GeoIP를 이용한 익명 네트워크에서 통신 속도 향상을 위한 성능 개선

Performance Improvement for Increased Communication Speed in Anonymous Network using GeoIP

박광철(Kwang Cheol Park)*, 임영환(Young Hwan Lim)**,
임종인(Jong In Lim)***, 박원형(Won Hyung Park)****

초 록

정보통신 기술이 발달함에 따라 우리는 많은 편리함을 누리고 있다. 하지만 정보화의 뒷면에는 수많은 역기능이 나타나고 있다. 특히, 인터넷상에서의 프라이버시와 보안에 대한 요구사항이 증가함에 따라서 익명성을 보장하는 IP 은닉 네트워크 기술이 지속적으로 개발되고 있다. IP 은닉 네트워크 기술은 사용자가 정보수집 필요시 대상 사이트 차단을 우회하여 접근하기 위해 사용될 수 있으며 악의적인 해커가 자신을 은닉한 공격을 수행할 목적으로 사용 될 수도 있다. 하지만 복잡한 라우팅 경로와 지역별 통신 대역폭의 상이함, 그리고 노드간 암호화로 인해 통신속도가 현저히 떨어지는 단점 또한 존재하는 것이 사실이다. 이에 본 논문에서는 GeoIP를 이용하여 네트워크 대역폭이 높은 특정국가를 지정하거나 경로길이를 제한하는 통신속도 측정실험을 통해 익명 네트워크의 성능을 개선 한다.

ABSTRACT

Although progress in information technology has made our life prosperous. But it accompanied a number of adverse effects in various aspects. Especially, internet according to the increasing requirements for privacy and security, IP concealment network technologies to ensure the anonymity are constantly being developed. IP concealment network technologies is aiding the user to bypass the blocked sites can be used to access for information gathering, and they could be used for a malicious hacker to hide his attacks. However, due to complex routing path, local communication bandwidth sangyiham, and internode encryption there are also disadvantages that communication speed is significantly less. In this paper, the research for improving the performance of anonymous networks is to proceed by the communication speed measurement that using GeoIP the particular country with high-bandwidth is Specified or path length is limited.

키워드 : 익명 네트워크, 토어, 프락시, 국가코드
Anonymous Network, TOR, Proxy, GeoIP

---

* 고려대학교 정보보호대학원
** 서울과학기술대학교 산업정보시스템공학과 박사과정
*** 고려대학교 정보보호대학원 원장
**** 교신저자, 서울과학기술대학교 산업정보시스템공학과 겸임교수
2011년 10월 19일 접수, 2011년 10월 28일 심사완료 후 2011년 11월 10일 게재확정.

1. 서 론

인터넷에서의 개인정보보호와 기술적 보안에 대한 요구사항이 증가함에 따라서 IP 은닉 네트워크 기술이 발전하였다. IP 주소 익명화를 통하여 사용자의 IP가 아닌 다른 곳의 IP로 서비스에 접근하는 일이 많아지고 있으며 유해사이트로 네트워크 접근이 차단된 사이트를 우회 접근을 하기 위한 수단으로도 사용되거나 상대방에게 자신을 은닉한 상태로 접근하기 위해 사용되기도 한다. 특히, 서버 익명화를 통하여 누가 서비스를 제공하는지 모르는 익명 서비스를 제공하기 위해서도 사용되고 있다. 또한, IP 은닉 네트워크 기술은 정보기관이나 수사기관에서 정보수집 필요시 유해사이트 차단을 우회하여 접근하기 위해 사용될 수 있으나 악의적인 해커가 자신을 은닉한 공격을 수행하는 목적으로 사용 될 수도 있다.

이에 본 논문은 최근 해커가 가장 많이 사용되고 있는 익명 네트워크 기술에 대해 알아보고 자동화된 익명 네트워크 도구를 이용하여 통신 속도를 향상시키기 위한 기술에 관해 연구한다. 이를 통해 가장 빠른 대역폭을 가진 국가와 노드를 실험을 통해 증명하며 향후 익명 네트워크를 활용한 사이버공격 발생시 대응할 수 있는 정책・기술적 기반을 마련한다. 또한, 익명네트워크에 관한 학술적 논문뿐만 아니라 속도 측정에 관한 논문이 전무하여 이 분야에 대한 기반기술 연구를 하였다.

