Study of BGP Convergence Time: A Survey

Rohit Nilkanth Devikar*[1], Dipak V. Patil[2], V. Chandraprakash[2]
[1]Departement of Computer Science and Engineering, K L University,
Vaddeshwaram, Guntur, India
[2]Departement of Computer Engineering, MET, Bhujbal Knowledge City,
Savitribai Phule Pune University, India
*Corresponding author, e-mail: rohit.devikar89@gmail.com

Abstract

Border Gatway Protocol (BGP), a path vector routing protocol, is a widespread exterior gateway protocol (EGP) in the internet. Extensive deployment of the new technologies in internet, protocols need to have continuous improvements in its behavior and operations. New routing technologies conserve a top level of service availability. Hence, due to topological changes, BGP needs to achieve a fast network convergence. Now a days size of the network growing very rapidly. To maintain the high scalability in the network BGP needs to avoid instability. The instability and failures may cause the network into an unstable state, which significantly increases the network convergence time. This paper summarizes the various approaches like BGP policies, instability, and fault detection etc. to improve the convergence time of BGP.

Keyword: BGP, BGP policies, convergence time, instability, link failure

1. Introduction

Border Gateway Protocol (BGP) is interdomain routing protocol. Such protocol offers routing functionality between autonomous sytem. Earlier the primary objective of BGP was to provide scalable and robust routing functionality, and time required for the network to recover from the failure was the secondary important. In this paper we analyse the BGP problems and identify various algorithms that improves the convergence time significantly. Labovitz et al. [1], [2] noticed that sometimes BGP takes a substantial amount of times and messages to converge, and stabilize the failure of some node in the internet. The Yehuda Afek et al. [3] has given a minor modification to BGP, that eliminates the problem pointed out and substantially reduced the convergence time and communication complexity. An important parameter in the BGP convergence time is minimum route advertisement interval. Basically it is a amount of time BGP enforce between the sending of consecutive announcement from routers to its neighbors. Griffin and Brian [4] shows that for each specific network topology there is an optimal value of minimum route advertisement interval (MRAI) that minimizes the convergence time. The MRAI value proposed in this approach changing from network to network that can't be efficient to improve the BGP performance. A new solution to reduce the convergence time complexity was introduced in [5]. They use the information provided in ASPath to define route consistency assertion and use this assertion to identify infeasible routes. However this technique requires extra computational resources for checking router consistency and to send extra information in the BGP messages. It also introduced difficulties in some cases, when AS partitions and some routers in the AS become disconnected from other routers in the same AS. The Yehuda Afek et al. [3] [dec 2004] proposed a ghost flushing solution to reduce the problem of convergence time. In the network sometimes incorrect information are forwarding for a long duration of time. This information is nothing but the ghost information. Such information disturbs the convergence of routers in case of both fail down and fail over mechanism [1]. The ghost information is outdated for network convergence that will enter the networks into unstable state. To improve this problem Yehuda Afek et al. [3] modify BGP by introducing ghost flushing rate and ghost flushing rule.

1.1. Route Cause Notification

The path vector protocol does not have periodic updates/advertisements. The update message can be triggered only when changes happened in the connectivity. These changes in the link connectivity will be detected by routers which is adjacent to that link. For any given destination, one of the nodes from two adjacent nodes may change its route; we call this node as root cause node. The root cause node attaches its ID to the update message, which will then propagate in to the network. Unlike to flooding (in link state routing), the Simple Path Vector Protocol-RCN (SPVP-RCN) [51] piggyback the root cause notification in the updates, due to this only direct neighbors and affected nodes are notified [22], [25].

