Journal of The Institute of Electronics and Information Engineers Vol.52, NO.11, November 2015 http://dx.doi.org/10.5573/ieie.2015.52.11.020
ISSN 2287-5026(Print) / ISSN 2288-159X(Online)

논문 2015-52-11-3

차단우회 및 익명성보장 웹브라우징 시스템

(Anti-Censorship and Anonymous Web-Browsing System)

이 은 수*, 이 석 복**

(Eunsu Lee and Suk-bok Lee©)

요 약

인터넷 사용 인구의 증가함에 따라 인터넷 차단우회 및 익명성 서비스에 대한 필요성은 해마다 증가하고 있다. 기존의 차단우회 및 익명성 서비스를 제공하는 시스템들은 각자의 기술적인 문제점들로 인하여 현실적으로 사용이 어려운 경우가 많다. 본 논문은 검열 ISP 안의 사용자와 자유 ISP 안의 사용자가 상호 협력을 통하여 차단 우회 및 익명성을 획득할 수 있는 방법에 대하여 제안한다.

Abstract

Internet censorship-circumvention and anonymizing services are becoming important with an increase in Internet population. Existing circumvention/anonymizing systems, however, have their own limitations, and they mainly suffer from the shortage of volunteers who relay others' traffic to bypass censors. In this paper, we present a new way of achieving censorship-circumvention while guaranteeing anonymity through the cooperation between censored and uncensored users.

Keywords : Anti-censorship, anonymity.

Ⅰ. 서 론

인터넷 검열 및 감시는 인터넷 사용의 편리와 함께 점점 더 증가하고 있는 추세이다. 전 세계 약 70%의 국가가 다양한 방법으로 인터넷을 통한 정보의 차단을 수행하고 있으며 이를 정치적, 사회적 이슈와 관련된 온라인에서의 만남에 대한 감시 및 체포와 정보의 공개 등을 차단하는데 사용하고 있다.[1] 이에 따라 사용자의 사생활을 보호하기 위한 인터넷 검열 및 감시 우회 방법의 중요성이 증가되고 있다.

인터넷 검열 및 감시를 우회하기 위한 방법으로 외부의 자원자를 거쳐서 프록시에 접속하는 방법이 많이 사용되고 있다. 이러한 방법은 자원자의 수가 많을수록 모든 자원자를 차단할 수 없기 때문에 검열이 어려워진다. 그러나 익명성 확보를 위해 주로 사용되는 자원자 기반 방법인 Tor[2]의 경우 하루 평균 약 75만 명의 사람들이 다양한 목적으로 이용하고 있음에도 불구하고[3] 자원자 부족 및 지능화된 차단 및 감시 시스템의 도입으로 인하여 중국과 같은 검열이 심한 국가에서는 사용이 어려운 실정이다.[4] 자원자를 모집을 독려하기 위한 방안으로 보상을 제공하는 다양한 방법들이 제안되고 있지만 정보 노출 등으로 인하여 실질적인 사용에는 어려움이 있다.

본 논문에서는 서로 다른 검열망에 있는 사용자들이

* 학생회원, ** 정회원 한양대학교 컴퓨터공학과
(Department of Computer Science and Engineering, Hanyang University)
※ 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2014R1A2A2A01003696).
© Corresponding Author(E-mail: sble@hanyang.ac.kr)
Received ; September 7, 2015 Revised ; September 21, 2015
Accepted ; November 4, 2015

상호협력을 통하여 인터넷 차단우회 및 익명성을 획득할 수 있는 시스템을 제안하고 있다.

본 논문에서 제안하는 시스템은 사용자들 간의 상호보완을 통하여 일반적인 자원자 모집보다 강력한 동기를 제공할 수 있으며 트래픽과 같이 일반적인 개인의 자원 교환을 바탕으로 하기 때문에 보상을 위한 별도의 재화를 도입할 필요가 없다. 또한 차단우회 및 익명성을 위한 최소 연결 구조, HTTP를 통한 웹브라우징을 고려한 내부 프로토콜 설계를 통하여 웹페이지의 응답시간을 최소화함으로 사용자의 대기시간을 줄이고 만족도를 증가시킬 수 있다.

