Prototyping and Evaluating a Tunnel-Based Solution to Circumvent Malicious IISP Blocking

Amer Al-Ghadhban, Marwan H. Abu-Amara
Computer Engineering Department
King Fahd University of Petroleum & Minerals, Saudi Arabia
{g199642170, marwan]@kfupm.edu.sa

***Abstract*–Recently, the Internet is essential in providing numerous services to different types of users. Preventing the users from accessing these services has a serious impact on the daily life of the user. In this paper we considered a scenario wherein a specific region is maliciously denied from accessing the Internet by a single upstream International Internet Service Provider (IISP). Assuming the availability of a cooperative AS, we prototype and evaluate a tunnel-based solution proposed by *M. Abu-Amara [1].* The prototyping is conducted in a real laboratory designed and configured to be close to the Internet's ASes connectivity structure. Different tunneling protocols are examined with different Internet applications and background traffic loads. The prototyping proves the ability of the tunneling techniques in circumventing the Internet access denial performed by the malicious IISP. In addition, the IP-in-IP tunneling technique has shown the lowest end-to-end delay and traffic overhead.**

Keywords: Network security, IISP blocking and countermeasures, performance of tunneling protocol, the circumventing Internet access denial.

I. INTRODUCTION

The Internet is so vastly important that the majority of traditional media services such as TV and Radio channels, telephones and newspapers have been reproduced themselves through their providers in order to be compatible with Internet applications. The Internet has provided new human interaction services such as social networking, online shopping, instant messaging and website forums. Also, new government, business, academic and banking services have been offered to the Internet users through suitable web services.

The Internet is comprised of numerous interconnected networks that have dissimilar extent, called Autonomous Systems (ASes). An AS is a set of connected computer networks under the control of an Internet Service Provider (ISP) or a large organization. The routing protocol that is responsible for discovering the required network destination in the Internet is Border Gateway Protocol (BGP) which is a path vector routing protocol used to interconnect different ASes [2]. The Internet is vulnerable to many sources of disruption. For example, an International ISP (IISP) can mistakenly or maliciously block incoming and outgoing Internet traffic to a specific region by entering few Access Control List (ACL) commands in their BGP boarder router. The Internet suffered from many mistakes that led to widespread damages. [3]. On 25 April 1997, a mis-configured router advertised a routing update that claimed it had the best route to all Internet destinations. This mistake disrupted the Internet for about 2 hours [4]. Also, another mistake done by Pakistan Telecom caused a denial of service to the You-tube website [5]. In recent years, many other incidents have happened and were reported by *Boothe et al.* [3]. The estimated cost of Internet outage in Egypt is $18 million per day [6].

In the literature the term Malicious Service Provider (MSP) has become a common term. In *Chen et al.* [7] they consider several kinds of MSP in Grid Computing, one of them is defined as a service provider that accepts tasks but does not process them. In *Stone-Gross et al.* [8] they define the malicious service provider based on the malicious activities performed by the service provider's customers that do not result in a serious response from the service provider preventing these activities or their source. In addition, malware, spam and phishing are initiated from hosted servers in their network [9][10][11]. Also, In *Wang et al.* [12] they define the malicious service provider as the service provider that hijacks other networks' prefixes. On the other hand, under political and national security reasons a service provider may isolate a specific region from the Internet. On 19 Feb. 2011, the Libyan government forced their local ISPs to block the Internet access [13].

In this paper we consider a specific region that is connected to the Internet through a single International Internet Service Provider (IISP) that maliciously blocks Internet access to and from that region. Although, the malicious IISP blocks the Internet access of that region, the malicious IISP's BGP router is still exchanging BGP messages with that region and advertising its prefixes into the Internet. We assume the availability of two cooperative ASes: one resides before the malicious IISP and another after it. With this assumption we prototype and evaluate a tunnel-based solution as proposed by [1] in a real laboratory. The laboratory is configured with same BGP configurations that are usually implemented in a real ISP. The purpose of the prototype is to assess the effectiveness of the proposed solution in circumventing the Internet access denial by the malicious IISP.

We have designed four Java programs to automate our testing environment and that has allowed us to test the proposed solutions so many times to get accurate results. These programs have the capability remotely connect to a specific router and configuring it with the required configuration and records the required times and events such as the time of blocking event and recovering from it.

The paper is organized as follows: Section 2 discusses the literature review. Section 3 describes the proposed work. The results and conclusion are explained in Section 4 and 5, respectively.

