ISSN (Online) : 0974-5645
ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(S2), 127–132, January 2015* DOI : 10.17485/ijst/2015/v8iS2/59169

Border Gateway Protocol Performance and its Protection against Disturbed Denial of Service attack

Rakesh Kumar Achar*, M. Swagath Babu and M. Arun

School of Electronics Engineering, VIT University, Vellore-632014, Tamilnadu, India; rakeshachryaa@gmail.com, mswagathbabu@gmail.com, arunm@vit.ac.in

Abstract

Now a day the internet has become very popular in the world. Simple work to complicated work you can accomplish by using internet. Such popularity leads to chances of exhaustion of Internet protocol version 4 which is currently available. To overcome such problem, IPv6 comes in the picture. IPv6 provides more address space, better addressing mechanism and equipped with high security protocol. Unfortunately these IP versions are not compatible to each other. To make such protocol compatible, various tunnelling mechanism are using. Along with tunnelling mechanism, various inter-networking attack like DDoS etc. become serious issues for various routing protocol e.g. Border Gateway Protocol (BGP). Such attacks make an impact to the performance of system such as delay, more updates, insufficient bandwidth utilizations and loss of valuable signal.

In this paper we propose a tunnelling mechanism which is based on the Border Gateway Protocol (BGP). BGP is an inter domain routing protocol basically designed to provide loop-free routing links between organizations. BGP is designed to work over a trustable transport layer protocol; it uses Transport Control Protocol TCP port 179 as the transport protocol layer because TCP is a connection-oriented protocol. We have also proposed two theorem to secure the Internet from Domain Name Server (DNS), Distributed Denial of service(DDoS) attacks which is using Border gateway routing protocol, first one to isolate defected region and correct region, suppressed unnecessary updates without hampering any effect on the define path. Secondly, to cut down the route swinging which is responsible to generates hell lot of updates and the paths selected are scrutinized to remove the attacked links. Our simulation shows the methods to eliminate false number of unwanted updates under the influence of the attacks, and isolate the effected part from the network.

Keywords: BGP, DDoS, DNS, IPV4, IPV6, Tunneling

1. Introduction

The current version of the Internet Protocol, IPv4 is very popular and widely used all over the world. It is very easy to configure, implement, and supports a wide range of applications. However, the growth of the Internet usage has depleted the IPv4 addresses. As number of user requires connectivity from the Internet increases, due to limit IPv4 addresses space, it is almost impossible to address this increasing demand currently. To overcome from such situation, IPv6 is come in the picture that resolves the problem of IPV4. For latecomers to the Internet explosion, IPv6 is going to become one of the important sources in the era of internet. Therefore in future IPv6 is expected to be widely used in the advancement of internet. But again one serious problem is the transition between IPv4 and IPv6 because these two protocols are not backward compatible. It is totally out of scenario to switch the entire internet over to IPv6 overnight. To overcome from this situation, various tunnelling mechanism (BGP) are developed to make these protocol compatible.

*Author for correspondence

Another sever issue is that Internet is now become critical global business applications. Various attacks targeting to this infrastructure of internet may be cause significant loss to individuals or institutions or business organisation. The well-known DDoS attacks can severely disrupt the routing system of the network, which leads to network loss of data, reducing throughput, unnecessary updates and lost connection and data. We are generally calling such attacks as DDoS attacks, which is generally generating lots of fake updates which lead to network to transmit wrong information to the wrong location and cause loopholes in the security. This attack is pre-dominant in Border Gateway Protocol.

To protect the network against the DDoS kind of serious attacks, it becomes basic necessity to reduce the number of unwanted updates. One of the perfect procedures is to protect BGP connectivity session from being closed continuously, such as S-BGP measure the data which is passed between Autonomous Systems using public key certificates. However, to get the data error free, such kind methods are costly in terms of money and space. As it is difficult to confirm absolute security of BGP sessions, HTTP link point, scalability, control and isolation on the next generation specified rule to segregate the Ethernet into a set of two isolated regions in the case of attacks which leads to enormous updates, which going to help the network to protect the change of network physical and logical topology and routing information from transmitting out of the region where the actual change occurs in the network. Link state routing protocol isolates the effected path locally in shortest path routing through different propagation velocity. Unfortunately, these works provide new protocols which leads change from BGP, so it is difficult to apply them into practical world. Moreover, they do not try to isolate attacks to the smallest scale.

