(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2015 년 7 월 9 일 (09.07.2015)

WIPO | PCT

(10) 국제공개번호
WO 2015/102446 A1

(51) 국제특허분류:
H04L 12/26 (2006.01)

(21) 국제출원번호: PCT/KR2015/000060

(22) 국제출원일: 2015 년 1 월 5 일 (05.01.2015)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2014-0001281 2014 년 1 월 6 일 (06.01.2014) KR

(71) 출원인: **고려대학교 산학협력단 (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION)** [KR/KR]; 136-701 서울시 성북구 안암로 145, Seoul (KR).

(72) 발명자: **김덕윤 (KIM, Duk Yun)**; 136-701 서울시 성북구 안암로 145, 고려대학교, Seoul (KR). **차성덕 (CHA, Sungdeok)**; 136-755 서울시 성북구 동소문로 34 길 24, 106-710, Seoul (KR). **권신일 (KWON, Shinil)**; 136-701 서울시 성북구 안암로 145, 고려대학교, Seoul (KR). **정세훈 (JEONG, Sehun)**; 136-701 서울시 성북구 안암로 145, 고려대학교, Seoul (KR).

(74) 대리인: **특허법인 충현 (CHUNG HYUN PATENT & LAW FIRM)**; 137-130 서울시 서초구 바우뫼로 225 한마음빌딩 4 층, Seoul (KR).

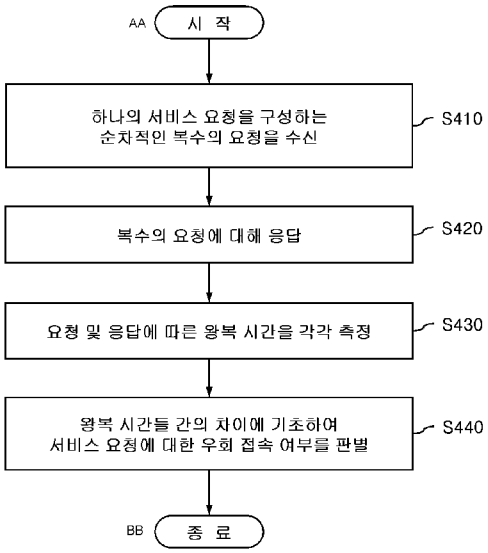
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[다음 쪽 계속]

(54) **Title**: METHOD FOR DETECTING BYPASS CONNECTION VIA ANONYMOUS NETWORK USING CHANGES IN ROUND TRIP TIMES

(54) **발명의 명칭** : 왕복 시간 변화를 이용하여 익명 네트워크를 통한 우회 접속을 탐지하는 방법



S410 ... Receive plurality of sequential requests constituting one service request
S420 ... Respond to plurality of requests
S430 ... Measure round trip times according to requests and responses, respectively
S440 ... Distinguish whether there is bypass connection to service request on basis of difference between round trip times
AA ... Start
BB ... End

(57) **Abstract**: Disclosed is a method for detecting a bypass connection via an anonymous network using changes in round trip times. In the method for detecting a bypass connection, a server receives a plurality of sequential requests constituting one service request; responds to the received plurality of requests; measures round trip times (RTTs) according to the requests and responses, respectively; and distinguishes whether there is a bypass connection to the service request on the basis of a difference between the measured round trip times.

(57) **요약서**: 왕복 시간 변화를 이용하여 익명 네트워크를 통한 우회 접속을 탐지하는 방법이 개시된다. 우회 접속을 탐지하는 방법은, 서버가 하나의 서비스 요청을 구성하는 순차적인 복수의 요청을 수신하고, 수신된 복수의 요청에 대해 응답하고, 요청 및 응답에 따른 왕복 시간(round trip time, RTT)들을 각각 측정하며, 측정된 왕복 시간들 간의 차이에 기초하여 서비스 요청에 대한 우회 접속 여부를 판별한다.

WO 2015/102446 A1

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

명세서

발명의 명칭: 왕복 시간 변화를 이용하여 익명 네트워크를 통한 우회 접속을 탐지하는 방법

기술분야

[1] 본 발명은 네트워크로부터의 우회 접속을 탐지하는 기술에 관한 것으로, 특히 네트워크 상에서 익명성을 보장하는 익명 네트워크를 활용하여 자신의 위치나 통신 경로를 숨긴 채 서버에 접근하는 악의적인 사용자의 우회 접속을 탐지하는 방법 및 그 방법을 기록한 기록매체에 관한 것이다.

배경기술

[2] 오늘날 대부분의 웹사이트들은 인터넷 통신 과정에서 발생하는 모든 패킷(packet)이나 트래픽(traffic) 등을 접속자 자신도 모르는 사이에 관리, 기록(log)하고 있다. 포털 사이트들의 검색창에 입력된 검색어들은 실시간 검색 순위 산출에 활용되고, 접속한 IP 주소를 통해 사용자의 위치 및 검색 패턴뿐만 아니라, 사용자의 성향 등도 마케팅 정보로 이용되고 있는 상황이다.

[3] 만약 악의적인 사용자가 자신의 IP 주소를 감추고자 하는 의도로서 패킷에서 소스(source) IP를 변경한다면 라우터에서 패킷이 드롭(drop)되거나, 또는 TCP의 경우 연결 자체가 성립될 수 없으므로 실제적으로 IP 자체를 변경하여 통신하는 것은 매우 어렵다. 이러한 악의적인 사용자들이 사이버 공격을 수행하기 위해, 과거에는 VPN(virtual private network)이나 프록시(proxy) 서버 등을 이용해 자신의 IP를 숨기는 기술이 많이 활용되었다. 그러나, 이러한 VPN이나 프록시 서버를 활용하더라도 중계 서버의 제공자를 신뢰할 수 없고 중계한 패킷의 정보가 수사 기관 등에 제공될 경우 실제 접속한 IP의 추적이 가능해질 수 있었다. 이를 극복하기 위해 등장한 개념이 TOR(the onion router), Zenmate와 같은 익명 네트워크이다. 이 외에도 알려지지 않은 많은 익명 네트워크가 있을 수 있다.

[4] 대표적인 익명 네트워크인 TOR는 사용자가 TOR 전용 브라우져를 이용하여 손쉽게 익명으로 인터넷을 이용할 수 있는 환경을 제공한다. TOR 브라우져는 전 세계의 수 천대 서버 중 임의로 선택된 3대를 경유하여 웹 서버에 접속한다. 3대의 서버 중 최종 서버인 엑시트 노드(Exit-node)가 사용자 컴퓨터를 대신하여 웹 서버와 접속한다. 그래서 웹 서버는 사용자 컴퓨터의 IP가 아닌 엑시트 노드의 IP만을 알게 된다. 따라서, 악의적인 사용자가 TOR를 이용하게 될 경우, 실제 패킷을 발송한 최초의 발신자를 확인할 수 없게 된다. 이러한 점을 악용하여 사이버 공격에 이용하는 사례가 점차 증가하고 있는 추세이다.

[5] 따라서, 익명 네트워크를 통한 우회 접속이나 악의적인 접근을 탐지하고, 이를 효과적으로 차단할 수 있는 기술적 수단이 요구되고 있다. "익명네트워크를 이용한 사이버공격에 대한 대응방안 연구, 이정현, 안관준, 박원형, 임종인,

한국융합보안학회, 2011년"에는 이러한 익명 네트워크 기술을 분석하고 이에 대한 대응 방안을 소개하고 있으나, 여전히 우회 접속을 근본적으로 식별할 수 있는 기술적 수단에 대해서는 침묵하고 있다.

발명의 상세한 설명

기술적 과제

[6] 본 발명이 해결하고자 하는 기술적 과제는, 종래의 익명 네트워크를 통한 우회 접속 방법들을 탐지함에 있어서, 단지 HTTP 헤더(header)만을 확인하거나, 익명 네트워크의 엑시트 노드의 IP 블럭을 미리 확보한 후 해당 IP로부터의 접속을 악의적인 접속으로 간주하는 등의 초보적인 수준의 탐지 방법에 머물렀기 때문에, 악의적인 사용자가 헤더를 미공개/조작하거나 교체된 IP를 사용하여 접속을 시도하는 경우 이러한 접근을 정확하게 탐지하지 못하는 한계를 극복하고, 나아가 특정 객체를 웹페이지 내에 삽입함으로써 사용자의 접속시 클라이언트 정보를 획득하는 방법을 활용할 경우, 개인정보의 유출/침해 가능성이 발생할 수 있다는 문제점을 해소하고자 한다.

과제 해결 수단

[7] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 익명 네트워크를 통한 우회 접속을 탐지하는 방법은, 서버가 하나의 서비스 요청을 구성하는 순차적인 복수의 요청을 수신하는 단계; 상기 서버가 수신된 상기 복수의 요청에 대해 응답하는 단계; 상기 서버가 상기 요청 및 응답에 따른 왕복 시간(round trip time, RTT)들을 각각 측정하는 단계; 및 상기 서버가 측정된 상기 왕복 시간들 간의 차이에 기초하여 상기 서비스 요청에 대한 우회 접속 여부를 판별하는 단계;를 포함한다.

[8] 일 실시예에 따른 상기 익명 네트워크를 통한 우회 접속을 탐지하는 방법에서, 상기 우회 접속 여부를 판별하는 단계는, 익명 네트워크를 통한 경유로 인하여 상기 왕복 시간들 간에 불규칙성이 발생하였는지 여부를 검사함으로써 수행될 수 있다.

[9] 일 실시예에 따른 상기 익명 네트워크를 통한 우회 접속을 탐지하는 방법에서, 상기 우회 접속 여부를 판별하는 단계는, 복수의 왕복 시간 중 제 1 요청에 따른 제 1 왕복 시간과 상기 제 1 요청에 대한 응답 이후 상기 서버에 수신되는 제 2 요청에 따른 제 2 왕복 시간 간의 차이값을 산출하는 단계; 및 산출된 상기 차이값이 미리 설정된 임계값 이상인 경우, 상기 서비스 요청을 익명 네트워크를 통한 우회 접속으로 추정하는 단계;를 포함한다.

[10] 일 실시예에 따른 상기 익명 네트워크를 통한 우회 접속을 탐지하는 방법에서, 상기 왕복 시간은 클라이언트가 서버에 요청을 전송한 후 이에 대한 응답을 수신하기까지의 소요 시간을 측정함으로써 획득될 수 있다. 또한, 일 실시예에 따른 상기 익명 네트워크를 통한 우회 접속을 탐지하는 방법에서, 상기 왕복 시간은 서버가 요청에 응답한 후 응답에 따른 후속 요청을 수신하기까지의 소요

시간을 측정함으로써 획득될 수 있다.

[11] 일 실시예에 따른 상기 익명 네트워크를 통한 우회 접속을 탐지하는 방법은, 판별 결과, 상기 서비스 요청이 우회 접속으로 추정된 경우 상기 접속을 차단하는 단계;를 더 포함할 수 있다.