2. 관련 연구

2.1 익명 네트워크 기술

TOR(The Onion Router)는 1998년부터 2001년까지 미국 해군연구소(NRI : Navy Research Institute)에서 연구 개발, 관리 및 운영을 수행했으나, 2001년 이후에는 EFF(Electronic Frontier Foundation)에서 관리 및 운영을 하고 있다. TOR는 현재 1755개의 Relay Node가 운영중에 있으며 2010년에는 5000개 이상의 Relay Node 확보를 목표로 하고 있다[7].

I2P(Invisible Internet Project)는 2003년에 익명 통신을 위하여 시작된 프로젝트로서 기존의 Freenet을 수정하여 개발하였으며 TOR와 달리 일반 인터넷을 익명으로 사용하기 위하여 개발되지는 않았으며 익명으로 게시판 등의 서비스를 제공하기 위해 제작되었다.

Peer-to-Peer 방식을 이용하여 통신을 하고 Garlic Routing 방식 사용하여 Onion Routing과 달리 메시지 단위별로 암호화 하여 경로설정을 수행한다. Distributed Network Database 사용하여 중앙에 네트워크 디렉터리를 유지하지 않고 노드마다 경로 정보를 유지한다. 또한, 중앙 디렉터리 서버를 별도로 유지할 필요가 없으며 디렉터리 서버가 유출되어 익명성이 저해되는 위험을 줄일 수 있다[11].

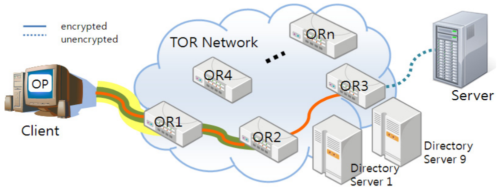
JAP(Java Anon Proxy)는 익명으로 인터넷을 사용하도록 지원하는 Java Application으로서 익명 인터넷 사용이 주목적이다. MIX 방식을 이용하여 웹 요청에 대한 익명성을 제공하며 Mix 서버는 암호화된 입력 메시지를 복호화하고 순서를 변경하여 각 Mix 서버 노드를 경유함에 따라 입력 메시지는 계층적으로 복호화 되고 임의 순서로 전달한다. 따라서 각 Mix 서버 노드는 바로 이전/다음 노드에 대한 정보만 인식이 가능한다. 몇 개의 중앙 노드가 연결 요청을 MIX 방식으로 처리하여 JAP을 실행 시키면 우선 InfoService

에 접근하여 Mix Station 정보를 얻어 온다. Mix Station은 여러 사용자로부터 받은 요청을 합하여 Middle Mix로 보내고 Middle Mix는 Last Mix로 보내고 Last Mix는 Cache-Proxy로 보내어 인터넷에 접근한다[12].

Peekabooty는 Cult of Dead Cow 해커그룹에 의해 개발되었으며 P2P 방식을 이용하는 분산된 협력적 프라이버시 네트워크로서 방화벽에 막혀 있는 사이트에 접속하는 경우 다른 컴퓨터가 대신 전달해 준다. 익명성을 제공하는 웹브라우징 도구를 사용하며 각각의 클라이언트가 프락시로 동작하는 Collaborative 통신을 수행한다[10].

2.2 익명 네트워크 동작 메커니즘

TOR 네트워크 구성은 Client, Server, Onion Router(OR), Directory Server(DS) 등으로 구성되어 있다. Client는 클라이언트 데이터의 익명화를 위해 Onion Proxy(OP) 소프트웨어를 구동한다. Server는 웹서버와 같은 TCP 응용 서버 프로그램을 실행하며 Onion Router(OR)는 클라이언트와 서버 사이의 중계 역할을 수행하는 특별 Proxy로 TOR에서는 Transport Layer Security(TLS) connection을 사용한다. Directory Server(DS)는 기본 DS로 9개(v.0.2.1.22)를 가지고 있으며 각 OR이 자신의 정보를 알리면 디렉토리 서버가 저장된다. OP는 맨 먼저 디렉토리 서버에 접근하여 OR의 정보(IP, 공개키, 정책, 대역폭, uptime 등)를 조회하게 된다. 이후 경로(path) 선택, 회선(circuit) 생성, TCP 스트림 전송 단계를 거쳐 데이터를 전송하게 된다. 아래 그림은 TOR의 전체 구성도이다.



〈그림 1〉 TOR 네트워크의 사용 화면[5]

2.3 익명 네트워크 전송 형태

전송 단위 셀(Cell) 유형은 512바이트의 셀로 처음 3바이트 헤더는 암호화하지 않고, 나머지 509바이트만 암호화한다. 셀 유형에는 Control 셀과 Relay 셀이 있으며 총 22개 유형이 존재한다. 아래 그림은 TOR의 Control 셀과 Relay 셀 형태를 나타낸다.