978-1-4673-1950-8/12/$31.00 ©2012 IEEE

II. Literature Review

The topic of BGP is discussed extensively in the literature. Many papers have focused on the scalability and the performance of BGP such as [5][14][15]. Other papers have focused on the security weaknesses, attacks or countermeasures, such as [16][17][18]. A comprehensive survey about the BGP security weakness and countermeasure is accomplished by *Butler et al.* [19].

In particular, BGP attacks have been discussed in [20] wherein four main purposes for these attacks were identified: 1. *Blackholing* 2. *Redirection* 3. *Instability* and 4. *Supervision*. *Blackholing* is an attack method of dropping all the traffic passing through the attacker router. Also, the attacker may drop only a traffic that belongs to a specific AS. *Redirection is* a method of redirecting the whole or specific user's traffic to another destination or a server for content analysis. *Supervision* is similar to the *Redirection* method but for a different purpose which is modifying the traffic content then forwarding it to the right destination. *Instability* is an attack method to harm the network with destabilizing events such as injecting false updates, link flapping or announcing successive advertisement then withdrawals.

Tunneling protocol is a method of making a tunnel between the tunnel's endpoints over an existing network such as the Internet. The tunnel is created through encapsulating the transmitted packets between source and destination with a new IP header which contains new IP addresses for source and destination. The two tunnel's endpoints will have two IP addresses one for the underlay network, such as the Internet, and another for the overlay network which is the tunnel network and usually called Virtual Private Network (VPN). Also, the two endpoints will see each other as directly connected (i.e. one hop distance). This feature was utilized by *Alrefai* [21] to attract the incoming Internet traffic through a required IISP and circumvent the Internet isolation performed by the malicious IISP. Several protocols are available for setting up a tunnel between two endpoints. A well-known tunneling protocol is IP-in-IP which is described in RFC 1853 [22], and it explains the execution mechanisms for encapsulating IP version 4 with IPSec and other protocols. In the IP-in-IP encapsulation technique, the IP datagram is encapsulated with new IP header covered the original IP header [22]. The second protocol is Generic Routing Encapsulation (GRE) described in (RFC 2784) which is another tunneling protocol works over the IP layer [23]. GRE has the capability in encapsulate different types of network layer protocols over any type of network layer protocol. The IPSec protocol is defined in (RFC 2401) which had been proposed to mend the security weaknesses in the IP protocol by authenticating and/or encrypting every IP packet transmitted between end-systems [24]. The IPSec is originally proposed for IPv6, but it is widely used in IPv4. It offers two modes of operation: tunnel mode and transport mode. The tunnel mode encapsulates the transmitted packet with new IP header and the whole packet is authenticated or encrypted. The transport mode only the payload of the transmitted packet is authenticated or encrypted. There are many other tunneling protocols such as PPTP [25] and L2TP [26] but they are out of our consideration. In [27] we prototype and evaluate a BGP-based solutions to overcome the malicious IISP blocking. In contrast, in this work we prototype and evaluate a tunnel-based solutions to overcome the same problem.

III. Proposed Work

In the following two subsections we describe the prototyping laboratory setup, and the prototype methodology, respectively.

A. Testing Environment and Laboratory Setup

The laboratory is equipped with seven Cisco 2811 routers, four Catalyst 2950 switches, one workstation and three servers. Figure 1 provides a network diagram showing how the different devices are interconnected. The AS100 represents the blocked region network and AS300 represents the malicious IISP. On the other hand, AS400 represents the remote cooperative AS and AS200 represents the neighboring cooperative AS. The three servers reside in LAN_R6 as they are on the Internet side. The workstation is on AS100 as it is a client in the blocked region network. Also, each server is assigned a distinct Internet application (i.e. FTP, HTTP and real-time application). A WireShark [28] network analyzer is installed in the client and the server sides. Iperf [29] is used to generate real-time traffic.

B. Testing Methodology

In the prototype we create a tunnel between the blocked region gateway router (i.e. R2 in AS100) and the remote cooperative AS (i.e. R5 in AS400). The remote AS is responsible for attracting the blocked region's incoming Internet traffic and forward it through the established tunnel .The incoming and outgoing traffic is subsequently forward over the cooperative AS (i.e. R3 in AS200). As such, the malicious IISP cannot recognize the traffic of the blocked region, when it passes through the malicious IISP network. Any type of IP layer tunnelling techniques could be used to hide the blocked region traffic identity. The tunnelling techniques that were examined are: IP-in-IP, GRE, GRE with Checksum, and IPSec in tunnel mode. These techniques have dissimilar overhead and processing requirements. We investigate the network performance using the aforementioned tunnelling techniques along with three