1.2. Routing Performance

The ghost flushing [3], RCN [6], [51], and FECN [7] analysis uses U delay model. The limitation of U model is that for all nodes there is same network-wide fix upper bound $h(G,[v \leftarrow u])$. But in the network topology each node may have different upper bound $h(G,[v \leftarrow u])$. The U model gives rough estimation of convergence time, also it fails to show the relationship between network topology and convergence time. Dan Pei et al. [9] proposed Q model which combines a queuing delay estimated into $h(G,[v \leftarrow u])$ and better reflect BGP implementation. For calculating queuing delay they consider sum of transmission and propagation delay on any link *(ld)*, maximum message processing time *PMax*, and summation of *ld, queuing delay*, and message *processing time*, when message is propagated from **u** to **v** denoted as $h(G,[v \leftarrow u])$. Inter-domain routing consists of problems like performance and route aggregation. Many people use geographic information for routing and addressing mechanism. Researchers have focused on reducing the geographical length of selected path by routing mechanism to improve the routing performance. The Taoyu Lia et al. [38] suggested that above technique does not used to improve the actual end to end transmission performance; rather they developed a performance model based on transmission delay. The transmission delay consists of both propagation delay and queuing delay. By experimental result they have shown the improvement in the performance of routing mechanism up to 50% by actual packet delivery mechanism.

2. BGP Policies

The BGP allows an AS to apply different local policies for selecting route and propagating reachability information to another domain. But autonomous systems have conflicting policies that leads to instability in routing. Sometimes routing oscillation reduces the performance of network in terms of quality of service (QoS). Up till now many modification have been made on BGP protocol that dynamically notice and solve policy-induced oscillation [14], [15]. In internet each AS have there routing policies for packet transmission [34]. As a result, if any policy destruction occurs at intermediate AS, causes packet dropping before reaching to the destination. BGP solve the problem of packet dropping. BGP works on the principle of hop by hop transmission, resulting in some routes are unreachable even though there is a physical path available to reach destination. To overcome this problem Jyh-haw Yeh et al. [33] have proposed a source policy route discovery protocol, which will resolve the false negative unreachable destination in BGP. The B. Quoitin et al. [36] allows the internet service providers to control the incoming traffic flow by proposing the utilization of redistribution communities. This has been done by controlling the distribution of routes advertisement with the peers. L. Xiao et al. [35] systematically studied the lifetime of BGP session under certain network congestion using statistical and simulation methods, which can be caused by worm attacks or by traffic engineering failure. Among independent ASs, when any changes happened in inter-domain routing, there is a need of on-demand routing adjustment. To resolve this problem Osamu Akashi et al. [37] have proposed a virtual router (VR) technique, which controls the conventional BGP routers from exterior world without any protocol extension. The virtual router combined with multi-agent system to adjust inter-AS routing. The VR controls inter-domain routing by dynamically switching transmission paths among alternate BGP entries. The AS consists of many attributes to express routing policies. The work have been done up to 2011 are not analyze the impact of routing policies on BGP convergence condition and convergence time by considering MED (Multi Exit Discrimator). The Huaming Guo et al. [42] fill the gaps and analyze the impact of routing policies on convergence condition and convergence time including

MED attributes. To represent routing policies in BGP including MED [42] first introduce a timeless model, later on they extended it to real time model by adding edge delay. They also derive a sufficient condition on the routing policies for robust convergence and an upper bound on convergence time. Martin O. Nicholes et al. [43] evaluated the effectiveness of Inter Domain Collaborative Routing (IDCR) using degree algorithm, greedy algorithm, and factor algorithm, which allows a friend routes to determine routes collaboratively.

2.1. Routing Tools

Lixin Gao et al. [10] proposed detail BGP model and a set of guidelines for AS to follow in setting its routing policies without considering global co-ordination among autonomous systems to improve the stability in the internet. Nick Feamster et al. [18] developed a tool called router configuration checker (RCC), which identifies fault in BGP configuration. RCC enables network administrator to test & debug configurations before deploying them in the network. The authors have analyzed the configuration on 17 different ASs to detect variety of faults which in turn used to improve internet routing infrastructure. For designing a stable BGP protocol Griffin et al. [16] have proposed a formal tool, but it fails to provide guaranteed service continuity when deploying any changes to BGP. To overcome this problem Luca Cittadini et al. [17] proposed a Greedy+ algorithm (improve traditional Greedy algorithm) which provides correct reports for stability of a network, also used to spotting the fault pints in the oscillated path, and checks the convergence of BGP in an abstract model. BGP configuration faults causes packets loss and forwarding loops that corresponds to failure in the network infrastructure. BGP configuration faults causes packets loss and forwarding loops that corresponds to failure in the network infrastructure.