2	1	509
CircID	CMD	Data

〈그림 2〉 TOR(Control) 셀 포맷

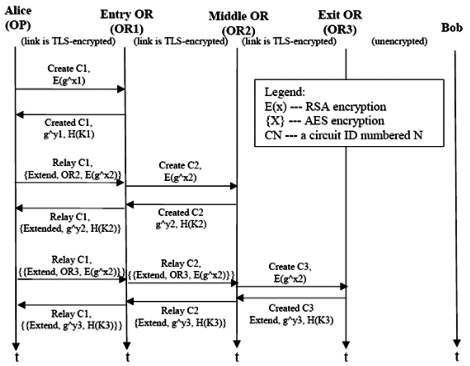
2	1	2	6	2	1	498
CircID	Relay	StreamID	Digest	Len	CMD	Data

〈그림 3〉 TOR Relay 셀 포맷

경로(path) 선택(기본 경로 길이는 3)은 디렉토리 서버에서 가져온 OR에 대한 Descriptor 정보를 이용하여 bandwidth capacity 정보를 기반으로 사용할 relay 노드(OR)를 선택하며 가장 먼저 Exit OR 노드 선택, 그 다음 Entry OR 노드 선택, 마지막으로 Intermediate OR 노드를 선택하여 결정한다.

회선(Circuit) 생성(Control 셀, Relay 셀 이용)은 링크 인증 및 암호화에 TLS/SSLv3 이용하여 세션 비밀키 협상에 Diffie-Hellman

(DH) handshake 프로토콜을 이용한다. Relay Extend 셀은 AES-CTR을 이용하여 암호화 하며 OP가 Create 셀, Relay Extend 셀을 보내 각 OR과 차례로 비밀키 협상한다. 아래 그림은 TOR의 회선 생성을 나타낸다.

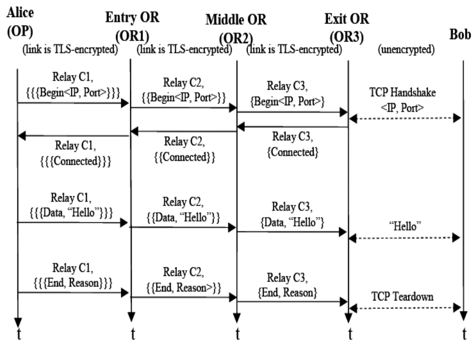


〈그림 4〉 회선(Circuit) 생성[9]

TCP 스트림 전송(relay 셀 이용)은 OP가 Exit OR에게 relay begin 셀을 전송하는 것으로 Exit OR에서 OP로 relay connected 셀을 보내 연결되었음을 알린다. 그러면 클라이언트가 서버로 Circuit을 통해 데이터 전송이 시작되며 전송이 끝나 클라이언트가 OP에게 연결을 끊을 것을 요청하면 OP가 서버에게 relay end 셀을 보내 연결 종료를 선언 한다. 아래 그림은 TOR의 TCP 스트림 전송을 나타낸다.

2.4 익명 네트워크 취약점과 전송 속도의 문제점

익명 네트워크의 취약점은 모든 클라이언트들이 모든 TOR 라우터 정보를 얻을 수 있고 여러 회선에서 들어온 셀을 라운드로빈 방식으로 내보내기 때문에 어느 특정 노드에



〈그림 5〉 TCP 스트림 전송[9]