[12] 상기 기술적 과제를 해결하기 위하여, 본 발명의 다른 실시예에 따른 익명 네트워크를 통한 우회 접속을 탐지하는 방법은, 서버가 HTTP 요청을 수신하는 단계; 상기 서버가 수신된 상기 HTTP 요청에 대해 응답하여 페이지 파일(page file)을 전송하는 단계; 상기 서버가 상기 페이지 파일 응답에 따른 제 1 왕복 시간을 측정하는 단계; 상기 서버가 상기 페이지 파일 응답에 따른 리소스 파일(resource file) 요청을 수신하고 대응하는 리소스 파일을 전송하는 단계; 상기 서버가 상기 리소스 파일 응답에 따른 제 2 왕복 시간을 측정하는 단계; 및 상기 서버가 측정된 상기 제 1 왕복 시간과 상기 제 2 왕복 시간 간의 차이에 기초하여 왕복 시간들 간에 불규칙성이 발생하였는지 여부를 검사함으로써 상기 서비스 요청에 대한 우회 접속 여부를 판별하는 단계;를 포함한다.

[13] 다른 실시예에 따른 상기 익명 네트워크를 통한 우회 접속을 탐지하는 방법에서, 상기 우회 접속 여부를 판별하는 단계는, 상기 제 1 왕복 시간과 상기 제 2 왕복 시간 간의 차이값을 산출하는 단계; 산출된 상기 차이값이 미리 설정된 임계값 이상인 경우, 상기 서비스 요청을 익명 네트워크를 통한 우회 접속으로 추정하는 단계; 및 우회 접속으로 추정된 경우, 산출된 상기 차이값의 통계적 분포를 이용하여 상기 익명 네트워크의 종류를 식별하는 단계;를 포함한다.

[14] 다른 실시예에 따른 상기 익명 네트워크를 통한 우회 접속을 탐지하는 방법에서, 상기 제 1 왕복 시간은 익명 네트워크 경유로 인한 시간 지연을 포함하며, 상기 제 2 왕복 시간에 비해 상대적으로 더 큰 값을 갖는다.

[15] 다른 실시예에 따른 상기 익명 네트워크를 통한 우회 접속을 탐지하는 방법에서, 상기 제 1 왕복 시간은 상기 서버와 클라이언트 간의 통신 경로를 이용하여 상기 서버가 상기 클라이언트에 상기 페이지 파일에 대한 응답을 전송한 이후 상기 클라이언트로부터 최초의 리소스 파일에 대한 요청을 수신하는 시점까지의 소요 시간이고, 상기 제 2 왕복 시간은 상기 서버와 상기 익명 네트워크 내에 위치한 우회 클라이언트 간의 통신 경로를 이용하여 상기 서버가 상기 최초의 리소스 파일에 대한 응답을 전송한 이후 상기 클라이언트로부터 다음 리소스 파일에 대한 요청을 수신하는 시점까지의 소요 시간일 수 있다.

[16] 다른 실시예에 따른 상기 익명 네트워크를 통한 우회 접속을 탐지하는 방법에서, 상기 제 1 왕복 시간 및 상기 제 2 왕복 시간 측정을 위한 대상 신호가 복수 개인 경우, 복수 개의 대상 신호 중 도착 시간이 최소인 값을 측정하여 각각의 왕복 시간을 산출할 수 있다.

[17] 한편, 이하에서는 상기 기재된 익명 네트워크를 통한 우회 접속을 탐지하는 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는

기록매체를 제공한다.

발명의 효과

[18] 본 발명의 실시예들은 서버에서 자신에게 접속하는 트래픽 분석을 통해 파일의 속성에 따라 왕복 시간의 차이가 존재하는지, 그 불규칙성을 검사함으로써 익명 네트워크를 통한 우회 접속을 정확하게 탐지할 수 있을 뿐만 아니라, 네트워크 및 서버에 추가적인 부담이 전혀 없으면서도 프라이버시 침해에 관한 논란 또한 전혀 발생하지 않는다는 장점을 갖는다.

도면의 간단한 설명

[19] 도 1은 익명 네트워크를 통한 침입과 그 구조의 개요를 설명하기 위한 도면이다.

[20] 도 2a 및 도 2b는 HTTP 서비스를 일례로 클라이언트 및 서버 간의 통신 방식을 설명하기 위한 도면이다.

[21] 도 3a 및 도 3b는 클라이언트 및 서버 간 직접 통신과 익명 네트워크를 경유하는 통신 방식의 왕복 시간 차이를 설명하기 위한 도면이다.

[22] 도 4는 본 발명의 일 실시예에 따른 익명 네트워크를 통한 우회 접속을 탐지하는 방법을 도시한 흐름도이다.

[23] 도 5a 및 도 5b는 일 실시예에 따른 도 4의 우회 접속 탐지 방법에서 각각 클라이언트와 서버 측에서 HTTP 왕복 시간을 측정하는 방법을 설명하기 위한 도면이다.

[24] 도 6a 및 도 6b는 일 실시예에 따른 도 4의 우회 접속 탐지 방법을 이용하여 왕복 시간의 측정이 이루어지는 과정을 직접 통신 방식과 익명 네트워크를 경유한 통신 방식을 비교하여 설명하기 위한 도면이다.

[25] 도 7은 본 발명의 HTTP 서비스 요청에 따른 익명 네트워크를 통한 우회 접속을 탐지하는 방법을 도시한 흐름도이다.

[26] 도 8 및 도 9는 다양한 네트워크 환경을 가정하여 왕복 시간을 측정한 실험 결과를 예시한 도면이다.

[27] <부호의 설명>

[28] 10 : 클라이언트

[29] 20 : 서버

[30] 30 : 익명 네트워크

[31] 31 : 엔트리 노드(entry node)

[32] 32 : 엑시트 노드(exit node)

발명의 실시를 위한 최선의 형태

[33] 본 발명의 일 실시예에 따른 익명 네트워크를 통한 우회 접속을 탐지하는 방법은, 서버가 하나의 서비스 요청을 구성하는 순차적인 복수의 요청을 수신하는 단계; 상기 서버가 수신된 상기 복수의 요청에 대해 응답하는 단계; 상기 서버가 상기 요청 및 응답에 따른 왕복 시간(round trip time, RTT)들을 각각

측정하는 단계; 및 상기 서버가 측정된 상기 왕복 시간들 간의 차이에 기초하여 상기 서비스 요청에 대한 우회 접속 여부를 판별하는 단계;를 포함한다.

발명의 실시를 위한 형태

[34] 본 발명의 실시예들을 설명하기에 앞서, 익명 네트워크 환경에서 발생하는 우회 접속의 특징과 문제점들을 검토한 후, 이들 문제점을 해결하기 위해 본 발명의 실시예들이 채택하고 있는 기술적 수단을 개괄적으로 소개하도록 한다.

[35] 도 1은 익명 네트워크를 통한 침입과 그 구조의 개요를 설명하기 위한 도면으로서, 익명 네트워크의 일례로 TOR를 가정하여 설명하도록 한다.

[36] 미 해군이 TOR를 구축한 목적은 인터넷 사용자가 정부나 특정 조직의 규제를 받지 않고 자유롭게 인터넷을 이용할 수 있도록 환경을 조성한 것이었다. 이를 위해 TOR는 웹서버(20)와 클라이언트(10) 사이에 3개의 중간 노드(entry, middle, exit)를 두어 클라이언트(10)가 웹서버(20)에 접속하는 각종 행위가 노출되지 않도록 구성하였다. 클라이언트(10)는 엔트리 노드(entry-node)(31)와 통신하고, 웹서버(20)는 엑시트 노드(exit-node)(32)와 통신하므로 클라이언트 IP가 노출되지 않는다. 또한 클라이언트(10)에서 엑시트 노드(32) 구간의 통신을 암호화하여 클라이언트(10)와 웹서버(32) 간 교환되는 정보의 노출을 방지하였다. 또한 사용이 편리하여 세계적으로 널리 이용되고 있다.

[37] 도 1을 참조하면, 서버(20)과 클라이언트(10)가 직접 통신하는 경우와 익명 네트워크(30)를 경유하여 통신하는 경우에 있어서, 서버(20)를 기준으로 서버 자신이 통신하는 대상이 상이함을 알 수 있다. 서버(20)가 직접 클라이언트(10)와 통신하는 경우, 서버(10)에서 전송되는 패킷은 직접 클라이언트(10)에 도달하고, 또한 클라이언트(10)로부터 전송되는 패킷을 서버(20)가 직접 수신하므로, 서버(20)는 클라이언트(10) IP를 알 수 있다. 이에 반해 익명 네트워크(30)를 경유하여 통신하는 경우, 서버(20)에서 전송되는 패킷은 익명 네트워크(30)를 구성하는 엑시트 노드(32)에 수신되고, 엑시트 노드(32)로부터 응답 메시지를 받게 되므로, 서버(20)는 진짜 클라이언트(10)의 IP를 알 수 없다. 서버(20)에서 알 수 있는 IP는 일종의 가짜 클라이언트(즉, 엑시트 노드(32)를 의미한다.)의 주소뿐이다.

[38] 상기된 바와 같이, 만약 클라이언트(10)가 익명 네트워크(30)를 통해 서버(20)에 우회 접속을 시도할 경우, 이러한 접속이 우회 접속인지 여부를 알 수 없는 문제점에 노출되게 된다.

[39] 한편, 도 2a 및 도 2b는 HTTP 서비스를 일례로 클라이언트 및 서버 간의 통신 방식을 설명하기 위한 도면으로서, 여기서는 HTTP 서비스의 통신 특징만을 간략히 소개하고, 이후 익명 네트워크에서 나타나는 문제점을 재차 설명하도록 한다.

[40] 도 2a를 참조하면, 하나의 인터넷 홈페이지는 1개의 페이지 파일(page file)과 이에 연결된 여러 개의 리소스 파일(resource file)로 구성된다. 예를 들어 n개(n은

자연수)의 꽃 그림이 포함된 홈페이지는 n개의 그림 파일과 이들을 HTML 형태로 묶어주는 1개의 페이지 파일로 구성된다.

[41] 이제, 도 2b를 참조하여 인터넷 홈페이지 접속 과정을 설명하면 다음과 같다. 정상적인 접속인 경우에 홈페이지 파일을 가져오는 과정은 크게 2 단계로 이루어진다.

[42] 1 단계에서, 클라이언트(10)가 웹서버(20)에 접속해서 페이지 파일을 가져온다. 즉, 클라이언트(10)의 제 1 요청이 서버(20)에 전달되고, 이에 대해 서버(20)로부터 제 1 응답(페이지 파일)을 수신한다. 1 단계 과정의 종료 후에 클라이언트(10)는 페이지 파일을 파싱(parsing)하여 웹페이지 구성에 필요한 리소스 파일에 대한 목록을 작성한다. 이 때, 캐쉬에 리소스 파일이 있는 경우에는 목록에서 해당 파일을 제외할 수도 있다.

[43] 2 단계에서, 클라이언트(10)는 웹서버(20)에 접속하여 목록 내에 포함되어 있는 리소스 파일을 가져온다. 즉, 클라이언트(10)의 제 2 요청이 서버(20)에 전달되고, 이에 대해 서버(20)로부터 제 2 응답(리소스 파일)을 수신한다.