Ⅱ장에서는 기존의 우회방법에 관하여 간략하게 설명하고 Ⅲ장에서는 일반적인 시스템 모델 및 가정에 대해 기술하며 Ⅳ장에서는 해당 시스템의 구성 및 프로토콜에 대해 상세히 설명한다. Ⅴ장에서는 Ⅱ장에서 설명한 기존의 방법과의 성능 비교 결과를 보이며 마지막 장에서 본 연구의 결론과 앞으로의 과제에 관해 기술한다.

Ⅱ. 기존 기술

인터넷 검열, 차단 우회 및 익명성을 확보하기 위해 다양한 방법들이 제안되었다.

프록시 기반 기법은 차단되어 있는 웹페이지에 접속하기 위해 검열망 바깥의 프록시 서버를 사용하여 접속함으로 검열망을 우회할 수 있는 방법이다. 사용자는 암호화를 통해 정보의 노출을 줄일 수 있다. 검열망 우회를 위해 많이 사용되는 VPN 서비스[5~6] 또한 프록시 기반 방법의 일종이다. 그러나 프록시 IP들은 잘 알려져 있어 블랙리스트에 등록함으로 쉽게 차단이 가능하다. 또한 사용자의 프록시 서버 사용이 쉽게 노출되고 프록시 서버에 사용자의 접속 기록 및 요청 기록이 남기 때문에 차단우회 및 익명성의 문제가 있다.

프록시 사용을 숨기기 위해 일반적인 HTTP 트래픽을 Skype, VoIP 와 같은 오디오, 비디오 트래픽인 것처럼 조작하여 데이터를 전송하는 방법들이 사용된다.[7][8][9] UDP 사용으로 인한 신뢰성 문제는 FEC방식으로 보완이 가능하지만 실제 오디오, 비디오 트래픽의 경우 패킷손실에 큰 영향을 받지 않는 특징을 이용하여 약 10~15% 가량의 패킷을 선택적으로 탈락시켜 HTTP 트래픽 전송을 방해하는 것이 가능하다.[10] 또한 오디오, 비디오 트래픽을 모방하기 때문에 응답 시간이 길고 사용자의 만족도가 낮다.

또 다른 검열 차단 방어 방법으로는 네트워크 시설에 의존하는 방법들이 있다. Telex[11], Decoy routing[12], Cirripede[13]등이 해당하는데, 일반적인 웹사이트의 트래픽을 생성하면, 네트워크 안에 의도적으로 배치된 디코이 라우터를 통하여 프록시로 연결된다. 기존의 프록시 기반 기법과는 다르게 실제로 사용하고 있는 프록시의 주소가 드러나지 않게 우회가 가능하지만 디코이 라우터의 배치를 위해서는 ISP의 협조가 필요하기 때문에 실용화가 어렵고 프록시 서버에서 결국 사용자의 정보가 노출된다는 어려움이 있다.

Tor[2]와 같은 자원자 기반 기법은 주로 검열망 우회와 개인 정보 보호를 위하여 사용되는데, 자원자들을 모아서 연계 서비스를 제공하는 것이다. 자원자가 충분하지 않은 경우 검열 ISP에서 일부 자원자 IP 차단으로 자원자 기반 기법을 방지하는 것이 가능하다.[4] 이를 방지하기 위해 자원자 기반 기법에서는 자원자 모집을 독려하기 위하여 가상 화폐[14~15]나 티켓[16]을 사용하여 우선순위를 획득하는 등 참여자에게 보상을 제공하는 방법 등이 제안되고 있다. 그러나 이러한 방법들은 자원자가 직접적으로 혜택을 누리기는 어려울 뿐만 아니라 정보노출의 가능성 또한 존재한다.

Ⅲ. 시스템 모델 및 가정

1. 공격 모델

본 논문의 온라인 검열 및 감시를 수행하는 검열 ISP와 온라인 감시를 수행하는 자유 ISP를 모두 고려한다.

검열 ISP 내부의 사용자들은 해당 지역의 ISP의 방침에 따라 특정한 웹페이지들은 접근이 불가능하며 검열 ISP는 사용자의 웹사이트 접근에 대한 감시를 수행한다. 검열 ISP는 온라인 검열 및 감시를 수행하기 위해 IP 주소 차단, 심층 패킷 분석(deep packet inspection), DNS 하이재킹(DNS hijacking) 등의 기법을 사용한다. 검열 ISP 내부의 사용자들은 기본적으로 허가 없이 검열 웹페이지를 제외한 외부의 다른 서버에 접속하는 것이 가능하다고 가정한다.