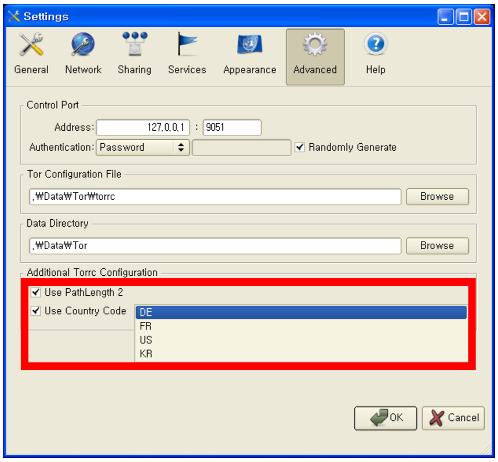
서의 로드가 많이 발생하면 다른 연결에서도 지연시간이 증가하는데 있다. 이는 악의적인 사용자가 특정 트래픽을 발생시켜 모든 TOR 노드들의 지연시간을 측정하고 특정 회선의 모든 relay 노드를 알아낼 수 있다. 또한, 디렉토리 서버가 각 TOR 노드의 정보를 체크하지 않고 저장하기 때문에 악의적인 정보를 디렉토리 서버에 보낼 수도 있고 비밀키 분배에 사용하는 Diffie-Hellman은 Man-in-the-middle-attack을 받을 가능성이 있다. 익명 네트워크의 통신속도가 느린 이유는 혼잡 제어(Congestion Control)에서 사용자가 자신이 실제 기여할 수 있는 네트워크 트래픽보다 많은 양을 설정할 수 있으며 기본적으로 모든 사용자에게 제어할만한 충분한 용량을 가지고 있지 않기 때문이다. 또한, 현재의 경로 선택 알고리즘은 로드를 분산시켜주는 기능도 없다. 클라이언트의 High/Variable Latency 또는 Connection Failure에 대한 처리 방법에 문제가 있으며 작은 대역폭을 갖는 사용자가 Directory 정보를 다운로드하는데 오버헤드가 많이 걸린다. 본 논문은 이러한 속도 저하현상을 극복하기 위해 GeoIP를 이용하여 통신 속도를 향상할 수 있는 기술에 대해 연구한다.

3. 익명 네트워크의 통신 속도 개선

3.1 통신속도 개선을 위한 UI 옵션 설정

익명 네트워크의 통신 속도 개선을 위해서는 기본적으로 대역폭이 큰 특정 국가코드를 지정하거나 경로길이 감소(3->2)시 속도 개선 효과가 발생할 것으로 가정한다. Vidalia UI에 TOR 국가코드 및 경로길이 설정 기능을 추가하여 LAN에서 TOR PC를 공유하여 사용하도록 Polipo에 프록시 외부 접근 허용 설정(polipo.conf)을 한다[4].

<그림 6>은 TOR의 Advance 옵션으로 Use PathLength 2 항목을 선택시 TOR 회선 길이 2 사용하게 되며 체크 해제시 기본 경로길이 3을 사용하게 된다. Use Country Code 항목을 선택시 특정 국가코드 지정이 가능하며 대역폭이 큰 독일(DE), 프랑스(FR), 미국(US), 한국(KR) 등의 국가코드 사용이 가능하도록 설계하였다. 선택 해제시 임의의 노드가 선택되도록 하였다.



〈그림 6〉 TOR Advance 옵션 설정 화면

3.2 익명네트워크에서 GeoIP 설정

TOR에서 GeoIP를 설정하기 위해 Data\Tor\torrc 항목을 재설정해야 한다. DataDirectory는 라우터 정보 등 TOR 실행에 필요한 데이터가 저장된다. GeoIPFile은 IP에 해당하는 국가정보가 포함된 GeoIP 파일을 지정한다. Socks-ListenAddress는 SOCKS listen 주소를 지정하며 ExcludeNodes에서는 노드 선택 시 제외할 노드를 지정 가능하다. Nickname, finger-print, 국가코드, 주소 패턴으로 설정된다. Short-Path(0|1)은 0으로 지정시 경로길이 3, 1로 지정시 경로길이 2를 사용하게 되며 기본값은 1이다. 아래 그림은 이에 대한 설정 내용이다.

```
# If non-zero, try to write to disk less frequently than we would otherwise.
AvoidDiskWrites 1
# Store working data, state, keys, and caches here.
DataDirectory .₩Data₩Tor
GeoIPFile .₩Data₩Tor₩geoip
# Where to send logging messages.  Format is minSeverity[-maxSeverity]
# (stderr|stdout|syslog|file FILENAME).
Log notice stdout
# Bind to this address to listen to connections from SOCKS-speaking
# applications.
SocksListenAddress 127.0.0.1
ControlPort 9051
ExcludeNodes {A1},{A2},{AD},{AE},{AF},{AG},{AI},{AL},{AM},{AN},{AO},{AP},{AQ},{AR},
{AS},{AT},{AU},{AW},{AX},{AZ},{BA},{BB},{BD},{BE},{BF},{BG},{BH},{BI},{BJ},{BM},{BN
},{BO},{BR},{BS},{BT},{BV},{BW},{BY},{BZ},{CA},{CD},{CF},{CG},{CH},{CI},{CK},{CL},{
CM},{CN},{CO},{CR},{CU},{CV},{CY},{CZ},{DJ},{DK},{DM},{DO},{DZ},{EC},{EE},{EG},{ER}
,{ES},{ET},{EU},{FI},{FJ},{FK},{FM},{FO},{FR},{GA},{GB},{GD},{GE},{GF},{GG},{GH},{G
I},{GL},{GM},{GN},{GP},{GQ},{GR},{GT},{GU},{GW},{GY},{HK},{HN},{HR},{HT},{HU},{ID},
{IE},{IL},{IM},{IN},{IO},{IQ},{IR},{IS},{IT},{JE},{JM},{JO},{JP},{KE},{KG},{KH},{KI
},{KM},{KN},{KP},{KR},{KW},{KY},{KZ},{LA},{LB},{LC},{LI},{LK},{LR},{LS},{LT},{LU},{
LV},{LY},{MA},{MC},{MD},{ME},{MF},{MG},{MH},{MK},{ML},{MM},{MN},{MO},{MP},{MQ},{MR}
,{MS},{MT},{MU},{MV},{MW},{MX},{MY},{MZ},{NA},{NC},{NE},{NF},{NG},{NI},{NL},{NO},{N
P},{NR},{NU},{NZ},{OM},{PA},{PE},{PF},{PG},{PH},{PK},{PL},{PM},{PN},{PR},{PS},{PT},
{PW},{PY},{QA},{RE},{RO},{RS},{RU},{RW},{SA},{SB},{SC},{SD},{SE},{SG},{SI},{SK},{SL
},{SM},{SN},{SO},{SR},{ST},{SV},{SY},{SZ},{TC},{TD},{TG},{TH},{TJ},{TK},{TL},{TM},{
TN},{TO},{TR},{TT},{TV},{TW},{TZ},{UA},{UG},{UM},{US},{UY},{UZ},{VA},{VC},{VE},{VG}
,{VI},{VN},{VU},{WF},{WS},{YE},{YT},{ZA},{ZM},{ZW},{??}
HashedControlPassword 16:139005DE5C18061660C5602D65CE3F230EE0F39D596E46E9A17304C247
```

