BGP SYN Attack 차단을 위한 개선된 BGP TCP 제안

박명종*, 이희조**
*고려대학교 컴퓨터정보통신대학원
**고려대학교 컴퓨터.통신공학부
e-mail : zzong@korea.ac.kr,

Improved BGP TCP proposals for BGP SYN Attack defeating

Myoung-Jong Park*, Hee-Jo Lee*
*Dept. of , Korea University
**Dept. of Computer Science & Engineering, Korea University

요 약

RFC 4271 에 규정되어 있는 BGP 는 대규모네트워크 망에서 효과적인 라우팅 정보전달을 위해 사용되어지는 프로토콜이다. 이러한 BGP 는 TCP Port 179 번을 사용함에 따라 TCP/IP 가 가지고 있는 보안위협에 노출되어 있다. BGP 보안 위협은 AS-PATH 공격, IP Hijacking 공격, BGP Neighbor 공격으로 라우터 자체의 보안설정으로 대부분 방어가 가능하나 BGP SYN Attack 에 대해서는 취약하다. BGP SYN Attack 은 호스트나 서버가 아닌 BGP 를 사용하는 라우터를 직접 공격하여 라우터의 TCP 나 BGP 관련 리소스를 고갈시켜 정상적인 기존 BGP 세션을 단절시키거나 새로운 BGP 세션 연결을 방해하여 결국 BGP 라우팅 정보를 교란하여 네트워크를 마비시킬 수 있다. 본 논문에서는 이러한 BGP SYN Attack 에 차단하기 위하여 이웃라우터간 안정적인 BGP 연결을 위해 설정한 BGP Neighbor Password 를 Key 로 활용한 개선된 BGP TCP 구조를 제안한다

1. 서론

정보통신 기술의 발전으로 인터넷사용이 폭발적으로 증가하였으며, 이러한 인터넷상에서 정보의 전달을 책임지는 네트워크를 구성하고 있는 장비를 라우터라 하고, 라우터간 정보를 전달하는 프로토콜을 라우팅 프로토콜이라 한다 이중 BGP(Border Gateway Protocol) 프로토콜은 대규모 네트워크의 라우팅정보를 전달하는 효과적인 프로토콜로 사용되어지고 있다[4][5]. BGP 는 RFC 4271 에 규정되어 있는 TCP/IP 네트워크상에서 라우터들이 경로정보를 교환하기 위한 프로토콜로 현재 BGPv4 (version 4)가 사용되어지고 있다[1]. BGP 는 TCP 포트 179 번을 이용해 이웃라우터간 라우팅 정보교환을 위한 통신이 이루어짐으로 인해 TCP/IP 가 가지고 있는 위험에 노출되어 있다. 그러나, 현재까지 DRDoS (Distribute Reflection Denial of Service)[2][3] 공격과 같이 악의적인 공격이 이루어지지 않고 있음으로 BGP 의 문제점을 크게 인식하고 못하고 있다.

본 논문에서는 BGP 프로토콜의 보안위협을 살펴보고, BGP 프로토콜 TCP Port 179 번을 대상으로하는 BGP TCP SYN Attack 이 라우터에 미치는 영향과 해결방안을 제시하고자 한다.

2. BGP 보안위협

BGP(Border Gateway Protocol)는 IETF “Standard Inter-domain routing protocol 이다. 현재 사용되어지고 있는 BGP 는 RFC 4271 에 규정된 프로토콜로 BGP 는 Policy Routing 프토토콜로써 네트워크 관리자가 최적의 경로를 설정해 주어야 한다. BGP 는 독자적인 경로 설정을 위해 AS(Autonomous System)을 사용하며, TCP 포트 179 번을 사용하여 BGP 라우터간의 라우팅 정보를 교환하기 위한 물리적, 논리적 연결인 네이버관계를 형성한다. 또한 Keepalive Message 를 통해 BGP Session 을 유지하며 네트워크 변화가 있을 때만 라우팅정보를 업데이트 한다[2]. 이러한 BGP 의 보안위협으로는 AS-PATH, IP Hijacking, BGP Neighbor 공격이 있다[4][5][6][7][8].