In this paper, we have established a tunnelling mechanism using the BGP routing rules to get rid of Core MPLS control plane and Internet prefix from the core. For protection from the internet based attacks we have proposed two mechanisms to eliminate the unnecessary update messages. Firstly, to separate the attacks in local region, some unnecessary updates are needed to suppress independent of the routing. Secondly, to cut down of the route swinging caused by repeatedly attacking of the links, the selected paths are corrected to detect the attacked links, which is results in the attacks are introduced to avoid deliberately attacking one target.

2. Proposed Model

2.1 Performance Analysis of BGP Compare with Other Tunnelling Protocol

Here we used two router named as R1 (7200 series) and R2 (7200 series)which is connected internally on IPv4 platform. IP address of two routers connected towards each other is 192.168.6.1(R1) and 192.168.6.2(R2). IPV4 platform has IP address 192.168.6.X/24.

Both R1 and R2 using Fast Ethernet port fe0/0 to build connection between them. The router R1 and R2 connected to external device which is using IPV6 address. For outer connection, they are using IPV6 address which are 2001::2/64 and 2001::1/64 and used a physical fast Ethernet port f0/1. Local Autonomous System for R1 is AS100 and for R2 is AS200.

2.1.1 Algorithm

- Prioritize the path which has the highest access weight.
- Prioritize the path which has the highest local preference.
- Prioritize the Exterior BGP over the Interior BGP.
- If both the paths are exterior, then prioritize the path based on FIFO.
- Prioritize the path that was originated locally from a network to redistribute command.
- Prioritize the path which has the lowest AS_PATH.
- Prioritize the path which has lowest ORIGIN type.
- Prioritize the path which has the lowest Multi Exit Discriminator.
- When both path are external, prioritize based on FIFO.
- Prioritize the route, coming from the BGP switch which has the lowest router ID reference.

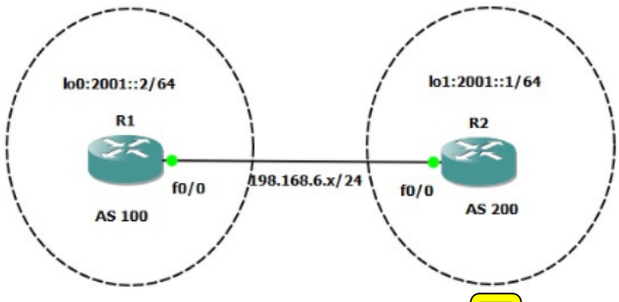

Figure 1. Tunnelling between IPv4 and IPv6

- If the router ID is the same for multiple paths, prioritize the path which has the minimum cluster list length among the complete one.
- Prioritize the path that comes from the lowest neighbour address.

2.2 Protection of BGP against from Disturbed Denial of Service

Above figure comprise of two LAN and six Ethernet Routers. BGP Routing Protocol is using to select the path. The key point of the DDoS invade is that route can be swings to creates too many update data to dissipate the resources of the routers or customers. In this paper, to eliminate the whole slightness of the system, we are trying to compress the redundant updates which are independent of routing. To cut down or shut down the route swinging happened by session failure and re-establishing, the selected best path are scrutinized to validate the attacked links, which cause of loss of data and cause unnecessary delay. In this paper, we assume only DDoS attack that's cause instabilities in the system and apply certain theorem so that we can get rid of such kind of attack.

2.2.1 Suppressing Unnecessary Updates

BGP is a very versatile routing protocol but again for everything there are certain disadvantages. BGP couldn't able to isolate the fault when it gets attack by the DDoS. Again BGP has slow table transfer, we are looking forward to implement a TCP delay Analyzer. Here we stated two mechanisms which we isolate the fault whenever BGP get attack by DDoS. Such method improves the performance of the network which we have shown in our result tab.

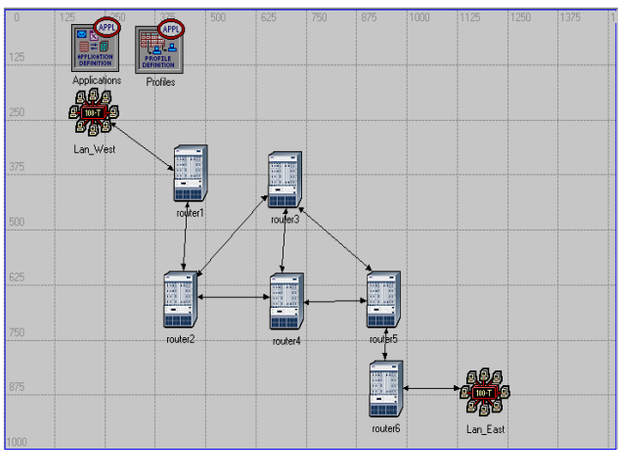

Figure 2. Connection between routers using BGP protocol.