온라인 감시를 수행하는 자유 ISP 내부의 사용자들은 자유롭게 다른 서버에 접속하는 것이 가능하지만 인터넷 감시에 노출되어 있다. 인터넷 감시는 주로 사용

자의 웹사이트 방문 기록에 관한 것으로 웹사이트 방문 기록은 SSL/TLS 등으로 암호화 되어 있더라도 노출되는 정보이다. ISP는 투명(transparent) 프록시 등을 이용하여 사용자의 동의 없이 사용자의 웹사이트 방문 기록을 수집하거나 중간자 공격을 사용하여 사용자의 접근을 막을 수 있다. 프록시를 사용하는 경우 또한 사용자의 정보가 프록시에 노출되고 트래픽을 암호화 하지 않은 경우, 경로상의 모든 노드들이 사용자의 정보를 취득할 수 있다.

2. 시스템 목표

본 논문에서 제안하는 시스템의 목표는 다음과 같다.

- 차단 방지(unblockability) 검열 ISP에서는 대부분의 IP를 차단하여 사용자의 인터넷 사용을 금지하지 않고서는 내부의 사용자들이 본 논문에서 제안하는 시스템을 사용하여 검열망을 우회하여 차단된 웹페이지에 접근하는 것을 막을 수 없다.

- 불관찰성(unobservability) 검열 ISP에서는 내부의 사용자가 본 논문에서 제안하는 시스템을 사용하는 것을 탐지할 수 없다.

- 불연계성(unlinkability) 본 논문에서 제안하는 시스템을 사용하는 경우 ISP에서는 사용자가 어떤 웹사이트에 접근하는지 알 수 없다.

- 짧은 지연시간(low latency) 본 논문에서 제안하는 시스템은 일반적인 지연시간과 비슷한 정도의 지연시간을 소모한다.

- 이용성(usability) 본 논문에서 제안하는 시스템은 TLS/TCP와 같이 일반적으로 사용되는 프로토콜을 기반으로 디자인 되었고 웹브라우저와 같이 사용이 쉬운 플랫폼을 택하여 만들어졌다.

Ⅳ. 구성 및 프로토콜

1. 기본 구성

그림 1은 본 논문에서 제안하는 시스템의 기본적인 구성 요소 및 연결 관계이다.

검열 ISP 내부의 사용자와 자유 ISP 내부의 사용자로 이루어진 짝은 서로간의 익명성 및 우회를 위한 트래픽 전달을 수행한다. 모든 사용자들은 익명성이 유지되기를 바라며 검열 ISP 내부의 사용자는 검열망을 우회하여 목표한 웹사이트에 방문하기를 원한다. 일반적

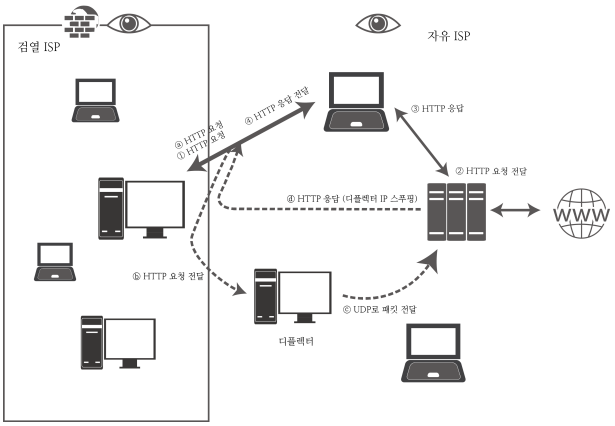


그림 1. 기본적인 구성 요소 및 연결
Fig. 1. System elements and its relationship.

으로 사용자들은 웹사이트 방문을 위한 클라이언트로 작동을 하며 서로간의 트래픽을 프록시 역할을 하는 서버로 전송한다.