[44] 여기서 주목해야 할 점은 1 단계를 거치지 않고서는 2 단계가 시작될 수 없으며, 2 단계에서 발생하는 어떠한 접속도 1 단계 완료 이전에 발생하지 않는다는 사실이다. 이에 비해 2 단계 내에서 여러 개의 리소스 파일을 가져오는 과정은 순서에 상관없이 병렬로 진행될 수 있기 때문에 대부분의 상용 웹브라우저들은 웹서버와 다수의 접속을 동시에 연결하고 각 접속이 여러 개의 리소스 파일을 가져온다. 도 2b에서는 2 단계에서 2 개의 접속(실선과 점선)이 형성되고 각 접속이 각각 다수의 리소스 파일을 가져오고 있는 상황을 표현하였다.

[45] 상기된 인터넷 홈페이지 접속 과정을 TOR를 경유한 우회 접속 방법을 중심으로 설명하면 다음과 같다.

[46] 1 단계에서, 클라이언트(10)가 특정 홈페이지에 접속을 요청하면 익명 네트워크를 구성하는 엔트리 노드(Entry-node)가 이를 수신하여 미들 노드(Middle-node)를 거쳐 엑시트 노드(Exit-node)에 전달한다. 그런 다음, 엑시트 노드가 웹서버(20)에 접속하여 해당되는 페이지 파일을 요청한다. 웹서버(20)는 요청에 대한 응답으로써 해당 페이지 파일을 다시 엑시트 노드에 전송하고, 이는 미들 노드 및 엔트리 노드를 거쳐 최종적으로 클라이언트(10)에 전달된다. 이제, 클라이언트(10)는 페이지 파일을 읽고 자신이 보유한 캐쉬 파일과 비교하여 웹페이지 표시에 필요한 리소스 파일 목록을 작성한다.

[47] 2 단계에서, 클라이언트(10)가 필요한 리소스 파일들을 엔트리 노드에 동시에 요청하면 이러한 요청들은 미들 노드를 거쳐 엑시트 노드에 전달된다. 그러면, 엑시트 노드는 웹서버(20)에 순차적으로 리소스 파일을 요청한다. 이 과정에서 상용 브라우저와 유사하게 복수의 접속이 동시에 수행될 수 있다. 이제, 엑시트 노드가 서버(20)로부터 응답으로써 수신한 리소스 파일들은 다시 미들 노드 및 엔트리 노드를 거쳐 최종적으로 클라이언트(10)에 전달된다.

[48] 도 3a 및 도 3b는 클라이언트 및 서버 간 직접 통신과 익명 네트워크를 경유하는

통신 방식의 왕복 시간 차이를 설명하기 위한 도면이다.

[49] 도 3a를 참조하면, 클라이언트(10)와 서버(20)가 직접 통신하는 경우, 페이지 파일을 전송하는데 따른 왕복 시간(① RTT_{pi})와 이후 리소스 파일(예를 들어, 이미지 파일이 될 수 있다.)을 전송하는데 따른 왕복 시간(② RTT_{ii})은 그 통신 경로에 큰 차이가 없으며, 그로 인해 측정된 시간 역시 유사할 수 밖에 없다.

[50] 이에 반해, 익명 네트워크(30)를 경유하는 우회 접속의 경우, 전송되는 파일에 따라 왕복 시간에 다소 차이가 발생한다. TOR를 통한 홈페이지 접속을 가정하고 있는 도 3b를 참조하면, 서버(20)로부터 페이지 파일을 전송하는데 따른 왕복 시간(③ RTT_{pi})와 이후 리소스 파일(예를 들어, 이미지 파일이 될 수 있다.)을 전송하는데 따른 왕복 시간(④ RTT_{ii})은 그 통신 경로에 차이가 있으며, 그로 인해 측정된 시간 역시 상이하다. 왜냐하면, 최초에 서버(20)로부터 전송되는 페이지 파일의 경우 실제 클라이언트(10)까지 도달하여야만 해당 웹페이지에 대한 파싱과 포함되는 리소스 파일의 목록을 생성할 수 있는데 반해, 일단 파일 목록이 생성되면, 익명 네트워크(30)를 통해 서버(20)의 다수의 연결을 맺고, 이를 통해 리소스 요청 및 응답이 이루어지게 된다. 따라서, 페이지 파일의 전송에 따른 통신 경로와 리소스 파일의 전송에 따른 통신 경로는 상이하며, 이로 인한 왕복 시간 역시 차이가 발생하게 된다. 당연히 페이지 파일의 전송을 위한 왕복 시간이 리소스 파일의 전송을 위한 왕복 시간에 비해 상대적으로 더 큰 값을 갖는다.

[51] 이상과 같은 차이점에 착안하여 본 발명의 실시예들은, 익명 네트워크를 이용하여 홈페이지 서버에 접속하는 트래픽을 탐지하기 위해 전송되는 파일의 속성에 따라 왕복 시간이 상이한 특징을 활용하고자 한다. 직접 접속에서는 물론 TOR와 같은 익명 네트워크를 통한 접속에서도 페이지 파일을 가져온 후 이를 파싱하는 과정은 반드시 클라이언트(10)가 직접 수행하고 있다. 반면, 리소스 파일을 요청하는 행위에서는 차이점이 발생한다. 정상 접속(익명 네트워크를 경유하지 않는 직접 접속을 의미한다.)에서는 클라이언트(10)가 리소스 파일을 서버(20)에 직접 요청하지만 익명 네트워크(30)를 통한 우회 접속에서는 엑시트 노드가 클라이언트(10)를 대신하여 서버(20)에 리소스 파일을 요청한다. 결국 익명 네트워크(30)를 통하여 접속한 경우 클라이언트(10)가 페이지 파일을 수신한 이후 첫 번째 리소스 파일을 요청할 때까지는 상당한 시간이 소요되는 반면, 일단 리소스 파일을 수신한 다음 다른 후속 리소스 파일을 요청할 때까지의 시간은 상대적으로 단축된다. 즉, 대부분의 통신에 소요되는 왕복 시간이 서버(20)와 익명 네트워크(일종의 가짜 클라이언트가 될 것이다.)(30) 간의 통신에 해당하나, 특정 파일의 경우에는 그 전송을 위한 통신이 서버(20)와 진짜 클라이언트(10) 간에 맺어지게 되는 속성을 이용한다. 이러한 시간 차이는 정상 접속의 경우에는 발생하지 않는다.

[52] 이하에서는 도면을 참조하여 본 발명의 실시예들을 구체적으로 설명하도록 한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지

기능 또는 구성에 대한 상세한 설명은 생략한다. 또한, 도면 전체에 걸쳐 동일한 구성 요소들은 가능한 한 동일한 도면 부호로 나타내고 있음에 유의하여야 한다.

[53] 도 4는 본 발명의 일 실시예에 따른 익명 네트워크를 통한 우회 접속을 탐지하는 방법을 도시한 흐름도로서, 다음의 단계들을 포함한다. 각각의 단계들은 적어도 하나의 프로세서와 연산을 처리하기 위해 활용될 수 있는 저장 공간, 그리고 통신 수단을 구비한 물리적인 하드웨어 장치(예를 들어, 서버가 될 수 있다.)로서 구현될 수 있으며, 웹서버에서 트래픽 분석을 통해 익명 네트워크를 이용한 우회 접속을 탐지하는 탐지 소프트웨어와 더불어 활용될 수 있다.

[54] S410 단계에서, 서버는 하나의 서비스 요청을 구성하는 순차적인 복수의 요청을 수신한다. 예를 들어, 이러한 서비스 요청은 HTTP 웹서비스 요청이 될 수 있을 것이며, 하나의 HTTP 서비스 요청에는 페이지 파일 요청이나 리소스 요청과 같은 다양한 요청이 포함될 수 있다. 이러한 복수의 요청은 파일의 속성에 따라 순차적으로 이루어지는 것이 보통일 것이며, 동일한 속성의 파일의 경우에는 병렬적인 동시 접속이 이루어질 수도 있다. 예를 들어, 페이지 파일과 리소스 파일의 요청은 반드시 순차적으로 이루어질 것이며, 이에 반해 다수의 리소스 파일들은 각각 병렬적으로 요청/응답될 수 있다.

[55] S420 단계에서, 서버는 상기 S410 단계를 통해 수신된 상기 복수의 요청에 대해 응답한다. 예를 들어, 서버는 클라이언트에 페이지 파일을 응답으로서 전송할 수도 있고, 리소스 파일을 응답으로서 전송할 수도 있을 것이다.

[56] S430 단계에서, 서버는 상기 S410 단계의 요청 및 S420 단계의 응답에 따른 왕복 시간(round trip time, RTT)들을 각각 측정한다. 왕복 시간 측정에 관한 보다 구체적인 내용은 이후 도 5a 내지 도 6b를 통해 설명하도록 한다.

[57] S440 단계에서, 서버는 S430 단계를 통해 측정된 상기 왕복 시간들 간의 차이에 기초하여 상기 서비스 요청에 대한 우회 접속 여부를 판별한다. 이러한 우회 접속 여부를 판별하는 단계는, 익명 네트워크를 통한 경유로 인하여 상기 왕복 시간들 간에 불규칙성이 발생하였는지 여부를 검사함으로써 수행된다. 앞서 도 3b를 통해 설명한 바와 같이 익명 네트워크를 경유하는 경우, 전송되어야 하는 파일들 간에 통신 경로에 차이가 발생하게 되고, 이로 인해 왕복 시간에도 차이가 나타나게 된다. 따라서, 측정된 왕복 시간들이 불규칙한 것으로 검사될 경우, 해당 접속이 익명 네트워크를 통한 접속인 것으로 판별할 수 있다. 만약, 판별 결과, 상기 서비스 요청이 우회 접속으로 추정된 경우 상기 접속을 차단할 수 있을 것이다.

[58] 보다 구체적으로, S440 단계에서 우회 접속 여부를 판별하는 과정은, 복수의 왕복 시간 중 제 1 요청(예를 들어, 페이지 파일의 요청)에 따른 제 1 왕복 시간과 상기 제 1 요청에 대한 응답 이후 상기 서버에 수신되는 제 2 요청(예를 들어, 리소스 파일의 요청)에 따른 제 2 왕복 시간 간의 차이값을 산출하고, 산출된 상기 차이값이 미리 설정된 임계값 이상인 경우, 상기 서비스 요청을 익명

네트워크를 통한 우회 접속으로 추정함으로써 수행될 수 있다. 이 경우, 제 1 왕복 시간은 상기 서버와 클라이언트 간의 통신에 따른 왕복 시간이고, 제 2 왕복 시간은 상기 서버와 상기 익명 네트워크 내에 위치한 우회 클라이언트 간의 통신에 따른 왕복 시간이다. 또한, 상기 제 1 왕복 시간은 익명 네트워크 경유로 인한 시간 지연을 포함하며, 상기 제 2 왕복 시간에 비해 상대적으로 더 큰 값을 갖는다.

[59] 도 5a 및 도 5b는 일 실시예에 따른 도 4의 우회 접속 탐지 방법에서 각각 클라이언트와 서버 측에서 HTTP 왕복 시간을 측정하는 방법을 설명하기 위한 도면으로서, 설명의 편의를 위해 HTTP RTT(round trip time)을 예시하여 왕복 시간을 설명하도록 한다.

