과 제3 시점 사이의 시간차를 제2

네트워크 지연으로서 결정하도록 구성되는 제2 결정 서브 모듈을 포함할 수도 있다.

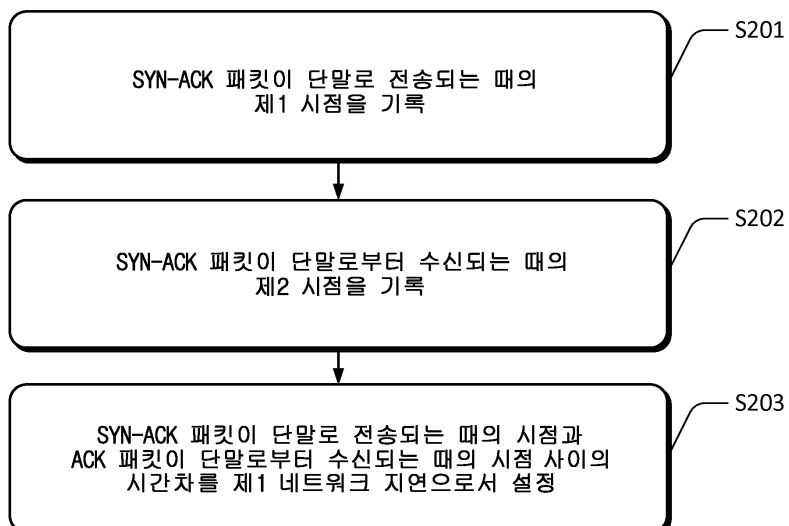
- [0060] 본 실시형태의 장치에 의해 구현되는 기능은, 도 1 내지 도 4b에서 도시되는 바와 같은 방법에 대응한다. 따라서, 본 실시형태에서 상세히 설명되지 않는 부분은, 상기 실시형태에서의 관련 설명을 참조할 수도 있으며, 본원에서는 중복적으로 설명되지 않는다.
- [0061] 통상적인 구성에서, 컴퓨팅 디바이스는 하나 이상의 프로세서(CPU), 입/출력 인터페이스, 네트워크 인터페이스, 및 메모리를 포함한다.
- [0062] 예를 들면, 도 6은 예시적인 장치(600), 예컨대 상기에서 설명된 바와 같은 장치를 더 상세히 도시한다. 한 실시형태에서, 장치(600)는, 하나 이상의 프로세서(601), 네트워크 인터페이스(602), 메모리(603), 및 입/출력 인터페이스(604)를 포함할 수도 있지만, 이들로 제한되지는 않는다.
- [0063] 메모리(603)는, 휘발성 메모리, 랜덤 액세스 메모리(random access memory; RAM) 및/또는 불휘발성 메모리, 예를 들면, 리드 온리 메모리(read-only memory; ROM) 또는 플래시 RAM과 같은 컴퓨터 판독가능 매체의 형태를 포함할 수도 있다. 메모리(603)는 컴퓨터 판독가능 매체의 한 예이다.
- [0064] 컴퓨터 판독가능 매체는, 휘발성 또는 불휘발성 타입, 착탈식 또는 비착탈식 매체를 포함할 수도 있는데, 이들은 임의의 방법 또는 기술을 사용하여 정보의 저장을 달성할 수도 있다. 정보는 컴퓨터 판독가능 커맨드, 데이터 구조, 프로그램 모듈 또는 다른 데이터를 포함할 수도 있다. 컴퓨터 저장 매체의 예는, 컴퓨팅 디바이스에 의해 액세스될 수도 있는 정보를 저장하기 위해 사용될 수도 있는, 상 변화 메모리(phase-change memory; PRAM), 스테틱 랜덤 액세스 메모리(static random access memory; SRAM), 다이내믹 랜덤 액세스 메모리(dynamic random access memory; DRAM), 다른 타입의 랜덤 액세스 메모리(RAM), 리드 온리 메모리(ROM), 전기적으로 소거가능한 프로그래머블 리드 온리 메모리(electronically erasable programmable read-only memory; EEPROM), 퀵 플래시 메모리 또는 다른 내장형 저장 기술, 콤팩트 디스크 리드 온리 메모리(compact disk read-only memory; CD-ROM), 디지털 다기능 디스크(digital versatile disc; DVD) 또는 다른 광학 스토리지, 자기 카세트 테이프, 자기 디스크 스토리지 또는 다른 자기 스토리지 디바이스, 또는 임의의 다른 비전송 매체를 포함할 수도 있지만, 이들로 제한되지는 않는다. 본원에서 정의되는 바와 같이, 컴퓨터 판독가능 매체는 일시적 매체, 예컨대 변조된 데이터 신호 및 반송파를 포함하지 않는다.