디플렉터는 검열 ISP 내부의 사용자와 짝을 이루고 있지 않은 자유 ISP의 사용자로 검열 ISP에서 받은 패킷을 로우 소켓(raw socket)을 통하여 읽어 들여 UDP를 사용하여 전달하며 실질적으로 연결에 참여하지는 않는다.

서버는 자유 ISP 내부의 사용자들과 통신하며 주로 프록시로 사용된다. 디플렉터로부터 패킷을 받아 디플렉터의 주소로 소스 IP 스푸핑을 수행하여 트래픽을 전송하여 서버의 IP주소를 숨긴다. 스푸핑 가능 지역이 줄어들고 있기 때문에[17] IP 스푸핑이 불가능한 경우, 대학 등에 서버를 설치하고 내부 사용자들이 디플렉터로 동작할 수 있게 돕거나 IP 스푸핑이 불가능한 지역에서 가능한 지역으로 트래픽을 전달하는 방법 등을 대신 사용할 수 있다.

검열 ISP 안의 사용자와 자유 ISP 안의 사용자는 서로 짝이 되어서 트래픽을 프록시 역할을 하는 서버로 전달하는데 서버는 어떤 사용자들이 서로 짝을 맺고 있는지 알 수 없다. 따라서 검열 ISP의 사용자는 자유 ISP의 사용자를 통하여 차단우회 및 익명성을 획득할 수 있고 자유 ISP 안의 사용자는 검열 ISP 안의 사용자를 통하여 익명성을 획득할 수 있다.

기본 요소 간의 연결 및 동작 방식은 다음과 같다.

사용자들은 사전에 이메일 등의 외부 시스템을 이용하여 서로의 IP 주소와 포트 번호를 교환한다.

검열 ISP 안의 사용자가 먼저 자유 ISP의 사용자에

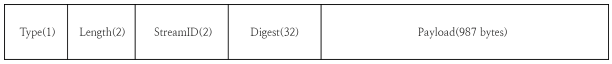


그림 2. 셀 구조
Fig. 2. Cell structure.

게 TLS 연결을 시도하여 짝을 만든다. 자유 ISP 안의 사용자는 서버와 연결을 만들고 검열 ISP 안의 사용자와의 연결과 서버와의 연결을 이어준다. 검열 ISP 내부의 사용자는 익명성을 제공하기 위해 짝이 아닌 다른 자유 ISP 안의 사용자를 디플렉터로 사용한다. 검열 ISP 내부의 사용자는 짝에게서 받은 트래픽을 디플렉터에게 전달하는데 디플렉터는 이를 로우 소켓을 사용하여 패킷 단위로 읽어와 UDP를 사용하여 트래픽을 전달하고 서버 측에서는 UDP 안의 패킷을 스푸핑하여 디플렉터에서 보내는 것처럼 만들어서 검열 ISP 안의 사용자에게 응답 트래픽을 전달한다. 검열 ISP 내부의 사용자는 자유 ISP 내부의 사용자와의 회선을 통해 전달함으로써 자유 ISP 내부의 사용자는 익명성을 획득할 수 있다. 모든 연결 안의 트래픽은 다음에 설명하는 프로토콜을 따른다.

회선 안의 서로 다른 사용자의 요청/응답 트래픽을 구분하기 위해서 그림 2와 같은 내부 프로토콜을 사용한다. 트래픽은 셀로 만들어져 이동되는데 각각의 셀의 크기는 1024 바이트로 헤더와 데이터 페이로드로 이루어져 있다. 헤더에는 4가지 종류의 필드가 존재하는데 Type은 요청/응답 트래픽, 암호화를 위한 키 교환 등 데이터의 성격에 따라 달라지며 Length는 Data의 길이, StreamID는 다중화를 위한 추가적인 정보를 기록하는데 사용되며 Digest는 SHA-2 등을 사용하여 회선의 종단 간 무결성을 보장한다. 사용자 및 서버는 각 단계마다 Digest를 확인한다.