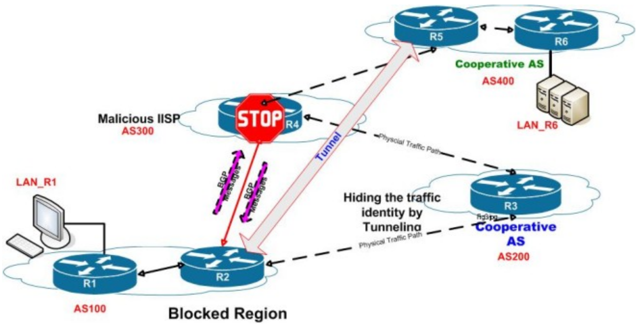

Figure 1. Laboratory Setup

different Internet applications; FTP, HTTP, and UDP. Moreover, we investigated the network performance under dissimilar traffic loads; 75%, 50% and 25% load. The 75% load means 75% of the link capacity is not available. So, for 2 Mbps link a load of 75% means that there is only 512 kbps left on the link.

We have written software, defined here *detecter*, that is capable of detecting the Internet blocking by the malicious IISP through using a simple ping mechanism. When it detects the blocking it directly configures the AS100 gateway router with one of the tunnelling techniques. After that, Wireshark with specific filter is started and one of the Internet applications is launched. We collect from the Wireshark the average throughput. The end-to-end delay and the drop rate is collected from the Iperf.

C. TCP and UDP Stream Testing Procedure

The TCP and UDP stream testing procedure is divided into multiple steps. In each step a tunneling protocol is tested with one of the following TCP or UDP application: FTP, HTTP or UDP traffic. During testing of the application, a network analyzer, Wireshark, is used to collect the required statistical results.

In step 1, one of the application's clients, such as FTP client, residing in the blocked region (AS100) starts communicating with the well-matched server that resides in AS400. At the same time Wireshark and *detecter* programs are running. At a specified instance in time a program telnets to the malicious IISP BGP speaker and configures it with the blocking configurations. When the *detecter* faces Internet connectivity failure, it immediately connects to the blocked region BGP speaker and configures it with one of the tunneling protocol, such as *GRE*. Note: the remote cooperative AS is already configured with the required tunneling protocol, except the final step which will be executed manually after Internet connectivity loss is detected. In real life, manual configuration is similar to making a phone call to the remote cooperative AS, asking it to implement the agreed tunneling solution.

Steps 2 and 3 are the same as step 1, but using HTTP and UDP traffic respectively.

In step 4 the previous steps is repeated but using a different tunneling protocol.

IV. Performance Evaluation

As stated earlier, the network performance is evaluated using each of the four tunnelling techniques considered. Also, the impact of these techniques on different Internet applications is investigated. We note that, the extra overhead that is introduced by IP-in-IP, GRE and GRE with checksum techniques are 20, 24 and 28 bytes, respectively [1]. The FTP file size used is 10 MB and the size of the used web page is 6 MB. Also, the UDP traffic is operated at 1.8 Mbps. In the following figures the *no tunnel* technique means the Internet applications are examined through the same network path without implementing any tunnelling technique.

Figure 2 illustrates the average throughput of the Internet applications examined with the selected tunnelling technique at 25% link load. The examined unencrypted tunnelling techniques showed a high utilization, especially with TCP applications, and that is very close to the throughput of the *no tunnel* technique Due to the small overhead of the IP-in-IP tunneling technique, it provides better FTP, HTTP and UDP average throughput than the other tunneling technique. However, there is a considerable difference between the plain tunneling technique and the *no tunnel* technique when they are examined with UDP application and this due to the behavior of UDP in sending the datagram as it is without segmentation, especially in this situation while we are sending the UDP datagram with 1.8Mbps and the link capacity is 1.5Mbps. Moreover, due to the encryption overhead in IPSec a significant drop in the average throughput is observed when it is implemented. The average throughout of the FTP with IPSec is only 40% of the average throughput for the unencrypted tunnelling techniques. Also, this conclusion is valid for HTTP and UDP. Similar observations are noticed with 50% and 75% link loads as evident from Figure 3 and Figure 4.