3. Fault Detection in BGP

Distance vector routing protocol have slow convergence problem. In distance vector, each router maintains its routing table that contains information about reachability to destination. Due to changes in the topology distance vector takes longer time to converge information, which were introduced count to infinity problem in the network [11]. The solution to above problem is the introduction of BGP, which provides a path vector approach contains entire path to reach destination. Another attempts to overcome count to infinity problem includes split horizon, diffusion update, and trigger update algorithm. The Craig Labovitz et al. [1] analyze the impact and the rate at which inter-domain routing repairs and failures, advertise this information through the internet. They proposed a novel approach to improve the convergence, but changes increases the router overhead and complexity. Pei et al. [6] improves the BGP convergence time by identifying a fault location and indicating all the routers which are in the path of fault zone to avoid the incoming updates, due to this other routers not using that path for future transmission.

3.1. Hot Potato Routing

Renata Teixeira et al. [19] proposed a Hot Potato routing technique works on the basis of link weights and link failure. The figure 1 shows router A will choose the egress router C to travel the traffic to different ASs. Suppose distance between A→C changes from 9 to 11 intentionally or link between A→C failed due to some interruption. Although the distance between A→C changes, still there is a path between A→C is available but has a large distance. A chooses the path A→B to forward the traffic. This routing which changes the path dynamically called hot potato routing. The routing in the network is flexible and visible to all neighbors in the network, which is efficient to improve the network convergence. But hot potato technique has the chances of packets loss due to slow convergence of BGP. The Alejandro Ruiz-Rivera et al. [50] have proposed a green networking technique in addition to hot potato called HOTPLEC that shutdown the least utilized links or routers during off peak hours. Due to shutdown of unutilized links or routers reduces the energy consumption of network without negative impact on BGP.

3.2. D-BGP

During route convergence, the transient routing failure, losses the end to end reachability of the internet path. Also, this failure causes the packet losses in the network which will create problems on voice over IP packet transmission. To reduce this Feng Wang et al. [27]

have studied transient routing failure during changes happened in the routing (such as failure and recovery in BGP system) by applying routing policies. Due to this network administrator can improve the performance and stability of the network. Also they developed Two path diversity aware routing protocols [28] D-BGP and B-BGP to improves the resilience of inter-domain routing. These protocols established multiple paths with low routing burdens by exploiting existence of path diversity in the network infrastructure. Yi Wang et al. [30] [2009] on the basis of neighbor routers apply the filtering policies to the BGP routers, to improve the fast transmission. Due to this routers select routes dynamically as per neighbor routers availability. The main problem with DBGP [28] is it increases path diversity by advertising multiple paths. If route failure occurs, D-BGP selects alternate path without considering its quality. To overcome this problem [30] proposed a technique, which established shortest path using D-BGP, but it selects alternate path based on link availability and bandwidth. This technique increases fault tolerance and reduce message overheads and updates. Chaitanya et al. [29] have proposed a technique that will provides BGP shortest path and OSPF lowest cost metric for mobile ad-hoc networks. It increases the routing table entries, but transmits the traffic to destination with lowest cost. Mohammad Yanuar Hariyawan [8] compared different technoques like Fast Reroute one to one backs up, local rerouting, Haskin, 1+1 path protection recovery mechanism and PSL oriented path protection mechanism technique for fast rerouting after failure. The performance shows that 1+1 path protection recovery mechanism has minimum packet loss, but having more cost.
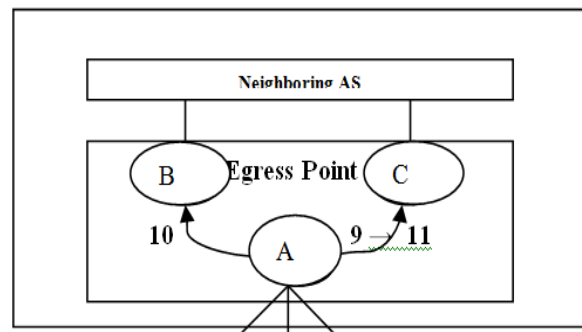