〈그림 7〉 TOR의 동작 1단계

3.3 익명 네트워크에서 프락시 설정

웹프록시 캐쉬로 파이어폭스 브라우저에서 설정할 수 있는 Polipo를 이용하여 설정한다. proxyAddress 항목은 polipo가 listen할 IP로 지정한다. “0.0.0.0”으로 지정할 경우 IPv4를 사용하는 모든 외부 클라이언트에게 서비스 제공이 가능하다. “::”으로 지정하게 되며 IPv4, IPv6를 모두 지원 받을 수 있다. allowedClients 항목은 polipo에 접근가능한 IP Address 지정하게 된다.

```
### Basic configuration
### ******************

# Uncomment one of these if you want to allow remote clients to
# connect:

# proxyAddress = "::0"        # both IPv4 and IPv6
proxyAddress = "0.0.0.0"    # IPv4 only

#proxyAddress = "127.0.0.1"
proxyPort = 8118

# If you do that, you'll want to restrict the set of hosts allowed to
# connect:

# allowedClients = "127.0.0.1, 134.157.168.57"
# allowedClients = "127.0.0.1, 134.157.168.0/24"

#allowedClients = 127.0.0.1
allowedPorts = 1-65535

# Uncomment this if you want your Polipo to identify itself by
# something else than the host name:

proxyName = "localhost"

# Uncomment this if there's only one user using this instance of Polipo:

cacheIsShared = false

# Uncomment this if you want to use a parent proxy:

# parentProxy = "squid.example.org:3128"

# Uncomment this if you want to use a parent SOCKS proxy:

socksParentProxy = "localhost:9050"
socksProxyType = socks5
```

〈그림 8〉 TOR의 동작 1단계

4. GeoIP를 이용한 통신 속도 개선 실험 평가

4.1 통신속도 개선을 위한 실험 개요

통신 속도 개선을 위한 실험 전 제약조건으로 전 세계 50여 개국 1,600여 개 TOR 노드를 이용하여 회선을 구성하고 현재 경로 길이 3을 사용하므로 최대 3개 국가를 거쳐 서버에 접속한다. 또한, GeoIP 정보를 통해 각 TOR 라우터의 국가정보 이용이 가능하며 동일 국가 내의 TOR 라우터들로 생성된 경로 사용 시 최대 3개 국가에 위치한 라우터들로 연결된 경로보다 통신 속도가 빠를 것으로 가정한다. 통신속도 개선 실험을 위해 TOR를 사용하도록 설정된 웹프록시를 환경변수로 지정하고 wget 프로그램[8]으로 여러 국가에 위치한 서버에서 다양한 크기의 데이터 다운로드 시 소요되는 시간을 측정한 후 데이터 1KB 다운로드 시 소요되는 평균시간과 비교한다. 이에 대한 전제조건으로 제공된 GeoIP의 IP에 해당하는 국가정보가 정확해야 하며 TOR 회선의 안정성을 위해 라우터가 많고 안정적인 국가를 선택 한다.