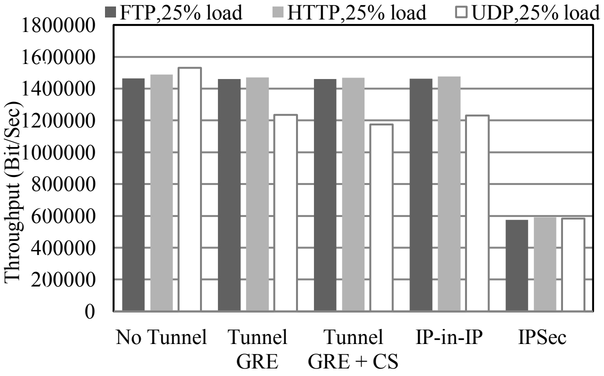

Figure 2. Average throughput of the Internet applications at 25% load

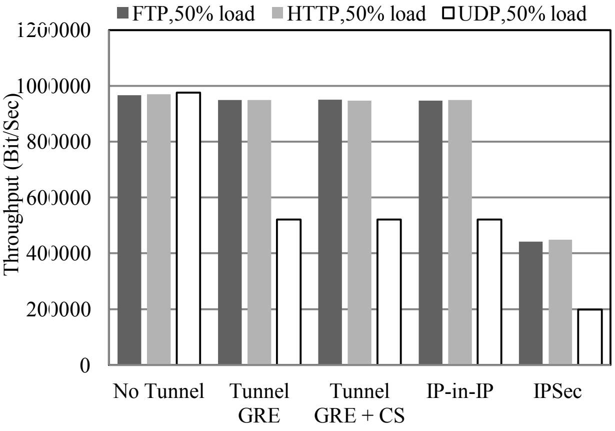

Figure 3. Average throughput of the Internet applications at 50% load.

Figure 5 shows the end-to-end delay of the FTP and HTTP with the examined tunnelling techniques under different traffic load. Obviously, the end-to-end delay increases proportionally with the increase in the traffic load. The unencrypted tunnelling techniques show almost the same end-to-end delays when they are compared with no tunnel technique. The IP-in-IP shows the lowest end-to-end delay when it is compared with the other tunnelling techniques due to it having the lowest overhead among the other tunnelling techniques. Furthermore, the percentage of the end-to-end delay is shown in Figure 6, where the IPSec shows the highest percentage of increase in the delay among other tunnelling techniques. In contrast, the lowest percentage of increase is shown with IP-in-IP technique.

Figure 7 illustrates the number of packets dropped after conducting UDP traffic at 100% (2.0 Mbps) and 75%. The percentage of lost packets at 75% load is less than 1% and it reaches 35% with 100% load. The GRE with checksum shows the highest number of lost packets, higher than IPSec, and GRE and IP-in-IP showed the lowest number of packets dropped.

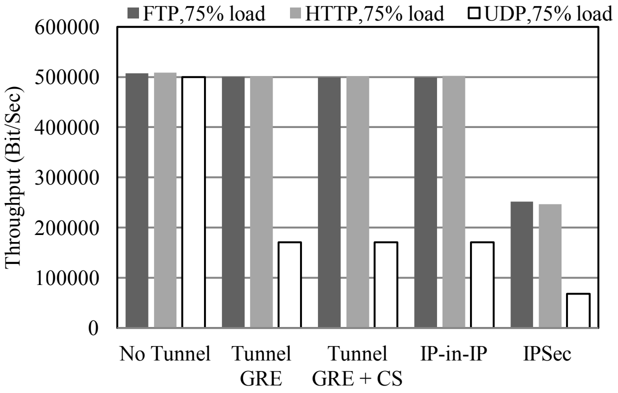

Figure 4. Average throughput of the Internet applications at 75% load.