2.1 AS-PATH 공격

AS 는 Single Technical Adminitration 에 속한 Network Aggregation 이다.[2]. BGP 에서 PATH 는 AS-PATH 를 의미하며, 목적지 네트워크까지 정보를 전송하기 위해 어떤 경로로 전송할 수 있는지 의미한다. BGP 는 네트워크 변화가 발생했을 때만 라우팅 업데이트가 이루어지며, 네트워크 정보를 전송할 때 자신의 AS 번호를 붙여서 전송하게 된다. 이러한 AS 번호는 자신의 존재뿐만 아니라 라우팅 루프가 발생되지 않도록 하기 위한 것이지만 이런 취약점을 이용하여 공격을 시도하게 된다. 즉 공격자가 BGP 메시지를 위.변조하여 공격할 수 있으며, BGP AS 번호가 위조된 것을 라우터에서 확인할 수 없다[4][5][6].

2.2 IP Hijacking 공격

IP 는 인터넷상에서 한 시스템에서 다른 시스템으로 정보를 전송하고자 할 때 사용되어지는 프로토콜로 인터넷상에서 동일한 IP 주소를 사용할 경우 충돌이 발생한다. BGP 에서는 AS 간 상호연결을 통해 IP 주소를 서로 교환한다. 그러나, BGP 는 인접한 라우터로부터 수신한 정보가 잘못된 정보인지 확인할 수 없으며 수신한 네트워크 정보를 그대로 다른 BGP 네이버 라우터로 전송한다. 결과적으로 IP 주소를 속여 마치 자신이 사용하고 있는 것처럼 공격한다. 이러한 공격행위를 IP Hijacking 이라 한다[4][5][6][8].

2.3 BGP Neighbor 공격

BGP 는 네이버 관계가 형성된 후 네이버 라우터를 통해 다른 네트워크의 정보를 수신하게 된다. 이러한 BGP 는 보다 안정적으로 BGP 세션이 이루어지기 위해 TCP Port 179 번을 이용해 네이버 관계를 형성한다. 또한 네이버 형성시 안정한 세션을 성립하고자 네이버 패스워드를 설정할 수 있다. 이러한 네이버 패스워드를 설정하지 않을 경우 TCP Reset 공격대상이 될 수 있다. 이렇듯 BGP 는 TCP 프로토콜 방식을 사용함으로 네이버형성의 안정성을 확보 할 수 있지만, TCP 프로토콜의 모든 공격의 대상이 된다[4][5][6][7].

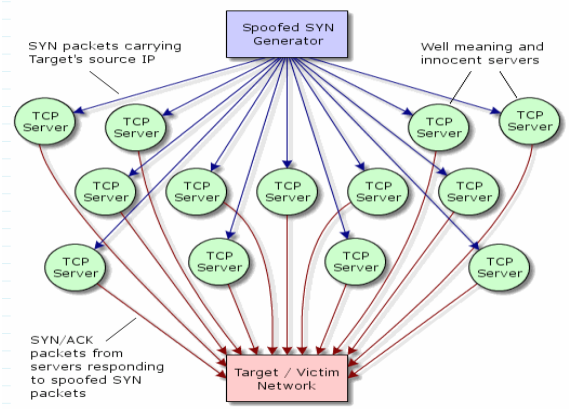
3. BGP TCP 공격의 위험과 개선된 TCP 구조

BGP 프로토콜을 대상으로하는 공격은 라우터에 영향을 주어 인터넷서비스가 단절되는 결과로 나타난다. 이러한 상기 2 항의 BGP 프로토콜의 보안 위협은 대부분 네트워크 관리자의 실수로 인해 발생하는 문제점으로 나타났다. 2003 년 국내 모 대학교에서 BGP 를 이용해 ISP 와 연동시 관리자의 실수로 ISP 망에 장애가 발생하는 사고[5][9], 2008 년 파키스탄에서의 유투브 AS-Path 오류 등을 들 수 있다.[15] 대부분의 BGP 라우터의 보안위협은 ACL(Access List), Neighbor 보안설정(MD5), uRPF(unicast Reverse Path Forwarding), PBR(Policy Base Routing) 등의 라우터 보안기능을 사용하여 취약점을 개선할 수 있다.[12][13][14] 그러나, DDoS 공격에 네트워크 망 시스템이 대상이 되어 BGP 프로토콜을 대상으로 한 TCP SYN Attack 은 심각한 위협이 되고 있다. 실제로 BGP TCP 취약점을 대상으로 DRDoS 공격이 있었다[2][3].

3.1 DRDoS ((Distribute Reflection Denial of Service)

DRDoS 는 Source IP spoofing 으로 공격자 추적불가와 봇 감염 불필요, 경유지의 서버목록 활용의 특징을 가지고 있으며, 공격의 형태는 (그림 1) 같다.