4.2 통신속도 개선을 위한 실험 테스트 환경

실험 환경은 Intel Core i7 CPU 860 2.80 GHz 3GBRAM PC와 리눅스 가상머신(VM ware, Fedora 10, 리눅스 2.6.27.41), TOR 버전 0.2.1.22, Polipo(웹프록시)를 설치하고 GeoIP 파일을 최신 정보로 업데이트 한다. 아래 <표 1>는 실험에 국가별 TOR 노드 수를 나타낸다.

〈표 1〉 국가별 TOR 노드 수[6]

전체	독일	프랑스	미국	네덜란드
1337	310	105	376	52

실험에 사용되는 국가는 TOR의 안정적인 회선 연결을 위해 라우터들이 많고 비교적 대역폭이 큰 라우터를 보유한 나라로 선정하며 국가코드를 0개~4개까지 실험 한다. 즉, 모든 국가 선택, 독일(DE), 프랑스(FR), 미국(US), 네덜란드(NL) 순으로 정의한다. 국가코드 조합은 TOR 라우터 미사용, TOR 라우

터 사용(ExcludeNodes 옵션이용)으로 한정되며 경로 길이는 3(기본값)과 2로 제한한다.

4.3 통신 속도 개선을 위한 실험 결과

TOR 선호국가에 따른 경로길이 대비 전송속도 실측값은 아래 <표 2>~<표 5>와 같다.

선호국가 미지정 시보다 한 개의 국가 지정 시 속도 개선효과 크다는 결론을 얻었다. 또한 경로길이가 3일 때보다 2일 때 대체로 속도 빠르지만 속도편차 존재한다는 사실을 알았다. 그리고 선호국가 미지정 시 속도가 빠른 경우 한 나라나 두 나라의 노드들로 경로가 구성되었다. 한국 서버에 경로길이가 3일 경우 대역폭이 큰 독일을 지정하여 TOR

〈표 2〉 한국 서버 전송속도

(단위: 초/KB)

경로길이 \ 선호국가	미지정	독일	프랑스	미국	네덜란드
3	0.0589094	**0.0506907**	0.0552534	0.0650392	0.0547576
2	0.0479672	0.0492486	0.0559484	0.0624355	**0.0388782**

〈표 3〉 일본 서버 전송속도

(단위: 초/KB)

경로길이 \ 선호국가	미지정	독일	프랑스	미국	네덜란드
3	0.046176	0.062989	0.133584	0.0629007	**0.040738**
2	0.0399041	**0.0311114**	0.0485771	0.0555746	0.0352321

〈표 4〉 미국 서버 전송속도

(단위: 초/KB)

경로길이 \ 선호국가	미지정	독일	프랑스	미국	네덜란드
3	0.0960105	**0.0715824**	0.0772194	0.120846	0.0841451
2	0.0588928	0.0535885	0.0957562	0.255869	**0.0502536**

〈표 5〉 중국 서버 전송속도

(단위: 초/KB)

경로길이 \ 선호국가	미지정	독일	프랑스	미국	네덜란드
3	0.0825214	**0.0412764**	0.0780305	0.0940780	0.0708755
2	**0.0561438**	0.0592831	0.0954539	0.0696852	0.0597585

사용 시 기본 TOR보다 24%, 경로길이가 2인 경우 네덜란드 국가 지정하여 TOR 사용 시 기존보다 44% 속도개선 효과가 있었다. 물론 각 서버에 따라 전송속도에 차이는 있었으나 노드의 거리보다는 대역폭이 높을수록 속도가 빠르다는 결론을 얻을 수 있었다.

4.4 통신 속도 개선을 위한 실험 평가

다음은 실험결과를 평가하기 위한 통계적 기반의 가설검증이다. 세 개 이상의 평균을 비교하는 방법으로 먼저 가설을 세운다.