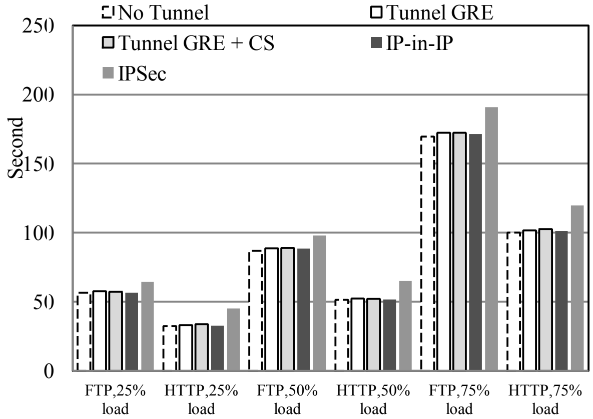

Figure 5. Shows the end-to-end delay of the examined tunnelling techniques

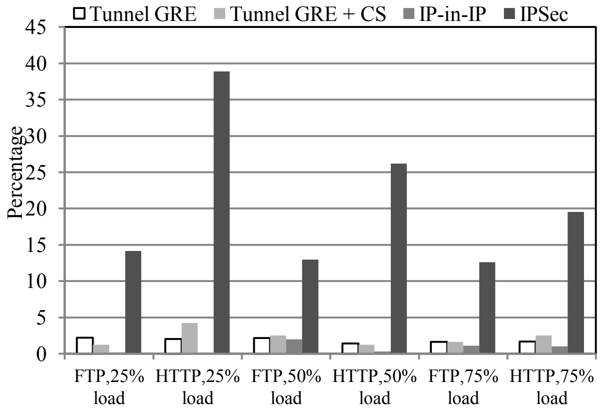

Figure 6. Shows the percentage increase in the end-to-end delay of the examined tunnelling techniques

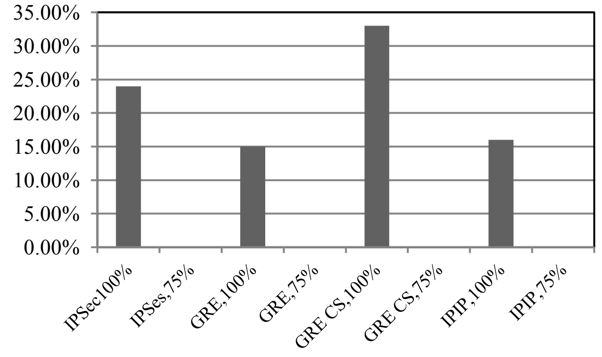

Figure 7. Shows the percentage of traffic drop

V. IN CONCLUSION

In this work we prototyped and evaluated a proposed tunnelling based solution to overcome IISP blocking. The prototyping and evaluating of the proposed solution is performed in a laboratory environment. It is of particular significance that e have designed our laboratory and configured its routers to be very close to the real Internet environment. Four different tunnelling techniques were considered; IP-in-IP, GRE, GRE with checksum, and IPSec. The examined tunnelling techniques have proved their ability to overcome the malicious IISP blocking by hiding the traffic identity. The results of evaluating the prototype show that the IPSec has introduced the highest traffic overhead on the examined Internet applications. Also, IPSec has the highest percentage of increase in the end-to-end delay. On the other hand, the lowest traffic overhead on the examined Internet applications and end-to-end delay is achieved by the IP-in-IP tunnelling technique. Moreover, the results show a significant difference between the examined tunnelling techniques and the *no tunnel* when the UDP application is considered. Finally, it was observed from the results that the GRE with checksum has the highest number of dropped packets.

ACKNOWLEDGMENT

The authors acknowledge the support provided by King Fahd University of Petroleum and Minerals (KFUPM). This project is funded by King Abdulaziz City for Science and Technology (KACST) under the National Science, Technology, and Innovation Plan (project No. 08-INF97-4).

REFERENCES

[1]. Marwan Abu-Amara, Mohammed A.K. Asif, Mohammed H. Sqalli, Ashraf Mahmoud, Farag Azzedin," Resilient Internet Access Using Tunnel-Based Solution for Malicious ISP Blocking," *In Proceedings of the 2011 IEEE International Conference on Communication Software and Networks, Xi'an, pp.85- 89, 27 – 29 May 2011.*

[2]. Y. Rekhter, T. Li, and S. Hares. (2006, Jan.) IETF-A Border Gateway Protocol 4 (BGP-4). [Online]. Available: www.ietf.org/rfc/rfc4271.txt

[3]. P. Boothe, J. Hiebert, and R. Bush, "How prevalent is prefix hijacking on the Internet?'' *in Proc. NANOG 36, Feb. 2006* [Online]. Available: http://www.nanog.org/mtg-0602/boothe.html

[4]. R. Barrett, S. Haar, and R. Whitestone, "Routing snafu causes Internet outage," *Interactive Week, Apr. 25, 1997.*

[5]. T. Bu, L. Gao, and D. Towsley,"On characterizing BGP routing table growth," *Computer Networks, 45(1), May2004.*

[6]. Parmy Olson, "Egypt's Internet Blackout Cost More Than OECD Estimates", Forbes, [Online]. Available: http://blogs.forbes.com/parmyolson/2011/02/03/how-much-did-five-days-of-no-Internet-cost-egypt/, Feb.2011.