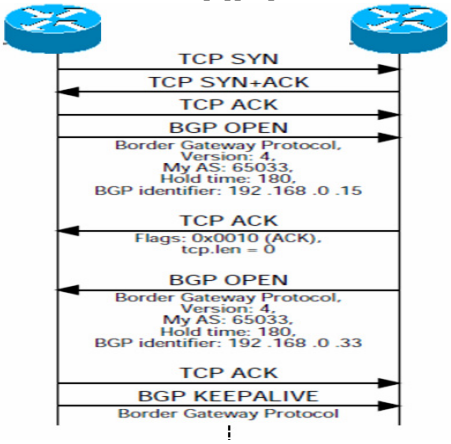
공격은 TCP/IP 의 취약점을 이용하며, Source IP 에 대한 변조, 경유지 서버에서는 아무런 의심 없이 변조된 IP 와 Port 로 TCP SYN Attack 이 시작된다. Victim 은 대량의 SYN/ACK 패킷에 의한 자원의 고갈이 발생하고, 경유지에서는 SYN/ACK 에 대한 ACK 패킷을 받지 못하면서 재전송이 발생하는 공격의 형태이다. 이러한 DRDoS 공격이 ISP 의 네트워크망의 BGP 라우터를 대상으로 발생할 경우 전체 네트워크망을 마비시킬 수 있는 파급력있는 공격의 형태이다[2][3].



(그림 1) DRDoS 공격 형태

3.2 기존 BGP TCP SYN Flood 방어기법

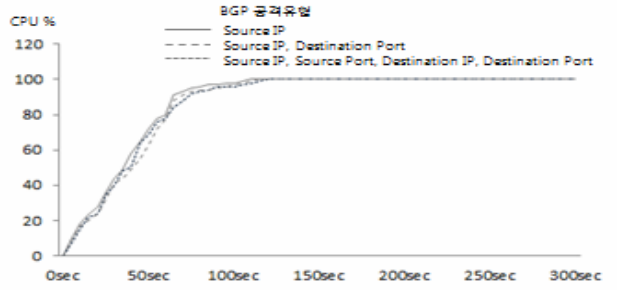
SYN Flood Attack 은 탐지가 어렵기 때문에 공격으로부터 완전히 해방되는 방법은 없다[10]. 이러한 이유는 SYN Flood Attack 은 RFC 793 에 정의되어있는 TCP 의 연결 설정 과정을 준수하는 형식을 이용하고 있기 때문이다. BGP 는 TCP 를 사용하여 Session 을 맺기 때문에 SYN Flood Attack 의 대상이 된다. (그림 2)은 BGP 3-Way Handshake 를 보여준다[3][11].



(그림 2) BGP Neighbor 3-Way Handshake

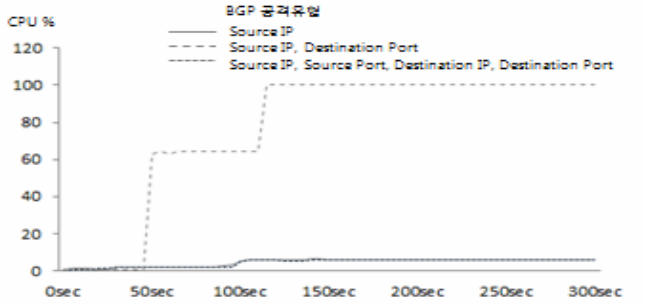
TCP 3-Way Handshake 의 취약점은 SYN_RCVD 상태에서 연결 상태를 큐에 저장하는데 있다. 큐는 메모리에 할당되기 때문에 크기에 한계를 가지고 있고 큐가 가득찬 상태에서는 더 이상의 접속요청을 처리할 수 없다. 이러한 큐는 상대방에서 ACK 패킷을 보내오거나 타임아웃이 발생하여 큐의 엔트리가 제거되어 큐에 빈자리가 생길 때까지 이후의 연결 요청은 받아들여지지 않게 된다[9][10]. 이렇게 TCP 백로그 큐의 크기보다 훨씬 많은 수의 연결요청에 응답하지 못하고 시스템은 다운되어 정상적인 서비스가 불가능해진다. (그림 3)은 라우터 BGP 179 번 포트를 대상으로 이웃라우터의 IP 로 위조하여 SYN Attack 을 가했을 때의 CPU 상태를 나타낸다.