[60] 단순 RTT는 네트워크에서 송신자가 수신자에게 신호를 보내고 수신자로부터 이에 대한 응답을 받기까지의 시간을 의미한다. RTT에 가장 큰 영향을 미치는 요소는 송신자와 수신자간 네트워크의 거리와 매체이다. 네트워크가 원거리인 경우에 RTT값이 크며 근거리인 경우에는 작은 값을 보인다. 그리고 네트워크 매체가 광케이블과 같은 고속 매체인 경우에는 RTT값이 낮으며 구리와 같은 저속 매체인 경우에는 증가한다. 현재 대부분 광역 네트워크가 광케이블로 구성된 점을 고려하면 네트워크상 지리적 거리가 RTT에 가장 큰 영향을 미친다.

[61] HTTP RTT는 HTTP 처리 과정에서 클라이언트가 요청(Request)을 웹서버에 보내고 나서 웹서버로부터 응답(Response)을 받기까지의 시간이다. 이를 클라이언트(10)에서 측정하면 도 5a와 같이 정상적인 형태인 요청(Request)에서부터 응답(Response)까지의 시간이 된다. 그러나, 이러한 시간 측정 방식은 클라이언트(10) 측에서 이루어질 수 있는 것으로서, 본 발명의 실시예들이 구현되는 우회 접속을 탐지하는 서버(20) 측에서는 활용하기 어렵다. 따라서, 도 5b와 같이 서버(20) 측에서 왕복 시간을 추정하는 방법을 활용할 필요가 있다.

[62] 도 5b를 참조하면, 웹서버(20)에서는 응답(Response)에서부터 다음 요청(Request)까지의 시간 간격을 측정함으로써 HTTP RTT의 측정하는 것이 가능하다. 이 상황에서는 클라이언트(10)가 응답을 받은 다음 요청(Request)을 즉시 서버(20)에 전송하여야 할 것이다. 이러한 방법을 활용하여 서버(20) 측에서도 왕복 시간을 추정하는 것이 가능하다.

[63] 요약하건대, 왕복 시간은 클라이언트(10)가 서버(20)에 요청을 전송한 후 이에 대한 응답을 수신하기까지의 소요 시간을 측정함으로써 획득될 수도 있고, 또는 서버(20)가 요청에 응답한 후 응답에 따른 후속 요청을 수신하기까지의 소요 시간을 측정함으로써 획득될 수도 있다.

[64] 도 6a 및 도 6b는 일 실시예에 따른 도 4의 우회 접속 탐지 방법을 이용하여 왕복 시간의 측정이 이루어지는 과정을 직접 통신 방식과 익명 네트워크를 경유한 통신 방식을 비교하여 설명하기 위한 도면이다.

[65] 앞서 설명한 바와 같이, 클라이언트(10) 서버(20)로부터 요청에 따른 파일을

획득한 이후, 다음 파일을 요청시까지의 시간은 HTTP RTT를 측정하는 방법으로 정확히 관측 가능하다. 편의상 클라이언트(10)가 페이지 파일을 가져가고 난 이후 첫 번째 리소스 파일을 요청하는데까지의 시간과 리소스 파일을 가져가고 난 이후 다음 리소스 파일을 요청하는데까지의 시간을 각각 RTT_{pi}와 RTT_{ii}라고 정의한다. 정상 접속과 TOR와 같은 익명 네트워크(30)를 통한 우회 접속에서 RTT_{pi}와 RTT_{ii}는 각각 도 6a 및 도 6b와 같이 측정된다.

[66] 1 개의 연결(Connection)에 대해서 페이지 파일에 대한 RTT_{pi}는 1 개임에 비해 리소스 파일에 대한 RTT_{ii}는 다수 측정될 수 있으므로 이중 최소값(Minimum)을 구한다. 최소값을 구하는 이유는, 해당 엑시트 노드(Exit-node)에서 요청을 처리하는 과정에서 통신 지연이 아닌 다른 이유로 지연이 발생할 수 있기 때문에, 가장 작은 값이 순수한 통신 지연에 가까운 값에 해당하기 때문이다. 여러 개의 연결(Connection)이 있을 경우에는 각 연결에 대해서 구한 RTT_{pi}와 RTT_{ii}의 산술 평균을 구할 수 있을 것이다. 본 발명을 제안하는 과정에서 시뮬레이션을 위해 TOR를 이용한 익명 네트워크 실험을 통해 분석한 결과, RTT_{pi}는 RTT_{ii}에 비해 수백배 내지 천배 수준의 높은 값을 보이는데 반해, 직접 접속의 경우에는 거의 동일하다.

[67] 특히, 본 발명의 실시예들이 제안하고 있는 우회 접속을 탐지하는 방법은, 단순히 웹서버에서 자신에게 접속하는 트래픽을 분석하는 작업만을 통해 TOR를 통한 홈페이지 우회 접속을 정확히 탐지할 수 있다. 나아가, 네트워크 및 웹서버에 추가적인 부담이 전혀 없으며 프라이버시에 대한 침해 논란 또한 전혀 발생하지 않는다는 장점을 갖는다.

[68] 이상에서 비교한 바와 같이, HTTP 응답(Response) 데이터의 양이 클 수 있기 때문에, HTTP RTT는 네트워크의 대역폭에도 영향을 받는다. 기차에 비유하면 1만Km 거리를 기차의 선두가 1초만에 주파했더라도 기차의 길이가 1만Km인 경우 선로의 개수에 영향을 받는다. 선로가 1개인 경우에는 추가로 1초가 소요되지만 n개의 선로가 있다면 추가 소요시간은 n배 감소한다. 또한 클라이언트와 웹서버 사이에 중계 서버가 존재한 경우에는 중계 서버가 데이터를 받아서 암호화/복호화하거나 내용을 확인하는 과정에서 추가적인 지연이 발생한다. TOR를 사용하는 경우에는 3대의 중계 서버가 존재(심지어, 3대가 다른 국가인 경우도 빈번하다.)하므로 네트워크 거리가 비약적으로 증가하며 클라이언트와 엑시트 노드 간 암호 통신을 하는 과정에서 암/복호화로 인해 상당한 지연(연구 결과에 따르면 TOR 이용시 인터넷 접속속도가 10배 이상 지연될 수 있다는 보고가 있다.)이 발생한다. 따라서, 익명 네트워크를 이용시에 필연적으로 발생하는 네트워크상 지연을 관측하고 지연의 시점과 원인을 세밀히 분석하는 과정을 통해 클라이언트와 웹서버 사이에 익명 네트워크가 존재하는 점을 포착할 수 있다.

[69] 도 7은 본 발명의 HTTP 서비스 요청에 따른 익명 네트워크를 통한 우회 접속을 탐지하는 방법을 도시한 흐름도로서, 앞서 기술한 도 4의 우회 접속 탐지 방법을

HTTP 서비스를 중심으로 재작성한 것이다. 여기서는 설명의 중복을 피하기 위해 그 개요만을 약술하도록 한다.

[70] S710 단계에서, 서버는 HTTP 요청을 수신하고, 수신된 상기 HTTP 요청에 대해 응답하여 페이지 파일(page file)을 전송한다. 이렇게 전송된 페이지 파일은 익명 네트워크를 경유하여 진짜 클라이언트에 도달한 후, 파싱된다. 그러면, 클라이언트 파싱 결과로부터 추가적으로 호출하여야 하는 리소스 파일의 목록을 작성하게 된다. 이제 클라이언트는 리소스 파일의 목록에 기초하여 서버에 리소스 파일을 요청하게 된다.

[71] S720 단계에서, 서버는 상기 페이지 파일 응답에 따른 제 1 왕복 시간을 측정한다. 여기서, 제 1 왕복 시간은 익명 네트워크 경유로 인한 시간 지연을 포함하며, 이후 S740 단계를 통해 측정되는 제 2 왕복 시간에 비해 상대적으로 더 큰 값을 갖는다. 왜냐하면, 제 2 왕복 시간은 리소스 파일에 대한 응답에 따른 왕복 시간이기 때문이다. 또한, 상기 제 1 왕복 시간은 상기 서버와 클라이언트 간의 통신 경로를 이용하여 상기 서버가 상기 클라이언트에 상기 페이지 파일에 대한 응답을 전송한 이후 상기 클라이언트로부터 최초의 리소스 파일에 대한 요청을 수신하는 시점까지의 소요 시간으로서 산출될 수 있다.

[72] S730 단계에서, 서버는 상기 페이지 파일 응답에 따른 리소스 파일(resource file) 요청을 수신하고 대응하는 리소스 파일을 전송한다. 이러한 리소스 파일의 전송은 진짜 클라이언트가 아닌 익명 네트워크를 구성하는 가짜 클라이언트, 즉 엑시트 노드와의 통신을 통해 전달된다.

[73] S740 단계에서, 서버는 상기 리소스 파일 응답에 따른 제 2 왕복 시간을 측정한다. 여기서, 제 2 왕복 시간은 상기 서버와 상기 익명 네트워크 내에 위치한 우회 클라이언트 간의 통신 경로를 이용하여 상기 서버가 상기 최초의 리소스 파일에 대한 응답을 전송한 이후 상기 클라이언트로부터 다음 리소스 파일에 대한 요청을 수신하는 시점까지의 소요 시간으로서 산출될 수 있다.

[74] S750 단계에서, 서버는 S720 단계 및 S740 단계를 통해 각각 측정된 상기 제 1 왕복 시간과 상기 제 2 왕복 시간 간의 차이에 기초하여 왕복 시간들 간에 불규칙성이 발생하였는지 여부를 검사함으로써 상기 서비스 요청에 대한 우회 접속 여부를 판별한다. 여기서, 우회 접속 여부를 판별하는 과정은, 상기 제 1 왕복 시간과 상기 제 2 왕복 시간 간의 차이값을 산출하고, 산출된 상기 차이값이 미리 설정된 임계값 이상인 경우, 상기 서비스 요청을 익명 네트워크를 통한 우회 접속으로 추정함으로써 수행될 수 있다. 특히, S750 단계의 판별 과정에서, 우회 접속으로 추정된 경우, 산출된 상기 차이값의 통계적 분포를 이용하여 상기 익명 네트워크의 종류를 식별하는 것이 가능하다. 여기서 통계적 분포란, 차이값의 범위, 편차, 시계열 등이 활용될 수 있으며, 보다 구체적인 식별 방법은 이후 도 9를 통해 소개하도록 한다.

[75] 나아가, 상기 제 1 왕복 시간 및 상기 제 2 왕복 시간 측정을 위한 대상 신호가 복수 개인 경우, 복수 개의 대상 신호 중 도착 시간이 최소인 값을 측정하여

각각의 왕복 시간을 산출하는 것이 바람직하다.

[76] 도 8 및 도 9는 다양한 네트워크 환경을 가정하여 왕복 시간을 측정한 실험 결과를 예시한 도면이다.