귀무가설(H_0) : $\mu_1 = \mu_2 = \mu_3 = \mu_4 = \mu_5$

대립가설(H_1) : not H_0(모든 집단의 평균이 모두 같지는 않을 것이다. 비교하려고 하는 그룹이 $A_1, A_2, \cdots, A_k$이고, 각 그룹의 자료 수가 n_i라고 가정하면,

$$y_{ij},\ i = 1, 2, \cdots, k,\ j = 1, 2, \cdots, n_i$$

$\overline{y}$: 전체 평균

$\overline{y_i}$: i집단의 평균

각 자료의 편차를 다음과 같이 분리해 보면,

$$y_{ij} - \overline{y} = (y_{ij} - \overline{y_i}) + (\overline{y_i} - \overline{y}) \qquad (1)$$

식 (1)로부터 모든 자료의 편차 제곱의 합을 다음과 같이 분리할 수 있다.

$$\sum_{i=1}^{k}\sum_{j=1}^{n_i}(y_{ij} - \overline{y})^2 = \sum_{i=1}^{k}\sum_{j=1}^{n_i}(y_{ij} - \overline{y})^2 + \sum_{i=1}^{k}\sum_{j=1}^{n_i}(\overline{y_i} - \overline{y})^2 \qquad (2)$$

SST = SSE + SSA

여기서 SST(Total Sum of Squares)는 각 자료값과 전체 평균과의 편차의 제곱을 한한 것으로 집단으로 나누지 않고 구한 총변동의 합이다.

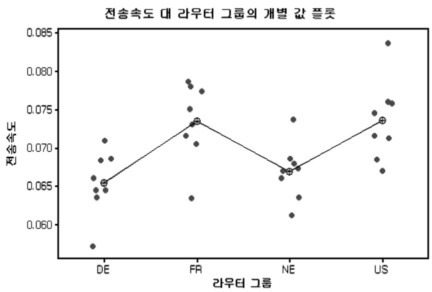
SSE(Error Sum of Squares)는 각 자료가 속한 집단의 평균과의 편차의 제곱을 합한 것으로 동일 집단 내에서의 편차의 제곱합이고, SSA(Among Treatments Sum of Squares)는 각 집단의 평균과 전체 평균과의 편차의 제곱을 합한 것으로 집단 간의 편차의 제곱합이다. 그리고 이때 각 집단에서의 분산(오차분산)은 동일의 오차분산이 동일하다는 가정이 기각되면 변수변화(주로 Log변화를 사용) 등을 통해 오차분산이 같도록 해주어야 한다. 그리고 Log변환을 해도 오차분산의 동일성 가정이 만족되지 않으면 Brown Forsythe나 Welch 등이 개발한 방법을 사용하거나 비모수적 방법으로 분석 한다.

이제 각각의 제곱합을 자유도로 나눈 집단 간 평균제곱(집단 간 분산)이 집단 내 평균제곱(집단 내 분산)에 비해 충분히 크다면 집단 간 평균차이가 의미가 있다고 결론을 내리게 된다. 반면에 집단 간 평균제곱이 집단 내 제곱변동과 비슷하거나 작으면 집간 간 평균차이는 의미가 없다는 결론을 내린다.

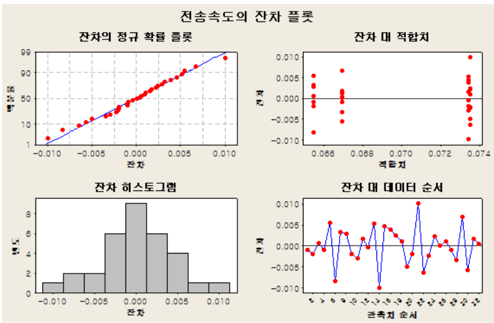
아래 <표 6>는 라우터 그룹에 따른 전송속도 자료의 분산분석표 이다. 분산 분석표에 따르면 자료의 F비는 6.895로 집단 간 평균제곱(집단 간 분산)이 집단 내 평균제곱(집단 내 분산)에 비해 6.895배이다. 그런데 자유도가 각각 3과 28인 경우 귀무가설이 참일 때 상위 5%에 해당하는 F값은 2.946으로 자료로부터 구한 값은 기준치 2.946보다 훨씬 크므로 귀무가설(그룹에 따라 전송속도에 차이가 없다)이 참이라면 우리 자료에서 관찰된 것

과 같은 차이가 나올 가능성이 0.001(유의확률, $P(F > 6.895|H_0$이 참)으로 우연히 나오기에는 너무나 큰 차이이다.

따라서 그룹 간 평균차이가 없다는 귀무가설을 기각하고 대립가설을 받아들여 그룹 간 차이가 통계적으로 유의하다는 결론을 내린다. 즉 전속속도에 따른 라우터는 통계적으로 유의한 차이를 보인다. <그림 9>를 보면, DE 라우터 그룹의 평균전송속도가 가장 낮은 것으로 나타났다.