- [0065] 메모리(603)는 프로그램 모듈(605) 및 프로그램 데이터(606)를 포함할 수도 있다. 일 실시형태에서, 프로그램 모듈(605)은 제1 결정 모듈(607), 제2 결정 모듈(608), 판정 모듈(609) 및 식별 모듈(610)을 포함할 수도 있다. 몇몇 실시형태에서, 제1 결정 모듈(607)은 제1 기록 서브 모듈(611), 제2 기록 서브 모듈(612) 및/또는 제1 결정 서브 모듈(613)을 포함할 수도 있다. 추가적으로, 일 실시형태에서, 제2 결정 모듈(608)은 제3 기록 서브 모듈(614), 제4 기록 서브 모듈(615), 제1 정의 서브 모듈(616) 및/또는 제2 결정 서브 모듈(617)을 포함할 수도 있다. 이들 모듈 및 서브 모듈의 상세는 상기 설명에서 발견될 수도 있으며 따라서 본원에서는 중복적으로 설명되지 않는다.
- [0066] 용어 "포함한다(comprise)", "포함한다(include)" 또는 이들의 임의의 다른 변형 어구는 비배타적인 포함(non-exclusive inclusion)을 포괄하도록 의도된다는 것을 유의해야 한다. 일련의 엘리먼트를 포함하는 프로세스, 방법, 제품 또는 장치는, 이들 엘리먼트를 포함할 뿐만 아니라, 명시적으로 열거되지 않은 다른 엘리먼트를 또한 포함하거나, 또는 이러한 프로세스, 방법, 제품 또는 장치에서 이미 존재하는 엘리먼트를 더 포함한다. 추가 제한이 없는 조건에서, 어구 "~하는 하나를 포함하는"에 의해 정의되는 엘리먼트는, 프로세스, 방법, 제품 또는 장치에서 존재하는 임의의 다른 유사한 엘리먼트를 배제하지는 않는다.
- [0067] 당업자는, 본 개시의 실시형태가 방법, 시스템 또는 컴퓨터 프로그램의 제품으로서 제공될 수도 있다는 것을 이해해야 한다. 따라서, 본 개시는 하드웨어만의 실시형태로서, 소프트웨어만의 실시형태로서 또는 하드웨어와 소프트웨어의 조합의 실시형태로서 구현될 수 있다. 또한, 본 개시는, 컴퓨터 실행가능 명령어를 저장하는 하나 이상의 컴퓨터 판독가능 저장 매체(이것은 자기 디스크, CD-ROM 또는 광학 디스크 등등을 포함하지만 이들로 제한되지는 않음)에 저장될 수 있는 컴퓨터 프로그램의 제품으로서 구현될 수 있다.
- [0068] 상기 설명은, 본 개시의 범위를 제한하도록 의도되지 않은 본 개시의 실시형태를 설명할 뿐이다. 당업자에 의해, 다양한 수정예 및 변경예가 본 개시에 대해 이루어질 수도 있다. 본 개시의 취지와 원칙의 범위 내에 있는 임의의 수정예, 대체예 및 개선예는 본 개시의 청구범위의 범위 내에 있을 것이다.