자유 ISP 안의 사용자와 검열 ISP 안의 사용자의 TLS 연결은 두 사용자가 공유하기 때문에 셀의 Type을 사용한다. 회선의 배치로 인하여 사용자가 회선에서 수신하는 HTTP 요청은 모두 짝의 요청이기 때문에 디플렉터 혹은 서버로 회선을 따라 전달하고 회선에서 들어오는 HTTP 응답은 자신이 보낸 요청에 대한 응답이기 때문에 무결성을 검사하고 웹브라우저로 전달하면 되도록 만들어져 있다. Type은 웹 페이지 응답시간을 줄이기 위해서도 사용되는데 HTTP 응답 셀들을 처리하는 중 요청 타입의 셀이 들어오면 우선적으로 전달하여 웹 페이지 요청이 즉시 처리되도록 디자인되어있다. StreamID는 웹브라우저 HTTP 요청의 다중화에 사용되는데 웹브라우저의 HTTP 요청이 들어오는 포트 번호를 StreamID로 정하여 셀을 생성한다. 수신측에서 요청에 대한 응답을 전송할 때는 요청 트래픽의 StreamID를 맞춰 셀을 생성하여 전송한다. 이후 패킷이 목적지에 도착하면 StreamID의 포트 번호로 데이터를 전송하면 된다.

모든 사용자들은 서로 다른 ISP 안에 있는 사용자들과 여러 개의 짝을 만들어서 HTTP 요청/응답을 보냄으로 응답 시간을 줄일 수 있다.

2. 구현

본 논문에서 제안하는 시스템의 실험을 위한 구현은 리눅스 환경에서 만들어졌다.

가. 사용자

사용자들은 각각 웹 클라이언트와 디플렉터 기능을 가지고 있으며 검열 ISP 안의 사용자와 자유 ISP 안의 사용자의 구조는 비슷하다.

웹 클라이언트로서 사용자들은 프록시를 기본으로 하여 만들어졌고 웹브라우저에서 프록시를 설정함으로 손쉽게 사용이 가능하다. 구현된 프록시는 회선 생성, 관리, 다중화와 역다중화, 셀의 우선순위 등을 관리한다. 각 회선은 SSL 1.0.1g 라이브러리로 암호화 되어서 전송되며 Diffie-Hellman 키 교환방식을 사용하기 위하여 타원곡선 암호에 기반을 둔 curve25519 라이브러리를 사용하였다. 회선 관리 및 셀의 우선순위 설정을 위하여 우선순위 큐를 사용하여 사용자의 HTTP 요청이 발생하는 경우 HTTP 응답을 처리하는 도중에 즉시 요청을 처리할 수 있도록 만들었다. HTTP 요청은 라운드 로빈 방식을 사용하여 여러 개의 회선으로 분산 전송된다.

자유 ISP 안의 사용자는 디플렉터의 역할을 겸하는데 리눅스 커널의 방화벽인 IPTABLES와 로우 소켓을 이용하여 은닉 회선에서 오는 패킷을 TCP/IP 헤더까지 포함하여 읽어 온 후 UDP를 사용하여 서버의 정해진 포트로 전달한다.

나. 서버

서버는 회선 관리하는 부분과 프록시로 이루어져 있다. 회선 관리 부분은 사용자와 크게 다르지 않지만 디

플렉터로부터 오는 UDP 패킷에서 TCP/IP 패킷을 추출하여 TUN 디바이스를 통해 외부에서 오는 패킷인 것처럼 만들어 준다. 서버 자체는 리눅스의 방화벽인 IPTABLES를 설정하여 투명 프록시로 행동하도록 설정하고 IP 주소를 스푸핑하여 응답 패킷을 전송한다. 다중화 및 역다중화를 위해서 서버 측에서는 회선 및 StreamID로 이루어진 매핑 테이블을 유지한다.

프록시 서비스를 위해서는 오픈 소스 소프트웨어 프록시 서버인 Squid(Version 3.1.19)를 사용하였다. 논문의 시스템과는 개별적으로 작동하기 때문에 다른 프록시 소프트웨어를 사용하여도 무관하며 HTTPS를 지원하기 위해서 CONNECT 요청을 처리하게 설정하였다