[77] 도 8을 참조하면, 직접 접속의 경우, 근거리 및 원거리의 경우 모두 RTT_{pi} 및 RTT_{ii}가 서로 유사한 값으로 측정되었으며, 그 결과 RTT_{pi}/RTT_{ii}가 1에 근사한 값으로 산출되었음을 보여주고 있다. 이에 반해, 익명 네트워클 활용한 우회 접속의 경우 RTT_{pi}가 RTT_{ii}에 비해 상대적으로 큰 값을 가지므로, 그 결과 RTT_{pi}/RTT_{ii}가 2 이상의 값으로 산출되었음을 보여주고 있다.

[78] 도 9를 참조하면, TOR를 이용한 우회 접속 이외에 Zenmate를 이용한 우회 접속에 따른 측정 결과를 도시하고 있다. 또한, 공개된 적어도 4개의 브라우저를 이용하여 실험을 하였다. 브라우저의 특성에 따른 파싱 지연 시간을 고려할 경우에도, 직접 접속의 경우에는 $MIN(RTT_{pi})/MIN(RTT_{ii})$가 거의 1에 근사한 값을 보여주고 있는 반면, TOR나 Zenmate를 이용한 우회 접속의 경우에는 2배 이상의 높은 값을 보여주고 있음을 확인할 수 있다.

[79] 한편, 본 발명의 실시예들은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[80] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현하는 것을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

[81] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

산업상 이용가능성

[82] 상기된 본 발명의 실시예들에 따르면, 서버에서 자신에게 접속하는 트래픽 분석을 통해 파일의 속성에 따라 왕복 시간의 차이가 존재하는지, 그 불규칙성을 검사함으로써 익명 네트워크를 통한 우회 접속을 정확하게 탐지할 수 있을 뿐만

아니라, 네트워크 및 서버에 추가적인 부담이 전혀 없으면서도 프라이버시 침해에 관한 논란 또한 전혀 발생하지 않는다는 장점을 갖는다.

청구범위

[청구항 1] 익명 네트워크를 통한 우회 접속을 탐지하는 방법에 있어서,
서버가 하나의 서비스 요청을 구성하는 순차적인 복수의 요청을 수신하는 단계;
상기 서버가 수신된 상기 복수의 요청에 대해 응답하는 단계;
상기 서버가 상기 요청 및 응답에 따른 왕복 시간(round trip time, RTT)들을 각각 측정하는 단계; 및
상기 서버가 측정된 상기 왕복 시간들 간의 차이에 기초하여 상기 서비스 요청에 대한 우회 접속 여부를 판별하는 단계;를 포함하는 방법.

[청구항 2] 제 1 항에 있어서,
상기 우회 접속 여부를 판별하는 단계는,
익명 네트워크를 통한 경유로 인하여 상기 왕복 시간들 간에 불규칙성이 발생하였는지 여부를 검사함으로써 수행되는 것을 특징으로 하는 방법.

[청구항 3] 제 1 항에 있어서,
상기 우회 접속 여부를 판별하는 단계는,
복수의 왕복 시간 중 제 1 요청에 따른 제 1 왕복 시간과 상기 제 1 요청에 대한 응답 이후 상기 서버에 수신되는 제 2 요청에 따른 제 2 왕복 시간 간의 차이값을 산출하는 단계; 및
산출된 상기 차이값이 미리 설정된 임계값 이상인 경우, 상기 서비스 요청을 익명 네트워크를 통한 우회 접속으로 추정하는 단계;를 포함하는 방법.

[청구항 4] 제 3 항에 있어서,
상기 제 1 왕복 시간은 상기 서버와 클라이언트 간의 통신에 따른 왕복 시간이고,
상기 제 2 왕복 시간은 상기 서버와 상기 익명 네트워크 내에 위치한 우회 클라이언트 간의 통신에 따른 왕복 시간인 것을 특징으로 하는 방법.

[청구항 5] 제 3 항에 있어서,
상기 제 1 왕복 시간은 익명 네트워크 경유로 인한 시간 지연을 포함하며, 상기 제 2 왕복 시간에 비해 상대적으로 더 큰 값을 갖는 것을 특징으로 하는 방법.

[청구항 6] 제 1 항에 있어서,
상기 왕복 시간은 클라이언트가 서버에 요청을 전송한 후 이에 대한 응답을 수신하기까지의 소요 시간을 측정함으로써 획득되는 것을 특징으로 하는 방법.

[청구항 7] 제 1 항에 있어서,
상기 왕복 시간은 서버가 요청에 응답한 후 응답에 따른 후속 요청을 수신하기까지의 소요 시간을 측정함으로써 획득되는 것을 특징으로 하는 방법.

[청구항 8] 제 1 항에 있어서,
판별 결과, 상기 서비스 요청이 익명 네트워크를 이용한 우회 접속으로 추정된 경우 상기 접속을 차단하는 단계;를 더 포함하는 방법.

[청구항 9] 익명 네트워크를 통한 우회 접속을 탐지하는 방법에 있어서,
서버가 HTTP 요청을 수신하는 단계;
상기 서버가 수신된 상기 HTTP 요청에 대해 응답하여 페이지 파일(page file)을 전송하는 단계;
상기 서버가 상기 페이지 파일 응답에 따른 제 1 왕복 시간을 측정하는 단계;
상기 서버가 상기 페이지 파일 응답에 따른 리소스 파일(resource file) 요청을 수신하고 대응하는 리소스 파일을 전송하는 단계;
상기 서버가 상기 리소스 파일 응답에 따른 제 2 왕복 시간을 측정하는 단계; 및
상기 서버가 측정된 상기 제 1 왕복 시간과 상기 제 2 왕복 시간 간의 차이에 기초하여 왕복 시간들 간에 불규칙성이 발생하였는지 여부를 검사함으로써 상기 서비스 요청에 대한 우회 접속 여부를 판별하는 단계;를 포함하는 방법.

[청구항 10] 제 9 항에 있어서,
상기 우회 접속 여부를 판별하는 단계는,
상기 제 1 왕복 시간과 상기 제 2 왕복 시간 간의 차이값을 산출하는 단계;
산출된 상기 차이값이 미리 설정된 임계값 이상인 경우, 상기 서비스 요청을 익명 네트워크를 통한 우회 접속으로 추정하는 단계; 및
우회 접속으로 추정된 경우, 산출된 상기 차이값의 통계적 분포를 이용하여 상기 익명 네트워크의 종류를 식별하는 단계;를 포함하는 방법.

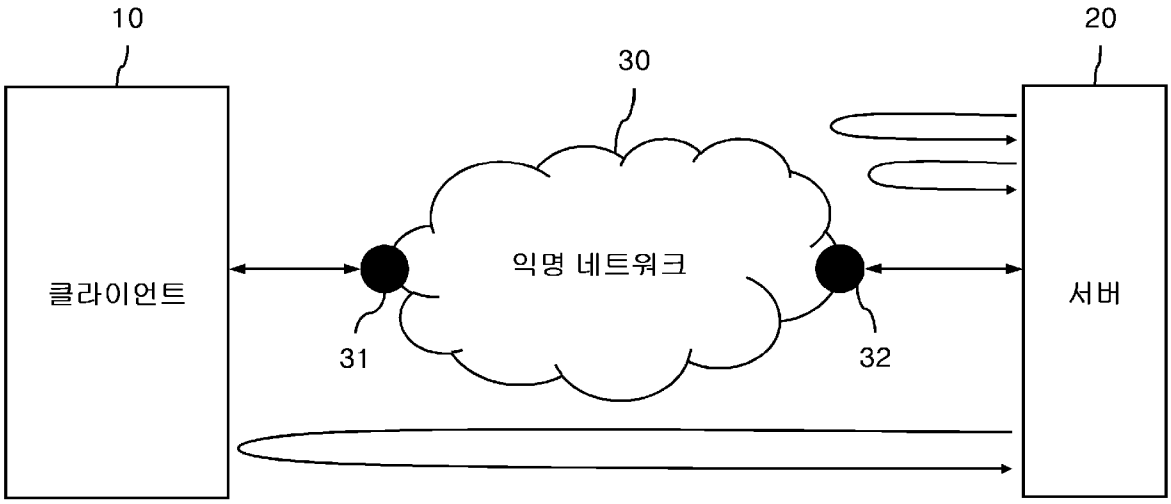
[청구항 11] 제 9 항에 있어서,
상기 제 1 왕복 시간은 익명 네트워크 경유로 인한 시간 지연을 포함하며, 상기 제 2 왕복 시간에 비해 상대적으로 더 큰 값을 갖는 것을 특징으로 하는 방법.

[청구항 12] 제 9 항에 있어서,
상기 제 1 왕복 시간은 상기 서버와 클라이언트 간의 통신 경로를

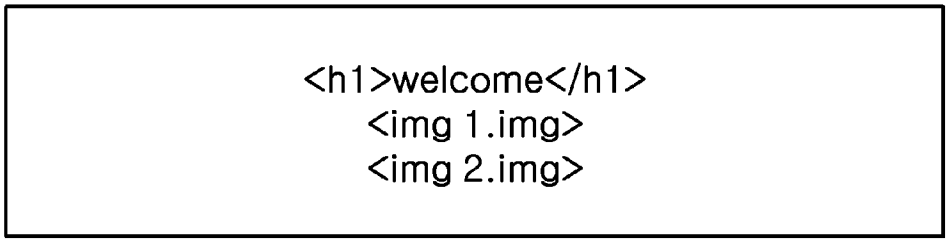
이용하여 상기 서버가 상기 클라이언트에 상기 페이지 파일에 대한 응답을 전송한 이후 상기 클라이언트로부터 최초의 리소스 파일에 대한 요청을 수신하는 시점까지의 소요 시간이고,
상기 제 2 왕복 시간은 상기 서버와 상기 익명 네트워크 내에 위치한 우회 클라이언트 간의 통신 경로를 이용하여 상기 서버가 상기 최초의 리소스 파일에 대한 응답을 전송한 이후 상기 클라이언트로부터 다음 리소스 파일에 대한 요청을 수신하는 시점까지의 소요 시간인 것을 특징으로 하는 방법.

[청구항 13] 제 9 항에 있어서,
상기 제 1 왕복 시간 및 상기 제 2 왕복 시간 측정을 위한 대상 신호가 복수 개인 경우, 복수 개의 대상 신호 중 도착 시간이 최소인 값을 측정하여 각각의 왕복 시간을 산출하는 것을 특징으로 하는 방법.