도면

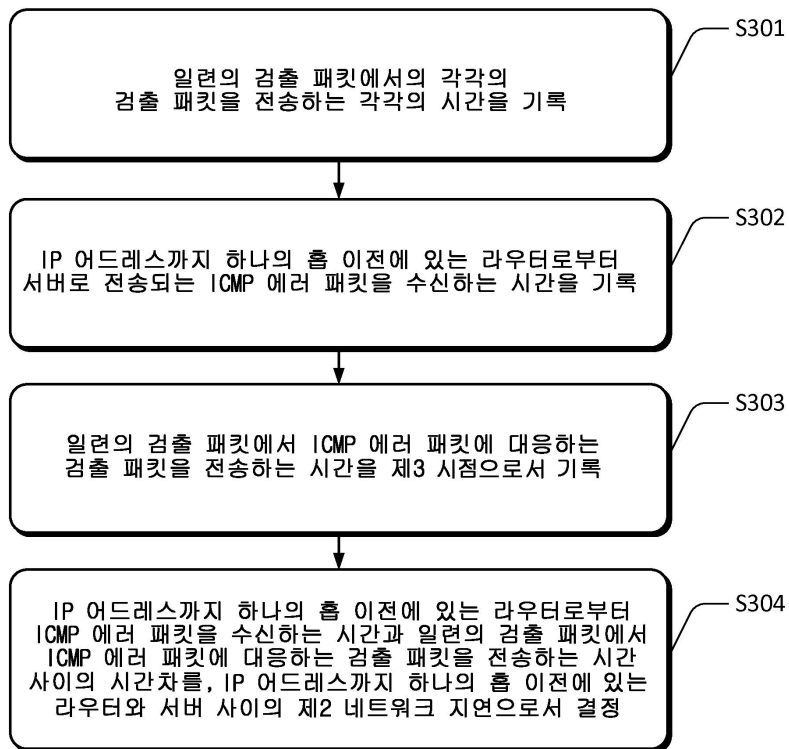
도면1



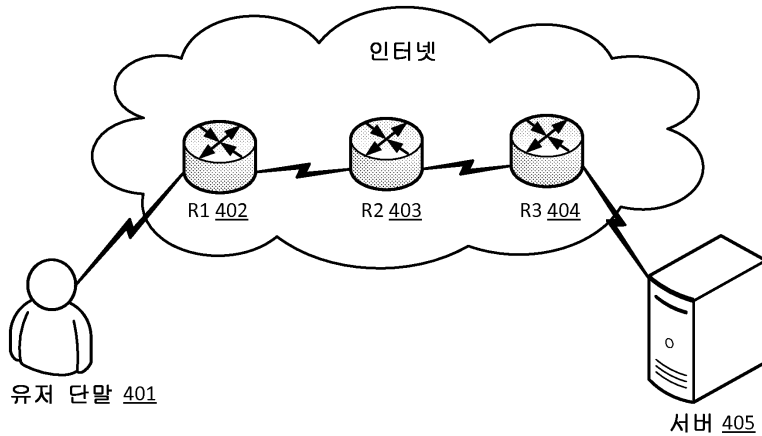
도면2



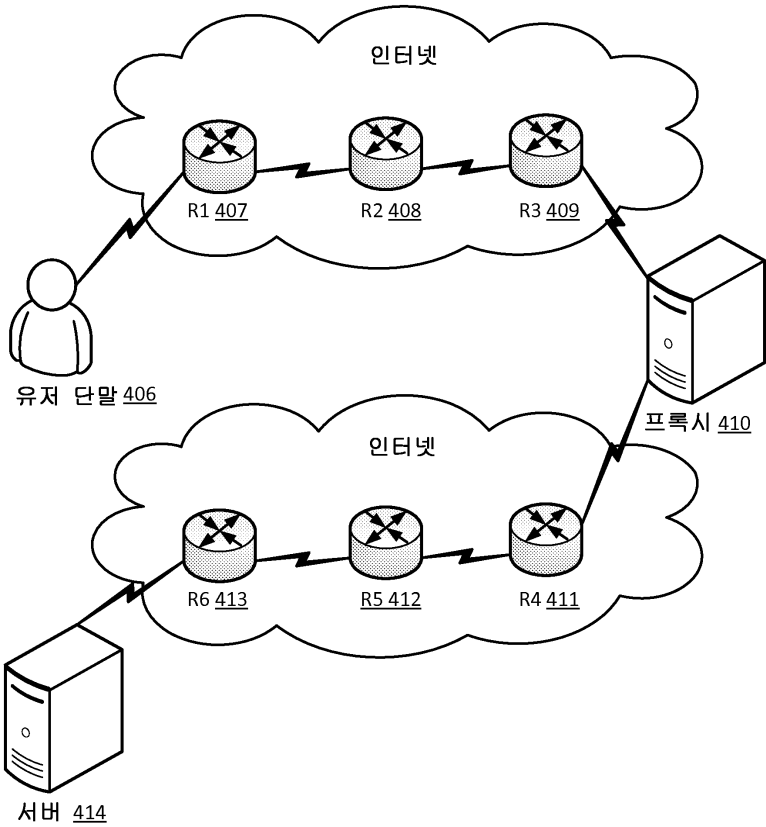
도면3



도면4a

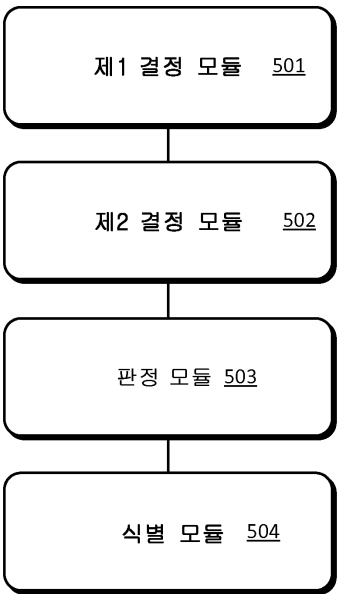


도면4b



도면5

500



도면6