라우터에서 BGP SYN Attack 으로부터 시스템을 보호하기 위해서 Access-list, Rate limit 와 같은 보안기능을



(그림 3) BGP default 설정상태에서 BGP SYN Attack 시 라우터 CPU 상태

이용하여 대응할 수 있다[13]. 그러나, Source IP, Destinatio IP, Port 가 일치하는 공격의 형태는 이웃라우터부터 BGP Neighbor 연결을 위한 정상적 패킷형태이기 때문에 라우터는 ACLs(access-list)와 같은 전통적 보안 기능으로는 차단할 수 없다. 최근에는 라우터가 별도의 설정없이 Session Level 에서 관리하며, 비정상적인 패킷에 대해 Rate limiting 하여 기존 세션을 보호하거나 피해를 최소화 하는 기능의 라우터가 출시되기도 하였다[12]. 이러한 보안기능에 의해 대부분의 공격에는 대응하였지만, (그림 4)에서 알 수 있듯이 IP 와 Port 에 일치한 공격에 대해서는 여전히 취약하다.



(그림 4) [12]의 보안기능 동작상태에서 BGP SYN Attack 시 라우터 CPU 상태

네트워크망에서 이웃 라우터간 BGP Neighbor IP 와 Port 에 일치한 DRDoS 형태의 BGP SYN Attack 이 발생한다면 라우터는 CPU 자원을 소모하여 BGP 다운 등 BGP 라우팅 정보를 교란시켜 네트워크에 심각한 영향을 주게된다. 본 논문에서는 이러한 BGP SYN Attack 에 차단하기 위하여 이웃라우터간 안정적인 BGP 연결을 위해 설정한 BGP Neighbor Password 를 Key 로 활용한 개선된 BGP TCP 구조를 제안한다

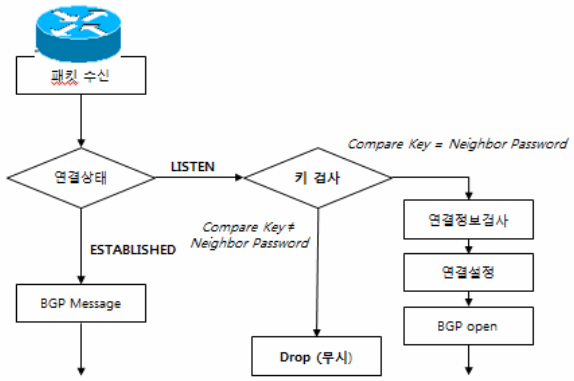
3.3 BGP TCP SYN Fool 공격을 차단하는 TCP 구조

[10]에서 Park 은 SYN Attack 을 차단하기 위해서는 TCP 연결 설정 과정의 취약점을 해결해야 하며 다음의 조건을 만족해야 한다고 제시하고 있다.

○ 서버는 클라이언트의 요청을 받은 후 응답을 보내고 그것에 대한 상태를 유지하지 않는다.

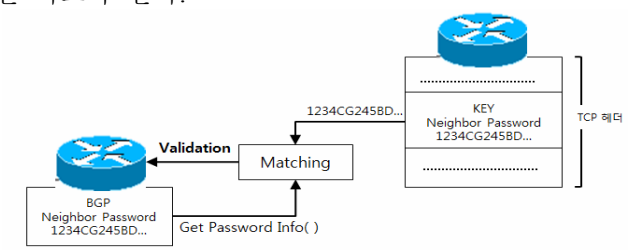
○ ACK 를 보낸 클라이언트가 연결 요청을 보낸 클라이언트임을 확신할 수 있어야 한다.

[10]에서 Park 은 확장 TCP 를 제안하였다. 확장 TCP 는 서버에서 생성한 비밀 키 값을 사용하며, TCP 연결설정 과정에서 연결정보를 유지하지 않기 때문에 SYN_RECEIVED 상태가 없다. [10]의 확장 TCP 는 클라이언트로 부터의 연결요청에 대해 서버가 항상 키 값을 생성하고, 응답이 온 패킷에 대한 검사를 하여야 하는 단점이 있다. 본 논문에서 제안한 개선된 TCP 는 [10]에서 Park 이 제시한 조건을 만족하며, 클라이언트 즉 라우터에서 이웃라우터로 BGP TCP 연결요청시 라우터는 요청된 패킷에서 키를 확인하고 확인된 연결에 대해서만 응답하도록 한다. 이때 사용되어지는 키는 BGP Neighbor Password 를 사용한다. BGP Neighbor Password 는 네이버쉽을 형성하는 과정에서 BGP 의 보안위협을 차단하기 위해 설정하는 것으로 MD5 로 해싱되어 라우터에 저장되며, 최근에는 모든 BGP 라우터에 적용되고 있다[1]. 라우터에 설정되어 있는 해싱된 Password 를 Key 로 사용함으로 Key 관리/교환을 위한 별도의 시스템이 필요하지 않다. (그림 5)은 개선된 BGP TCP handshake 과정을 보여준다.