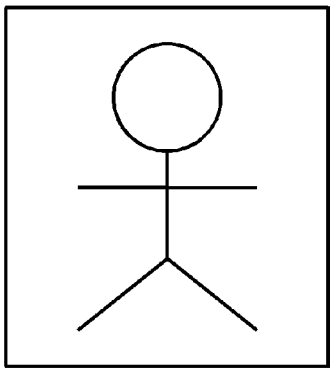
[Fig. 1]



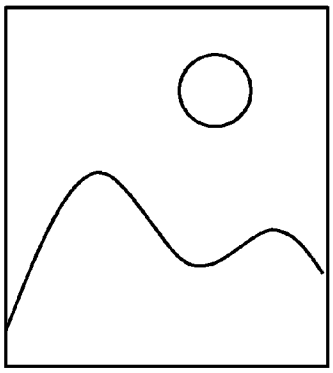
[Fig. 2a]



[페이지 파일]



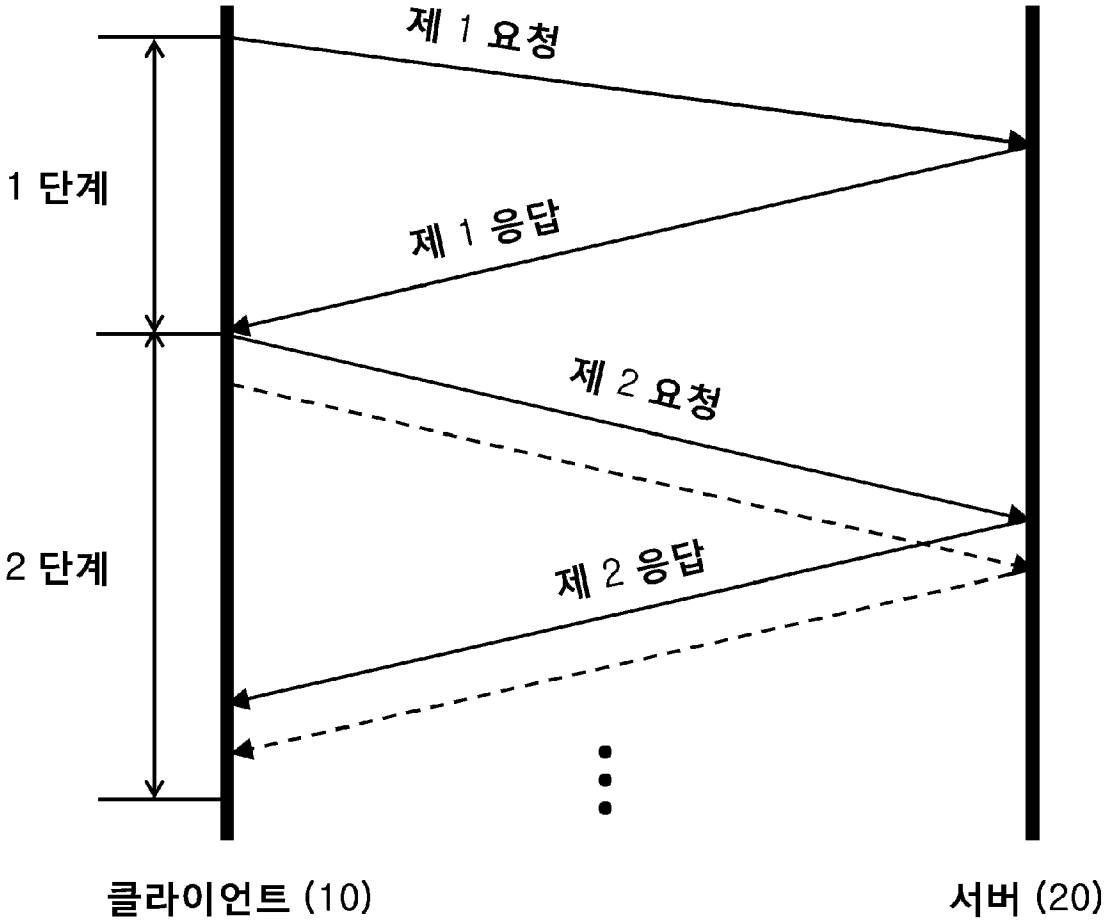
1.img



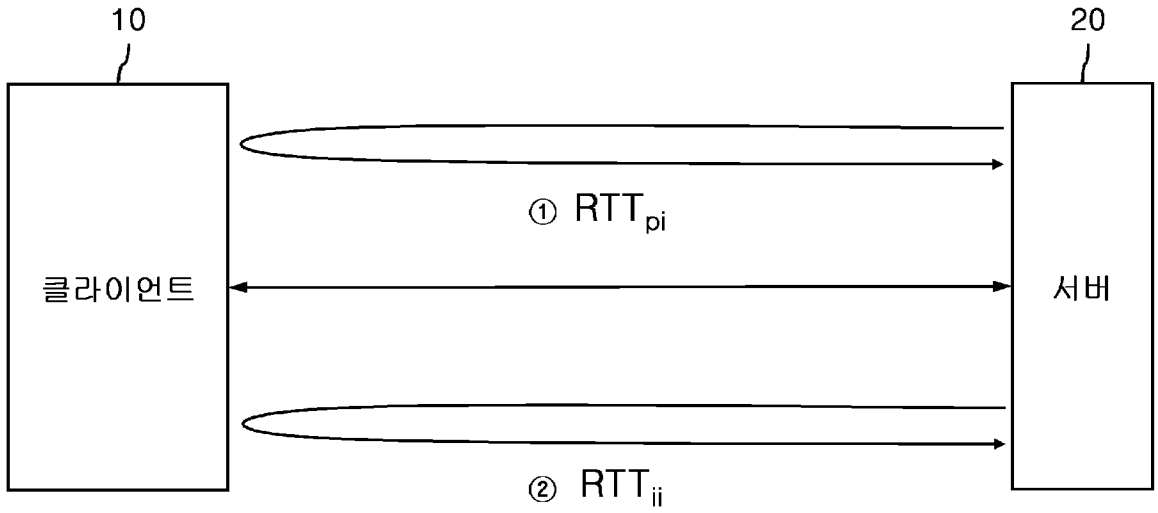
2.img

[리소스 파일]

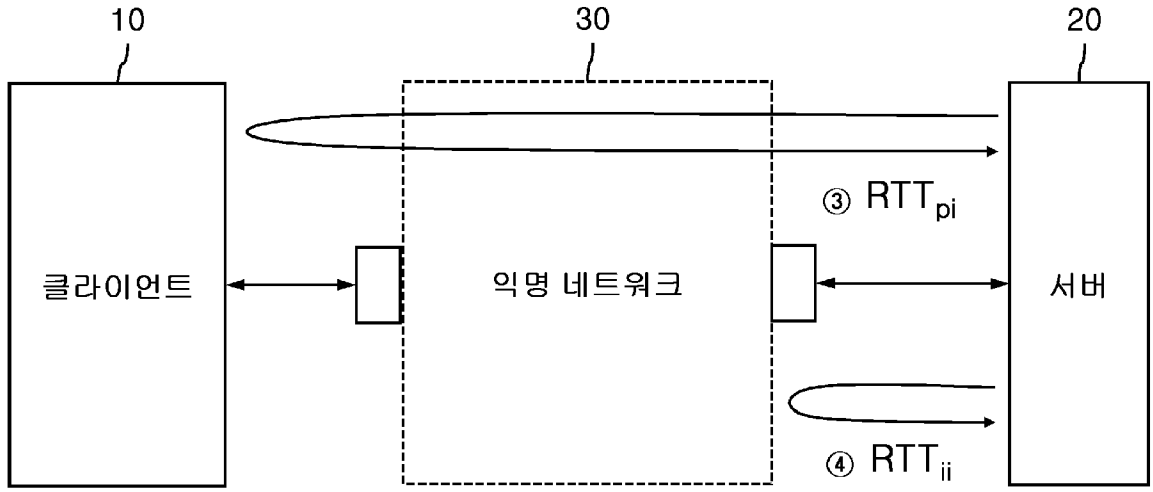
[Fig. 2b]


제 1 요청
1 단계
제 1 응답
제 2 요청
2 단계
제 2 응답
클라이언트 (10)
서버 (20)

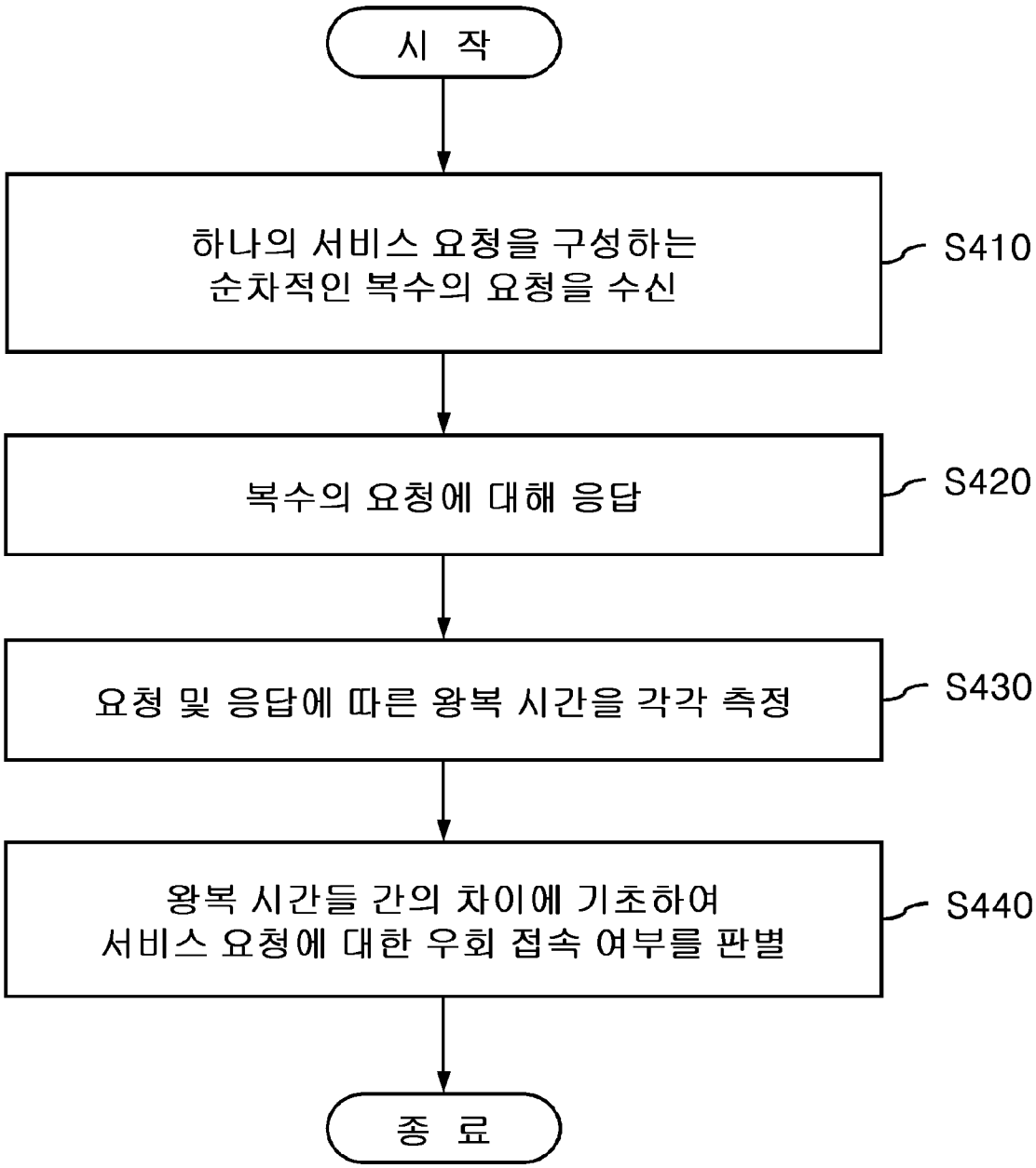
[Fig. 3a]