Assumption 1: Here we assume that most suitable path from AS v to $d \in \upsilon$ is $best_d(v)$, and AS m is corresponds to the path, i.e. $m \in best_d(v)$, $m \neq u \neq v$. the condition is if the most suitable part of m while propagating to reach the destinations d changes from p_1 to p_2, and the length values are in the range is $0 < |p_2| \leq |p_1|$, broadcasting the changes that contain p_2 does not change the partial path between m and v in $best_d(v)$, i.e.$best_d(v)^{m-v}$

Solution: We consider that initially there is no updates happen, the most desirable path p_1 and $best_d(v)$ are chosen among the various available paths R_d^m and R_d^v in m and v respectively. If any changes is going to occurs, the suitable paths in m and v change $R_d^m - p_1$ and $R_d^v - p$ to where $p \in R_d^v, p_1 \subset p$. Thus the taken out not does cause any change the assign local preference number that is pre-defined assigned and rules in m and v *values.* If the changes just a broadcasting, and when the broadcasting is introduce with the help changing rules, the suitable paths of m and v are remain stagnant as R_d^m and R_d^v; such changes when applied to link associate with m and v, the idle routes in m and v are change to $R_d^m Up_2$ and $R_d^v Up$, respectively, where p is the available path to reach the destination d from v that meeting each other at $p_2 \in p$. However previously, the values of the local preference and m and v remain same and didn't changes happen. After that, all the paths which is added are of $R_d^v Up - R_d^v$ are formed by aggregating partial path $\{p_1^{m-v} | p_1 \in R_d^v, m \in p_{1\}}$ and p_2, for all the updates belong to the same affected condition under the one operations. Finally the local preference changed in m not in v. Hence we got conclusion as follows:

Corollary 1: When we are choosing a new path. If there is no longer path than it is to be replaced it with best path, compressing the new route independent network topology and routing can be seen as from the AS's got rid

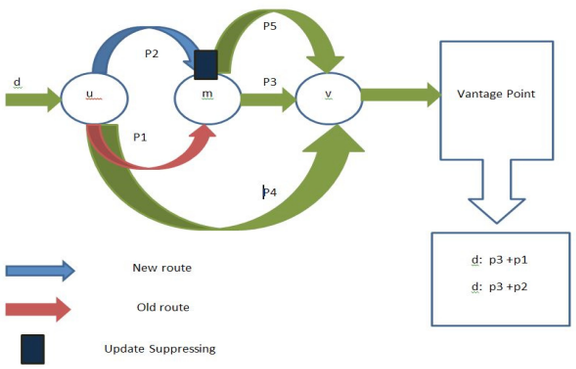

Figure 3. Routing flow diagram.

of the effected region to the AS who is generally creating unnecessary problem in building up a connections.

Taking Figure 3 for example, if the most suitable route from AS v to d is the initial condition, the path is going to be changed i.e $p_3 + p_1$. When an external parameter trying initialized the most suitable path changing from p_1 to p_2 at AS m, and p_2 is going to updated to AS v, if $|p_2| \leq |p_1|$, v is going to keep $p_3 + p_2$ as the new most suitable best route, even though $p_5 + p_1$, $p_5 + p_2$ and p_4 are of the same equal length with $p_3 + p_1$. Thus v will be going through the path p_3 to reach the place d, which causes the same effect if the path p_2 is suppressed at m AS.

According to our assumptions, we are broadcasting the updates which comprise of paths whose original length expanding, and impact created the chosen path again increasing longer as span goes on. Since the path no longer remains shortest cause unnecessary delay in the transmission. To avoid such kind of critical scenario, we broadcasting few path of shortest length path if and only if the accepted root is the preferred path[2], which is the route to one destination that that is always present in the routing table for the longer span of the time. The idea over here that internet usually ignore such data that are usually taking to much time to each the destinations and manually you can do configure to make them resolve. But if the recovery time for shorter path is not acceptable and creates lots of unnecessary updates. Finally we need to set up a set a rules to isolated such attacks in the local region of BGP:

C1: All data and routes are same,

C2: Route length becomes small and the route is available is more referring as the preferred path.