(그림 5) 개선된 BGP TCP 3-Way Handshake 과정

(그림 6)과 같이 라우터에서 BGP Neighbor 설정을 위한 TCP 연결요청시 flag=SYN, Key(설정된 Neighbor Password 삽입) 로 키 연결요청 패킷을 송신하고, 이웃라우터는 자신에게 설정되어 있는 키(Neighbor Password)와 비교하여 일치하면 flag=SYN_ACK, Key 를 송신하고 그렇지 않은 경우 Drop 한다. 키는 TCP 헤드 옵션의 사용되지 않고 있는 Reserve 영역에 추가되어 송신 되도록 한다.

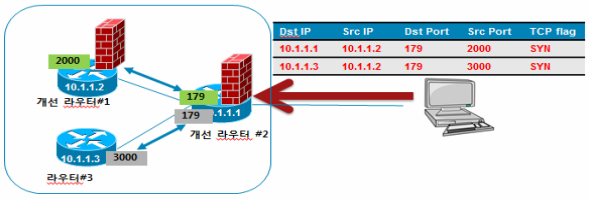


(그림 6) BGP Neighbor Password 를 사용한 KEY 확인

본 논문에서는 BGP 를 운용하는 라우터의 사용하는 라우터에는 필수사항으로 BGP Neighbor 패스워드가 설정하여야 한다. 설정된 패스워드는 BGP TCP 패킷을 송신할 때 TCP 헤더 영역에 추가되어 송신되고, 수신측에서는 설정된 패스워드 정보와 수신된 키를 비교하는 것으로 사용되어진다. 이러한 과정을 통하여 BGP SYN Attack 을 차단한다.

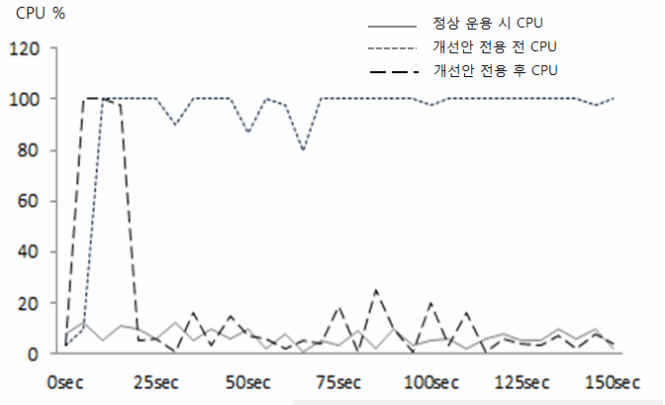
4. 성능평가

본 논문에서 개선된 BGP TCP 성능을 측정하기 위하여 Windows 시스템내 가상 라우터를 구현하였으며, TCP SYN Attack 에 대한 성능시험 하였다. 라우터에 설정되는 것과 같은 BGP Neighbor 패스워드를 가상의 라우터에 설정하여 Key 로 사용되도록 하였다. 라우터는 다수의 이웃라우터로 요청을 동시에 처리할 수 있도록 하였으며, 100Mbps 네트워크 대역폭으로, CPU 모니터는 Window 의 성능모니터로 측정하였다. 실험환경 구성은 (그림 7)와 같다.



(그림 7) 가상라우터 실험 환경 구성도

본 시뮬레이션은 일반적인 BGP TCP 연결과정의 가상의 라우터와 개선된 TCP 연결과정의 가상의 라우터를 비교하여 가상의 라우터 CPU 자원에 미치는 영향을 비교하였다.