10
20
① RTTpi
클라이언트
서버
② RTTii

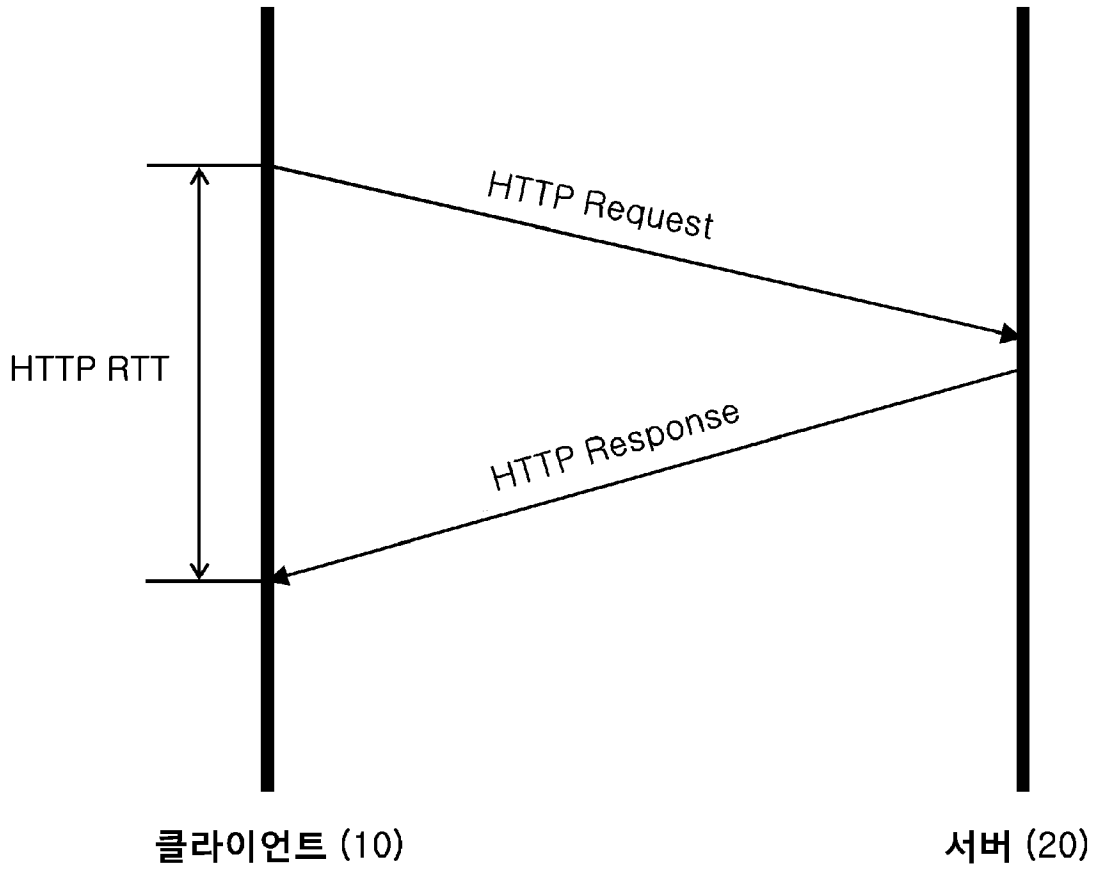
[Fig. 3b]


10
30
20
③ RTTpi
클라이언트
익명 네트워크
서버
④ RTTii

[Fig. 4]

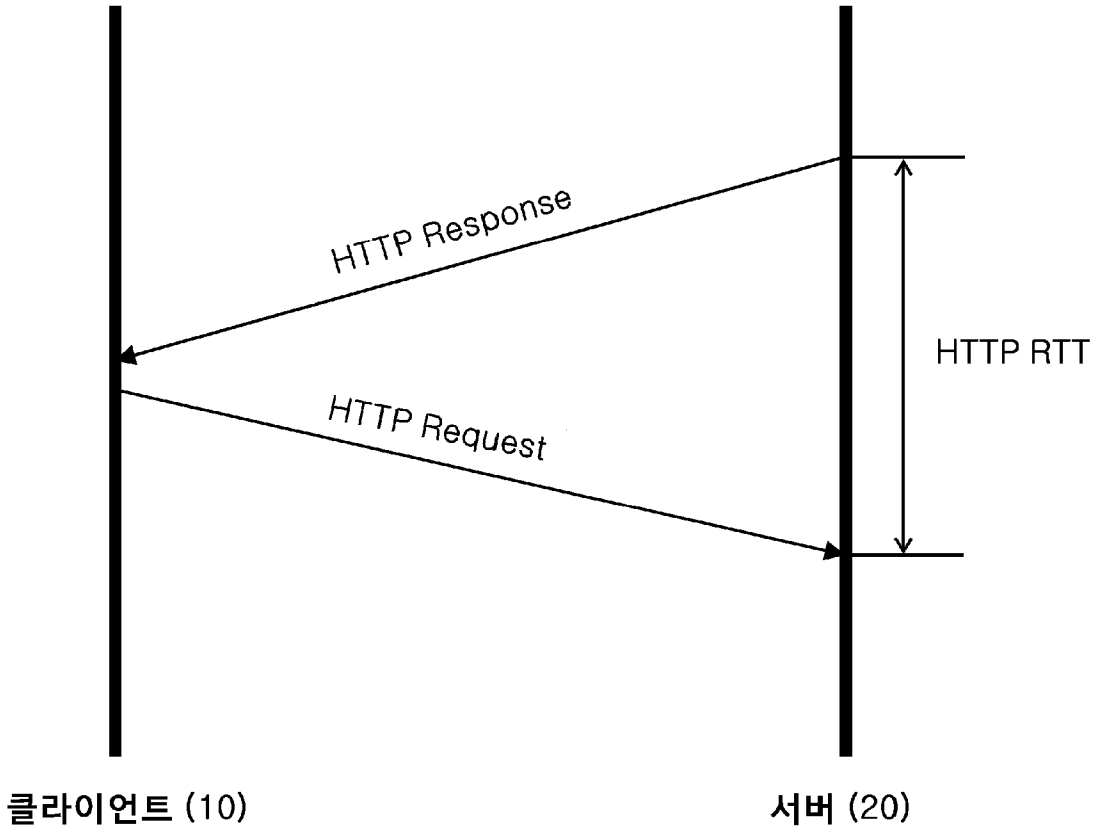

시 작
하나의 서비스 요청을 구성하는
순차적인 복수의 요청을 수신
S410
복수의 요청에 대해 응답
S420
요청 및 응답에 따른 왕복 시간을 각각 측정
S430
왕복 시간들 간의 차이에 기초하여
서비스 요청에 대한 우회 접속 여부를 판별
S440
종 료

[Fig. 5a]



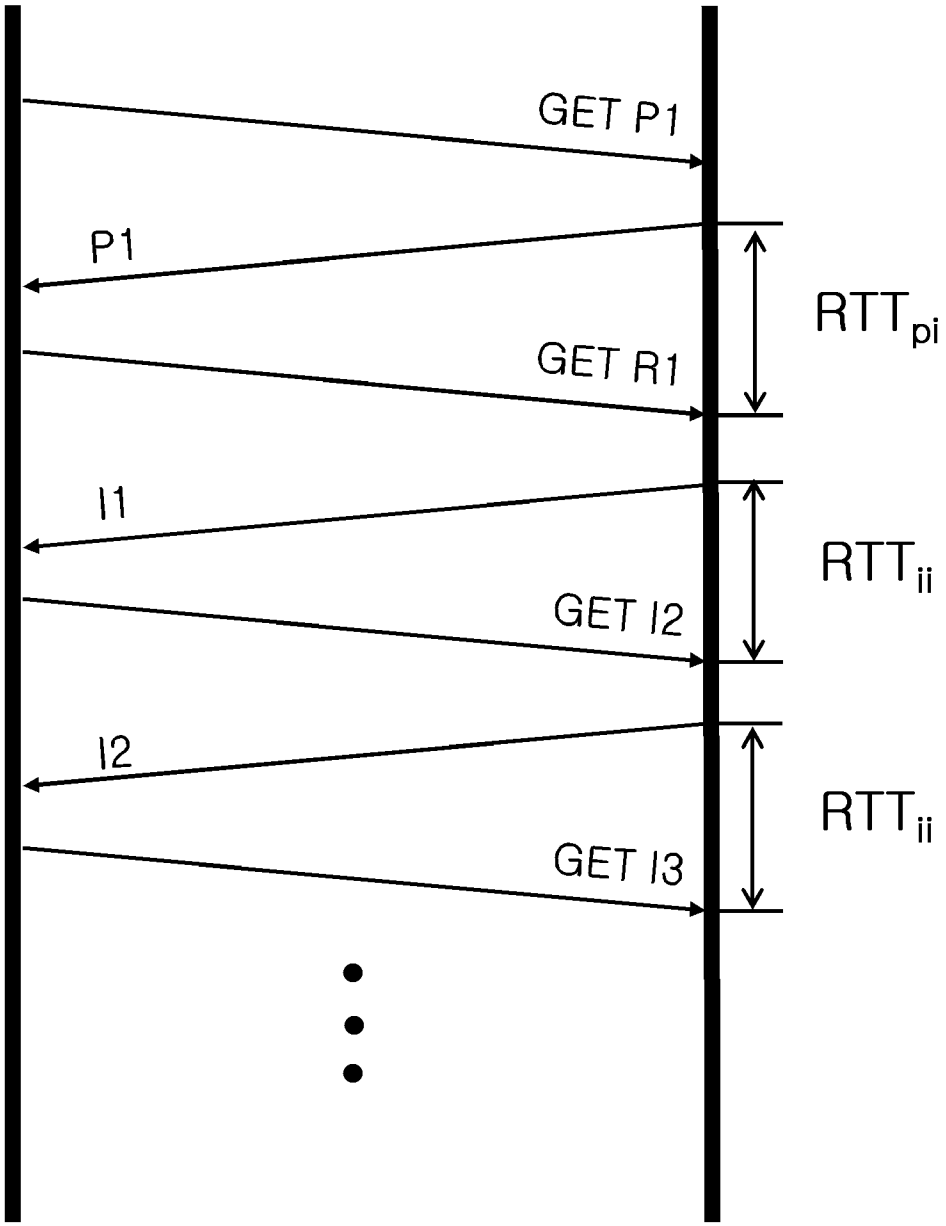
[Client-side HTTP RTT]

[Fig. 5b]