As stated in[2], changes in rules cause a huge amount of changes in the path's length, so C1 will consequently reduce the number of the updates. Work in[1] analyzers how the results that in a real BGP data which is in the raw state and proved that around 60 percent of the changes broadcast the path with same length, and around 10 percent broadcasting shorter path. 16 and 20 percent for longer path and uncertain result. The significance of C1 and C2 is that, it reduces the too many numbers of updates. All these are practically shown in our paper with the help of the OPNET simulator.

2.3 Broken Route Flapping

Since the necessity of DDoS attack cause lot of interrupt and creates a problem in the connections which further leads to generation of the hell lot of update. So it is become crucial to cut down the route that cause a swing in the attack against of such kind of severs issues. As illustrated in[2], we observed the time period, how long it is going to affect the path of the system. Based on that session time is decided. The continuous problem of the disconnection going to cut down and bring the system to the original states. The basic idea here to eliminate the problem of connection congestion. Consequently we can identify the attacked link and can able to trace the suitable solution for it. Such security analysis removes the needs of the firewall and makes the system cheap and healthier. Now when system is under the impact of the attacks, we have to select the stable path first in the nearest of prefix d. Once stable path selected and after that we can check the instability and set the path name p1 and p2. If the specified path set facing same kind of the problem again and again, we can determine that some external source trying to access the system. To reduce such effects, it is important to get to the location of the system. By combining the two paths, we assure that, p1 is the stable path before any instability occurs.

Again with process, once we find the effected path, we can later check the instability system, check it out from which IP we are getting wrong updates and reduce the chances of snooping. Our approach can gently enhance the stability of the system and makes the routing protocol efficient.

3. Result

Part I: BGP Performance

In[1], they found that (on the basis of IPv6 Transition mechanism in order of lowest delay) 6PE and dual stack over MPLS has lowest delay around 0.333 sec whereas this research paper obtained a delay on average of 17 ms. Hence it improved the performance of the system efficiently.

3.1 Comparison Tabular Column

Data Rate (Mbps)	Delay(msec) using BGP	Delay(msec) using Dual Stack on MPLS	Bandwidth Utilization (Hz) using BGP	Bandwidth Utilization (Hz) using Dual Stack on MPLS
0.064	0.06271	0.081523	381.928	420.012
0.128	0.034	0.0459	588.235	637.0585
0.256	0.02	0.0262	1000	1100.23
0.512	0.013	0.01742	1538.461	1692.3071
2.048	0.00775	0.0101	2580.645	2838.7095
5	0.0067168	0.00873184	2977.608	3275.3688
10	0.0063582	0.008123	3145.544	3522.86
50	0.0060718	0.008001	3293.916	3687.21
100	0.0060358	0.008124	3313.562	3796.81

Figure 4. Comparison tabular column between Delay and Bandwidth Utilization.

3.2 Comparison in Graphical Format

Part II: Protection Against DDoS

Above simulations show that in simple BGP, if there is no proper way of isolating the attack cause abrupt change in throughputs and leads to the waste of the data. It is indicated by red colour. Whereas when we applied the two policies which are mentioned in introduction, we found that it tries to stabilise the abrupt change in throughput. It leads to reduction in wastage of data. Hence enhance the overall performance of the system or network.

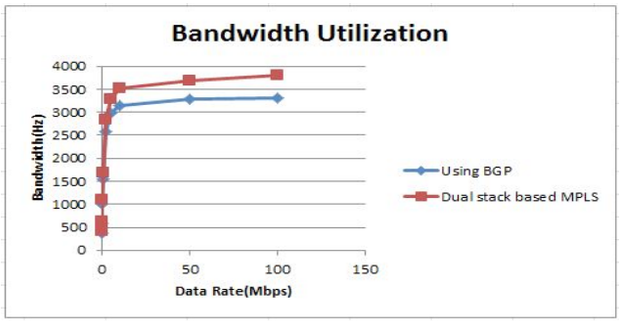

Figure 5. Bandwidth Utilization curve for BGP and Dual Stack MPLS.