[7]. W. Chen, W.Z, and Yang G, "On the Malicious Participants Problem in Computational Grid," *In Proceeding of Grid and Cooperative Computing: Second International Workshop,(GCC 2003). Volume 3032 of Lecture Notes in Computer Science., Springer-Verlag (2004) 839–848*

[8]. Brett Stone-Gross, Christopher Kruegel, Kevin Almeroth, Andreas Moser, and Engin Kirda, "FIRE: FInding Rogue nEtworks," *In Proceeding Computer Security Applications Conference, 2009. ACSAC '09. Annual, Honolulu, HI, pp. 231 – 240, 7-11 Dec. 2009*

[9]. N. Wang, Y. Zhi, and B. Wang, "AT: an origin verification mechanism based on assignment track for securing BGP," *In Proceedings of the 2008 IEEE International Conference on Communications, Beijing, pp. 5739-5745, 19-23 May 2008.*

[10]. V. Hanna. Spamhaus: Cybercrime's U.S. Hosts. [Online]. Available: http://www.spamhaus.org/news.lasso?article=636, 2008.

[11]. D. Bizeul. Russian Business Network Study. [Online]. Available: http://www.bizeul.org/files/RBN study.pdf, 2007.

[12]. B. Krebs. Report Slams U.S. Host as Major Source of Badware. [Online].Available: http://voices.washingtonpost.com/securityfix/2008/08/report slams us host as major.html, 2008.

[13]. Deena Beasley, "Libya cuts off Internet service: network monitor,"Reuters, [Online]. Available: http://www.reuters.com/article/2011/02/19/us-libya-protests-Internet-idUSTRE71I3XJ20110219

[14]. J. Li, M. Guidero, Z. Wu, E. Purpus, and T. Ehrenkranz. "BGP routing dynamics revisited." ACM SIGCOMM CCR, vol.37(1), pp.2013–2027, April 2007.

[15]. T. Griffin and B. Premore. "An experimental analysis of BGP convergence time," *In Proc. ICNP, 2001. pp.53-61, Nov. 11-14, 2001.*

[16]. C. Meyer and A. Partan, "BGP security, availability, and operator needs," *In Proc. NANOG 28, Jun. 2003.*

[17]. Y. Hu, A. Perrig, and D. Johnson, "Efficient security mechanisms for routing protocols," *In Proc. ISOC Network and Distributed Systems Security Symp. (NDSS), San Diego, CA, Feb. 2003.*

[18]. S. Kent, C. Lynn, J. Mikkelson, and K. Seo, "Secure Border Gateway Protocol (S-BGP) real world performance and deployment issues," *In Proc. ISOC Symp. Network and Distributed System Security (NDSS), San Diego, CA, Feb. 2000.*

[19]. K. Butler, T. Farley, P. McDaniel, J. Rexford, "A Survey of BGP Security Issues and Solutions," *In Proceedings of the IEEE, vol. 98, issue 1, pp. 100-122, 2010.*

[20]. O. Nordstrom and C. Dovrolis, "Beware of BGP Attacks," ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 1-8, Apr. 2004.

[21]. A. AlRefai, "BGP-Based Solutions for International ISP Blocking," *Master Thesis submitted to Deanship of Graduate Studies, King Fahd University of Petroleum and Minerals, May 2010.*

[22]. C. Perkins, "IP encapsulation within IP," RFC 2003, Internet Engineering Task Force, Oct. 1996.

[23]. D. Farinacci, T. Li, S. Hanks, D. Meyer, and P. Traina, "Generic routing encapsulation (GRE)," RFC 2784, Internet Engineering Task Force, Mar. 2000.

[24]. R. Atkinson, "Security architecture for the Internet protocol," RFC 1825, Internet Engineering Task Force", [Online]. Available: http://www.rfc-editor.org/rfc/rfc1825.txt, Aug. 1995.

[25]. W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, and B. Palter, "Layer Two Tunneling Protocol (L2TP)," RFC 2661, Internet Engineering Task Force, August 1999.

[26]. K. Hamzeh, G. Pall, J. Taarud, W. Little, and G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, Internet Engineering Task Force, July 1999.

[27]. A. AlGhadhabn A. Mahmoud, M. Abu-Amara, , F. Azzedin, M. Sqalli, ," Prototype and Evaluate BGP-Based Solutions to Overcome Malicious ISP Blocking," In Proceedings of the 2011 2nd International Conference on Networking and Information Technology, Hong Kong, vol. 17, pp.134- 143, 25 – 27 Nov. 2011.

[28]. "WireShark," [Online]. Available: www.wireshark.com

[29]. "Iperf," [Online]. Available: http://sourceforge.net/projects/iperf/