〈그림 9〉 전송속도 대 라우터간 개별값 플롯



〈그림 10〉 전송속도의 잔차 플롯

즉, 경로길이대비 전송속도가 가장 낮으므로 독일 라우터의 속도가 가장 빠르다는 것을 알 수 있다.

5. 결 론

본 논문에서 제안한 실험방법을 통해 얻어진 결과는 대역폭인 높은 국가를 지정 시 노드가 많고 안정적인 국가를 선택할 필요가 있다. 또한 경로길이를 2로 변경하기 위해서는 소스 변경 필요했다. 노드 개수만큼 전송데이터에 암호화가 이루어지므로 경로길이 감소 시 익명성 보장 감소하는 단점이 있을 것으로 보인다. 국가코드 지정은 별도의 프로그램을 구현하여 TOR 설정이 가능 하였으며 실험결과 가장 속도를 빠르게 하기 위해서 상위 대역폭 노드를 다량 보유한 독일 국가를 지정하는 것이 가장 좋은 결과를 보였다. 본 연구는 해커의 측면에서 해킹을 위한 속도 개선에 관한 연구가 아닌 보안의 측면에서 독일과 같이 대역폭이 높은 노드에 대한 보안관제를 위한 선행연구 이다. 또한, 향후 TOR와 같은 익명 네트워크를 이용한 사이버 공격이 점차 늘어날 것으로 예상되며 이러한 공격을 탐지하고 차단하기 위해서 익명 네트워크에 대한 지속적인 정책적·기술적 연구가 활발히 진행 되어야 한다.

〈표 6〉 전송속도 자료의 분산분석표

변동인자	제곱합	자유도	평균제곱	F 비	P-값	F 기각치
처리	0.0004342	3	0.000145	6.895305578	0.001277	2.946685
잔차	0.0005878	28	2.1E-05	-	-	-
계	0.001022	31	-	-	-	-

참 고 문 헌

[1] Martin Suess, "Breaking TOR Anonymity," http://www.csnc.ch/misc/files/publications/the_onion_router_v1.1.pdf, 2008.

[2] Steven, J. Murdoch, "Tor : Anonymous Internet Communication System," University of Cambridge, Computer Laboratory, 2006.

[3] Timothy, G. et al., "Browser-Based Attacks on Tor," http://web.mit.edu/tabbott/www/papers/tor.pdf, 2007.

[4] Bauer et al., "Low-Resource Routing Attacks Against Tor," WPES 2007, pp. 11-20, New York, 2007.

[5] Invisible Internet Project, http://www.i2p2.de.

[6] K. W. J. et al., "Egregious use of Tor servers?," RechtenForum, 2007.

[7] Maxmind GeoIP, http://www.maxmind.com.

[8] Mike Perry, "TorFlow, Tor Network Analysis," In HotPETs 2009, p. 14, 2009.

[9] Steven, J. and Murdoch et al., "Low-Cost Traffic Analysis of Tor," IEEE Symposium on Security and Privacy, 2007.

[10] Tor Network Status, http://torstatus.blutmagie.de.

[11] Tor project, http://www.torproject.org.

[12] Tor Status, http://torstatus.kgprog.com.

저 자 소 개

박광철 (E-mail : muryo@naver.com)
2002년~2005년 고려대학교 정보보호대학원 석사과정 졸업 (정보보호 전공)
2007년~현재 고려대학교 정보보호대학원 박사과정 수료 (정보보호 전공)
관심분야 보안관제, 보안정책, 침해사고대응

임영환 (E-mail : yhlim@seoultech.ac.kr)
2008년 서울과학기술대학교 산업대학교 정보산업공학과 (공학석사)
현재 서울과학기술대학교 IT정책전문대학원 산업정보시스템전공 (박사과정)
관심분야 융합보안, 네트워크보안, 디지털포렌식

임종인 (E-mail : jilim@korea.ac.kr)
1986년 고려대학교 대학원 수학과 박사 (암호학)
현재 고려대학교 정보보호대학원 원장
대검찰청 디지털수사자문위원회 위원장
금융보안연구원 보안전문기술 위원회 위원장
행정안전부 정책자문위원회 위원
한국저작권위원회 위원 등
관심분야 보안정책, 사이버보안, 정보보호

박원형 (E-mail : infosecure@seoultech.ac.kr)
2009년 경기대학교 정보보호학과 (이학박사)
2010년 서울과학기술대학교 산업정보시스템공학과 겸임교수
관심분야 보안관제, 융합보안, 윈도우포렌식