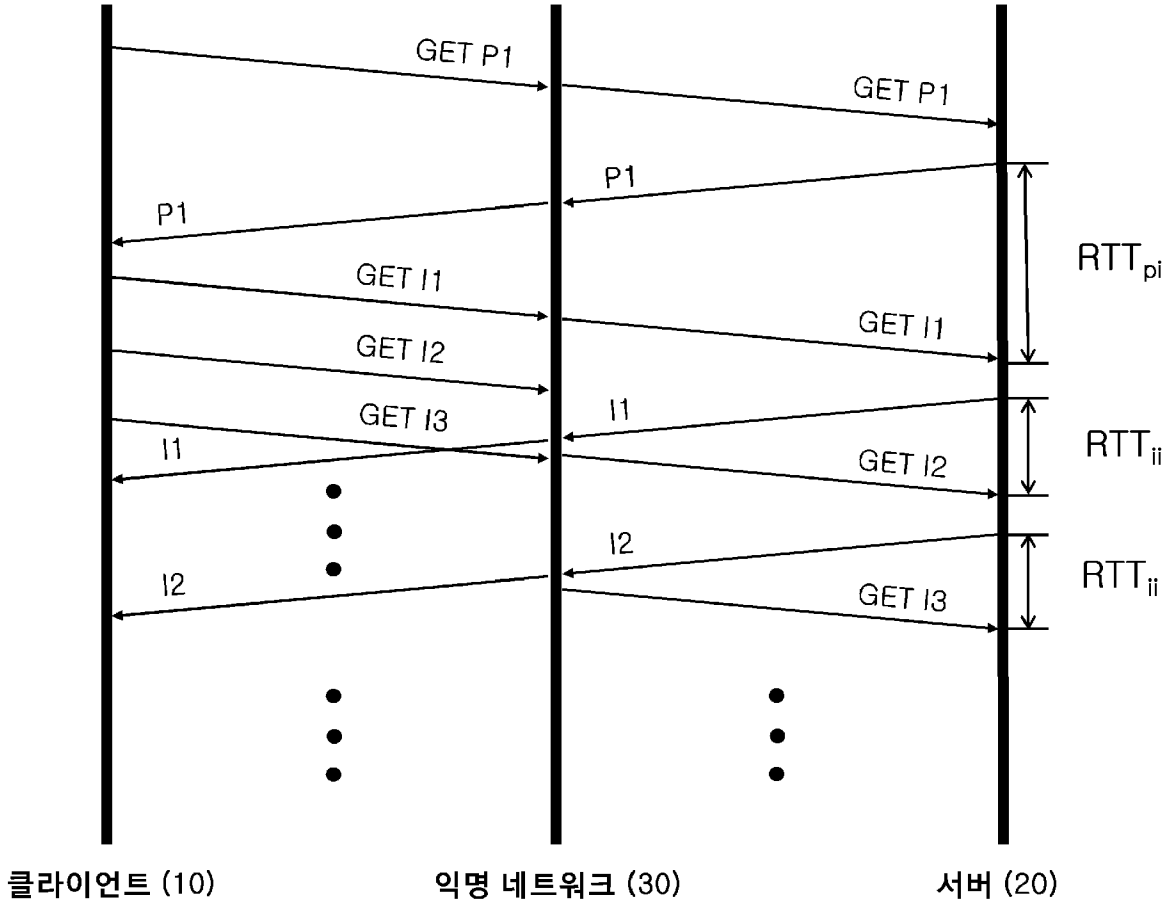


[Server-side HTTP RTT]

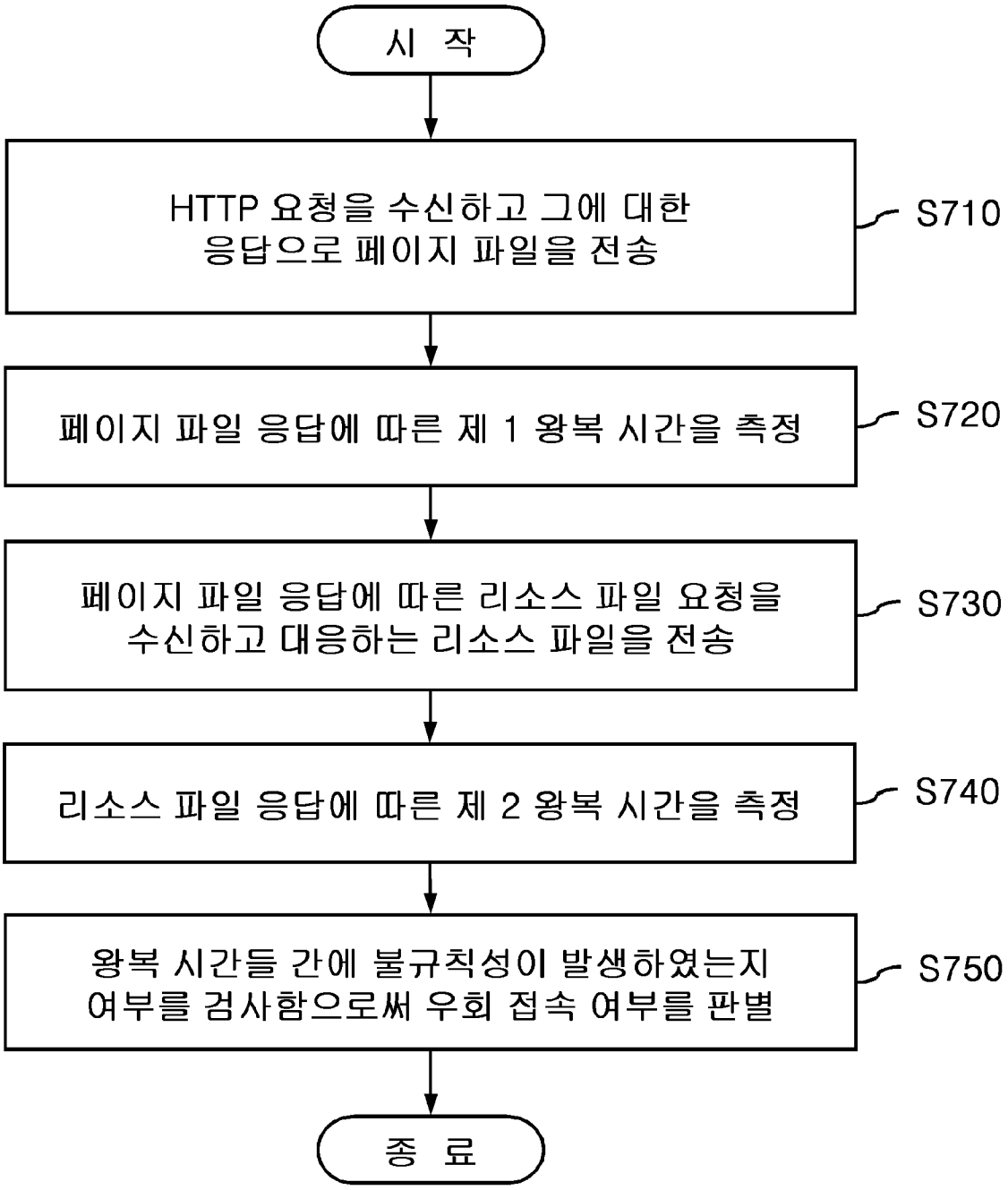
[Fig. 6a]


GET P1
P1
RTTpi
GET R1
I1
RTTii
GET I2
I2
RTTii
GET I3
클라이언트 (10)
서버 (20)

[Fig. 6b]


GET P1
GET P1
P1
P1
GET I1
GET I1
GET I2
GET I3
I1
I1
GET I2
I2
I2
GET I3
RTTpi
RTTii
RTTii
클라이언트 (10)
익명 네트워크 (30)
서버 (20)

[Fig. 7]



[Fig. 8]

	RTT_{pi}	RTT_{ii}	RTT_{pi}/RTT_{ii}
직접접속	크다	크다	1.0~1.3
익명 네트워크 이용시	크다	작다	> 2.0

[Fig. 9]

접속방식	클라이언트	브라우져	RTT_{pi}			RTT_{ii}			$MIN(RTT_{pi})/MIN(RTT_{ii})$
			MAX	MIN	AVG	MAX	MIN	AVG	
직접 접속	국외(미국 서부)→국내	Explorer	608	222	330	238	201	218.2	1.1
		Chrome	261	224	240	315	204	241	1.1
		Safari	261	203	240	229	198	205	1.0
		FireFox	397	245	321	201	194	196	1.3
TOR 이용 접속	1차 : 국외(미국 서부)→TOR(?)→TOR(독일)→국내	FireFox	772	610	623	303	292	296	2.1
	2차 : 국외(미국 서부)→TOR(?)→TOR(프랑스)→국내	FireFox	982	730	813	310	294	298	2.5
	3차 : 국외(미국 서부)→TOR(?)→TOR(오스트리아)→국내	FireFox	1140	658	728	326	316	320	2.1
Chrome Zenmate 이용 접속	1차 : 국외(미국 서부)→Zenmate(홍콩)→국내	Chrome	1132	453	659	59	46	51	9.8
	2차 : 국외(미국 서부)→Zenmate(독일)→국내	Chrome	779	730	756	314	308	311	2.4
	3차 : 국외(미국 서부)→Zenmate(미국)→국내	Chrome	512	335	416	186	183	184	1.8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2015/000060

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/26(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 12/26; G06F 15/16; H04L 29/10; G06F 21/20; H04L 12/28; H04L 12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: "round trip time", "RTT", "server", "client"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2010-177839 A (HITACHI SOFTWARE ENG CO., LTD.) 12 August 2010 See paragraphs [0012]-[0016]	1-8 9-13
Y	KR 10-2007-0034341 A (SAMSUNG ELECTRONICS CO., LTD.) 28 March 2007 See paragraphs [0054]-[0062] and figure 4	9-13
A	KR 10-0854137 B1 (BEA SYSTEMS, INC.) 26 August 2008 See paragraphs [0035]-[0039] and figure 2	1-13

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
03 APRIL 2015 (03.04.2015)	**06 APRIL 2015 (06.04.2015)**
Name and mailing address of the ISA/**KR** Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2015/000060

Patent document cited in search report	Publication date	Patent family member	Publication date
JP 2010-177839 A	12/08/2010	NONE	
KR 10-2007-0034341 A	28/03/2007	CN 101268674 A0	17/09/2008
		CN 101268674 B	02/01/2013
		EP 1927234 A1	04/06/2008
		US 2007-0073730 A1	29/03/2007
		US 8260843 B2	04/09/2012
		WO 2007-035053 A1	29/03/2007
KR 10-0854137 B1	26/08/2008	NONE	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2015/000060

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 12/26(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04L 12/26; G06F 15/16; H04L 29/10; G06F 21/20; H04L 12/28; H04L 12/56

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: '왕복 시간' , 'RTT' ,'서버', '클라이언트'

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X Y	JP 2010-177839 A (HITACHI SOFTWARE ENG CO., LTD.) 2010.08.12 단락 [0012]-[0016]	1-8 9-13
Y	KR 10-2007-0034341 A (삼성전자주식회사) 2007.03.28 단락 [0054]-[0062] 및 도면 4	9-13
A	KR 10-0854137 B1 (비이에이 시스템즈 인코포레이티드) 2008.08.26 단락 [0035]-[0039] 및 도면 2	1-13

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2015년 04월 03일 (03.04.2015)	2015년 04월 06일 (06.04.2015)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 ++82 42 472 7140

심사관
전용해
전화번호 +82-42-481-5765

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2015/000060

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
JP 2010-177839 A	2010/08/12	없음	
KR 10-2007-0034341 A	2007/03/28	CN 101268674 A0	2008/09/17
		CN 101268674 B	2013/01/02
		EP 1927234 A1	2008/06/04
		US 2007-0073730 A1	2007/03/29
		US 8260843 B2	2012/09/04
		WO 2007-035053 A1	2007/03/29
KR 10-0854137 B1	2008/08/26	없음	