V. 실 험

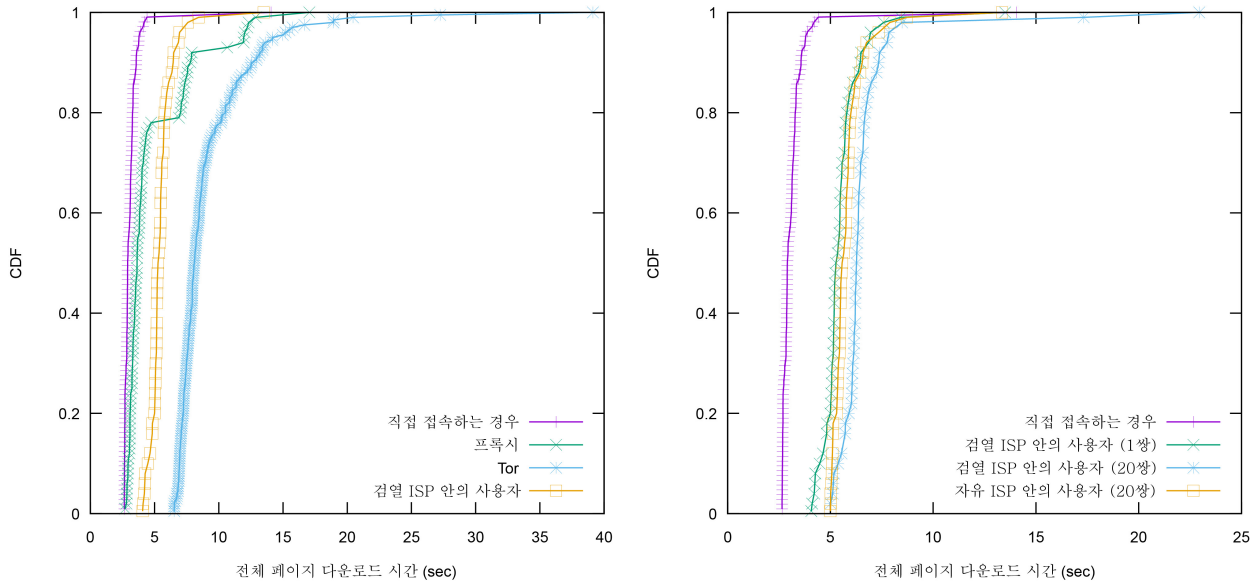
실험을 통하여 본 논문에서 제안한 시스템과 다른 우회 방법들과의 성능 비교와 시스템의 사용자 수의 증가에 따른 성능 향상에 대하여 알아보았다.

실험을 위한 설정은 다음과 같다. 서버는 미국 유타에 위치한 Emulab을 사용하였고, 2개의 자유 ISP의 사용자는 각각 유타 주와 컨터키의 Emulab을 사용하였다. 검열 ISP 안의 사용자는 중국에 위치하고 있다. 검열 ISP의 사용자는 켄터키의 사용자와 짝을 이루고 유타에 있는 사용자를 디플렉터로 사용한다. 이러한 상황에서 각각의 사용자들은 50회씩 en.wikipedia.org에 접속하여 전체 페이지(571.48 KB)를 다운로드 받는데 걸리는 시간을 측정한다.

성능을 평가하기 위한 비교대상으로는 자유무역지대인 중국 상하이에서 대상 페이지로 직접 접속하였을 때, 미국의 사설 프록시를 사용하였을 때, 미국에 있는 브릿지를 이용하여 Tor를 사용하였을 때 전체 페이지 다운로드에 걸리는 시간을 측정해보았다.

그림 3의 (a)는 다른 우회방법들과 전체 페이지를 다운로드 받는데 걸리는 시간을 비교한 것으로 한 쌍의 사용자가 동작할 때 검열 ISP 안의 사용자의 응답시간을 측정하였다. 다른 우회 기법들과 비교하여 볼 때 전체 페이지 다운로드 시간은 1~2초 내로 큰 차이를 보이지 않는다.

그림 3의 (b)는 참여 사용자 수와 종류에 따른 전체 페이지 다운로드 시간을 비교한 것이다. 검열 ISP 안의 사용자 20명이 자유 ISP 안의 사용자와 각각 짝을 이루었을 때 전체 페이지 다운로드 시간을 비교한 것으로 프록시를 사용하였을 때의 전체 페이지 다운로드 시간과 사용자의 수가 증가하였을 때의 다운로드 시간은 비슷하다. 사용자 수가 증가하여도 요청 HTTP 셀의 처리가 우선적으로 처리되기 때문에 여러 사용자과 짝을



(a) 다른 방법들과의 비교 결과 (b) 여러 사용자가 작동하는 경우의 비교

그림 3. 성능 비교
Fig. 3. Evaluation results.