(그림 8) BGP SYN Attack 에 의한 CPU 변화율

(그림 8)은 일반적인 운용 상황과 BGP TCP SYN Attack 이 발생하였을 때 CPU 사용률 차이를 보여주고 있는 결과이다. 개선전 BGP SYN Attack 에 의해 CPU 자원은 공격패킷의 흐름과 같이 고갈되는 모습을 볼 수 있다. 라우터에서는 공격에 의해 CPU 자원의 고갈됨에 따라 정상적인 패킷 처리가 불가능해져 결국에는 BGP 가 다운되는 것을 예상할 수 있겠다. 개선 후 BGP TCP 구조를 적용한 결과는 개선전과 비교하여 볼 때 초기 CPU 자원은 소모되지만, 시뮬레이션 프로그램의 특성상 초기 쓰레드 형성을 위한 것이며, 이를 제외하면 CPU 자원은 즉시 안정되는 것을 확인 할 수 있다. 이는 TCP SYN Attack 이 개선된 알고리즘에 의해 라우터에 설정된 Neighbor Password 로 지정된 Key 가 확인되지 않은 패킷은 즉시 Drop 되어 TCP SYN Attack 에서 나타나는 연결설정 과정의 정보저장에 의한 큐 오브플로어가 발생되지 않음에 따라 CPU 가 안정되는 것을 알 수 있다.

5. 결론

본 논문에서는 대규모 네트워크망에서 라우팅정보를 전달하는데 사용되어지는 BGP 보안위협에 대해서 살펴보았으며, 특히 BGP TCP SYN Attack 이 실제 운영되는 라우터에 미치는 영향을 분석하였다. 분석결과 Source IP, Destination IP, Port 가 일치한 공격에 대해서는 ACLs 등 전통적 라우터 보안설정과, 고 성능의 보안 라우터 기능으로도 대응할 수 없음을 알 수 있었다. 이러한 결과로 현재까지는 네트워크의 라우터를 직접 대상으로하는 영향력있는 BGP SYN Attack 은 없었지만, 네트워크망의 라우터가 대상이 된다면 심각한 문제가 발생할 수 있음을 알 수 있다[3][4].

이를 해결하기 위하여 BGP 보안설정에 사용되어지는 BGP Neighbor Password 를 Key 로 활용한 개선된 BGP TCP 구조를 제안하였다. 라우터는 TCP 3-way handshake 과정에서 Key 를 확인하지 못하면 잘못된 패킷으로 간주하고 해당 패킷을 폐기하여 라우터 자원을 확보할 수 있었다.

참고문헌

[1] Y. Rekhter, “A Border Gateway Protocol 4(BGP-4)”, RFC4271, RFC4271, Jan. 2006
[2] Steve Gibson, “DRDoS(Distributed Reflection Denial of Service)” February 2002
[3] 정충교, “네트워크 분산반사 서비스 거부 공격(DRDoS)에 대한 역추적 시뮬레이션 설계 및 구현” 강원대학교 산업기술연구소 논문집, 제 27 권, 2007 년
[4] B. Kevin, F. Toni, M. Patrick, P. Jennifer, “ A Survey of BGP Security”, Vol. V, No. N, April 2005
[5] 진성복, “BGP 라우팅 프로토콜의 취약성 분석 및 개선방안”, 서강대학교, 2007 년
[6] E, Kranakis, P.C. van Oorschot, and Tao Wan, “Security Issues in the Border Gateway Protocol(BGP)”, Technical Report 05-07, Carleton University, 2005
[7] 정용훈, “Hop-Count 를 이용한 BGP 에서의 TCP Reset Attack 의 대응 모델”, 아주대학교, 2004
[8] 홍성철, 서신석, 홍원기, “IP Hijacking 유형분석 및 방지 방안 연구”, 포항공과대학교, 2008
[9] Yun Ling, Ye Gu, Guiyi Wei, “Detect SYN Flood Attack in Edge Routers”, International Journal of Security and its Applications Vol. 3 NO. 1, January, 2009
[10] Zin-Won Park, Joon-Hyung Lee,Myung-Kyung Kim, “Design of Extended TCP for preventing DoS Attacks”, Proceeding of 2003KORUS, 2003, Page(s)385-389
[11] CHARLES M. KOZIEROK, “TCP/IP Guide”, Oreilly & Associates Inc, 2005
[12] Cisco, “Cisco IOS XR Security Guide, Release 3.6” http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.6/security/design/guide/sg36book.html
[13] Cisco, “Defeating DDoS Attacks”, http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5888/prod_white_paper0900aecd8011e927.html
[14] Cisco, “Configuring BGP Neighbor Session Options”, http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration
[15] RIPE, “YouTube Hijacking: A RIPE NCC RIS case-study”, http://www.ripe.net/news/study-youtube-hijacking.html