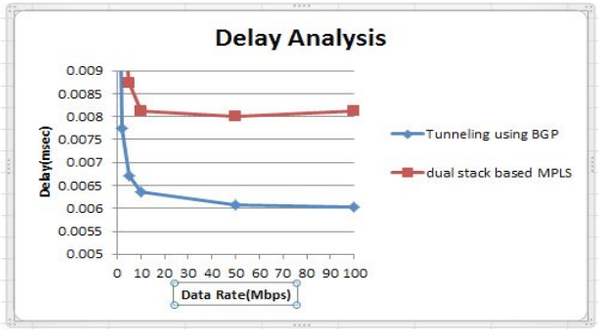

Figure 6. Delay Analysis curve for BGP and Dual Stack MPLS.

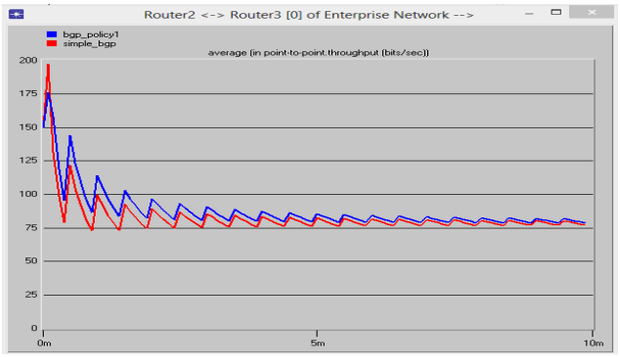

Figure 7. Isolation mechanism curve for BGP and simple BGP.

4. Conclusion and Future Work

BGP protocol provide a great role to a communication between two different network and makes the platform where IPV4 and IPV6 address can talk to each other without any needs to have addition hardware architecture. Various tunnelling method can be accommodate using BGP new rules without any further cost. Only requirement is to get knowledge of the software. Another biggest advantage of the BGP, to avoid the interference BGP is provided with access weight. It increases the scalability of the MPLS and enhances the performance of the network.

The MPLS tunnelling mechanism force the core routers to forward packets using identifier known as a label only without destinations information in the IP routing. Only edge routers forward packets by looking up their destinations in the routing table. This means that edge routers need to have this information, so they need to run BGP. In this paper we show that BGP tunnelling required on average of 17ms to setup the connection which compared very less to[1]. Again BGP Mechanism can be applied on any tunnelling method without need of additional hardware.

DDoS attacks are become serious issue for internet and researches are going on these, how to tackle their impact in the critical internet applications. Such attacks cause lots of false updates and makes panic to users. Again it becomes a friend of hacker which further leads to loss of the data in the system. Here we applied two rules to tackle such kind of attacks. First one to isolate defected region and correct region, suppressed unnecessary updates without hampering any effect on the define path. Secondly, to cut down the route swinging which is responsible to generates hell lot of updates and the paths selected are scrutinized to remove the attacked links. Our simulation shows the methods to eliminate false number of unwanted updates under the influence of the attacks, and isolate the effected part from the network. In future work, BGP has slow table transfer; we are looking forward to implement a TCP delay Analyser.

5. References

1. Mazzuchi T, Grayeli P, Sarkani S. Performance Analysis of IPV6 transition Mechanism over MPLS. IJCNIS. 2012; 4(2):91–103.

2. Kaur H, Kaur N, Goyal J, Govil J. An examination of IPv4 and IPv6 networks constraints and various transition mechanisms. Southeastcon IEEE; 2008.
3. Wu J, Bi J, Leng X. IPv4/IPv6 transition technologies and univer6 architecture. IJCSNS. 2007; 7(1):232–43.
4. Dutta N, Biradar SR, Chakraborty K. Simulation of IPv4-to-IPv6 Dual Stack Transition Mechanism (DSTM) between IPv4 hosts in Integrated IPv6/IPv4 Network. IEEE International Conference on Computers and Devices for Communications; 2009.
5. Zhu P, Bonaventure O, Wang X. Stabilizing BGP routing without harming convergence. 14th IEEE Global Internet Symposium (GI) 2011. IEEE INFOCOM.
6. Carpenter B, Moore K. Connection of IPv6 Domains via IPv4 Clouds. IETF RFC 3056. 2001. Available from: http://dl.acm.org/citation.cfm?id=RFC3056.
7. Zhang R, Bartel M. BGP design and implementation. Available from: http://www.scribd.com/doc/44597538/BGP-Design-and-Implementation.
8. Cisco IP Routing Manual: BGP Configuration Guide. Available from: http://www.cisco.com/c/en/us/td/docios-xml/ios/iproute_bgp/configuration/15-s/irg-15-s-book.pdf.