맺고 있는 자유 ISP 안의 사용자와 한 사용자와 짝을 맺고 있는 검열 ISP 안의 사용자의 성능이 큰 차이가 나지 않는다.

Ⅵ. 결 론

본 논문에서는 사용자간의 상호 협력을 통하여 기존의 차단우회 및 익명성 서비스에서 어려웠던 사용자 모집을 독려하고 우회 단계를 줄여 성능을 향상시킨 차단우회 시스템을 제안하였다. 검열 ISP 내부의 사용자와 자유 ISP 안의 사용자가 익명성과 차단우회라는 필요성을 충족시키며 직접적으로 자원을 교환 할 수 있도록 만들어졌으며 사용자의 편의를 위하여 웹 브라우저에 최적화된 시스템을 디자인하였다.

REFERENCES

[1] S. Kelly, M. Earp, L. Reed, A. Shahbaz, and M. Truong. Freedom on the Net 2014. Freedom House, pp. 1-22. 2014, December.
[2] Tor Porject: Anonymity Online, https://www.torproject.org
[3] M. Graham, S.D. Sabbath. The anonymous Internet. Information Geographies at the Oxford Internet Institute, 2014
[4] P Winter, S Lindskog. How the great firewall of china is blocking tor. USENIX FOCI, pp. 1-9, Bellevue, WA.2012, August.
[5] VPN Gate, http://www.vpngate.net/en/
[6] ZenMate, https:/zenmate.com
[7] H. M. Moghaddam, B. Li, M. Derakshani, and I. Goldberg. SkypeMorph: Protocol obfuscation for Tor bridges. ACM CCS, pp. 97-108. NC, USA. 2012, October.
[8] A. Houmansadr, T. Riedl, N. Borisov, and A. Singer. I want my voice to be heard: IP over Voice-over-IP for unobservable censorship circumvention. NDSS Symposium. San Diego, CA United States. 2013, February.
[9] Q. Wang et al. Censorspoofer: Asymmetric communication using IP spoofing for censorship-resistant web browsing. ACM CCS, pp. 121-132. NC, USA. 2012, October.
[10] J. Geddes, M. Schuchard, and N. Hopper. Cover your ACKs: Pitfalls of covert channel censorship circumvention. ACM CCS, pp. 361-372. Berlin, Germany, 2013, November.
[11] E. Wustrow, S. Wolchok, I. Goldberg, and J. A. Halderman. Telex: Anticensorship in the network infrastructure. USENIX Security Symposium. San Francisco, CA. 2011, August.
[12] J. Karlin et al. Decoy routing: Toward unblockable Internet communication. USENIX FOCI. San Francisco, CA. 2011, August.
[13] A. Houmansadr et al. Cirripede: Circumvention infrastructure using router redirection with plausible deniability. ACM CCS, pp. 187-200. Chicago, IL. 2011, October.
[14] E. Androulaki, M. Raykova, S. Srivatsan, A. Stavrou, and S. M. Bellovin. PAR: Payment for anonymous routing. PETS, pp. 219-236. Leuven, Belgium. 2008, July.
[15] R. Jansen, A. Johnson, and P. Syverson. LIRA: Lightweight incentivized routing for anonymity. NDSS Symposium. San Diego, CA United States. 2013, February.
[16] R. Jansen et al. Recruiting new Tor relays with BRAIDS. ACM CCS, pp. 319-328. Chicago, IL. 2010, October.
[17] The CMAND Spoofer project. http://spoofer.cmand.org.

저 자 소 개

이 은 수(학생회원)
2014년 한양대학교 컴퓨터공학과 학사 졸업.
2014년~현재 한양대학교 컴퓨터 공학과 석사과정
<주관심분야 : 컴퓨터네트워크>

이 석 복(정회원)
2004년 홍익대학교 컴퓨터공학과 학사 졸업.
2006년 홍익대학교 컴퓨터공학과 석사 졸업.
2011년 UCLA 컴퓨터공학과 박사 취득.
<주관심분야 : 컴퓨터네트워크>