Figure 1. Hot potato routing changes from C to B

The Chengchen Hu, et al. [55] provides a technique for recovery after failure. By using AS-level complete map and IXP database, they measure the path diversity, recovery ration and shifted the path in different failure scenarios. The experimental result shows that the proposed technique is efficient to recover the failed routing. In network, time to time changes are arise, due to this changes, the complexity of BGP for maintaining service availability is very challenging task. The Stefano Vissicchio et al. [53] shows that current system do not provides the guarantees for BGP reconfiguration with respective traffic disruptions and also for guaranteed packet loss. The [53] proposed a BGP framework that runs two separate BGP control plane in parallel, to enable the lossless reconfiguration. The first control plane stores initial configuration of routing table and second control plane store final configuration of routing table. The traffic forwarding has been taking place on the basis of final RIB, which reduces the packer loss. In many of the cases, after failure network have choose the alternate path for transmission but the current system utilize the disjoint end to end path efficiency. The source is unaware about the selection of alternate path. The Miao Xue et al. [32] have proposed a technique called source directed path diversity using which, sources can gives alternate paths to forward the traffic. In packet header, sources specify the tag called as source directed tag (SDT) that informs BGP routers for path selection. BGP routers on the basis of Source indication, forward the traffic independently on the indicated path. In order to address the link failure between autonomous systems LI Chun-xiu et al. [48] has proposed a fast reroute scheme by incorporating Software Defined Networking (SDN) with BGP called software defined autonomous system level fast rerouting (SD-FRR). By considering routing policies SD-FRR

aims to provide policy compliant path to protect forwarding of data locally, which avoids packet losses and efficiently improves the network availability. The above section described the detection of fault in the network. Detection of faults in early stage reduces the packet loss, which will improve the performance of network.

4. Instability In Inter-Domain Routing

The oscillation in the internet causes wastage of bandwidth, due to extra and unnecessary route hops. To reduce the oscillation in the BGP, Vivian Elliott et al. [34] used the explicit withdrawals technique. This technique will reduce the overall transaction traffic and path length. Route oscillation and path exploration reduces the performance of packet forwarding that will increase BGP instability. The existing solution cannot efficiently solve the BGP instability problem. Yang Richard Yang et al. [22] reported the results on efficiency and stability to achieve the traffic engineering objectives in interdomain routing when interactions among routing to multiple destinations cause instability in routing even if each route to destination has unique solution. Route selection problem is stable only if the interaction among the ISPs follows the set of interdomain traffic engineering guidelines; otherwise instability occurs in route selection process. The accidental activities such as failure, misconfiguration, route flapping, induced several BGP instabilities in the network lead to delays, loss of data and connectivity. Route flap damping (RFD) is considered to be a good approach that stabilizes the internet routing. But has a problem to wrongly suppress relatively stable routes for a longer duration of time [20], [40]. This technique introduced a complex interaction between BGP path exploration and how RFD algorithm finds route flaps. Sahoo et al. [12] consider the group processing update technique called as batch processing updates. When any update comes, router extracts the destination address from it and queue the update correctly, results in reducing the number of updates in the network. In this technique authors maintain a separate logical queue for each and every destination. The processing of all the updates takes place on the basis of destination. This technique is efficient for reducing updates. The Zhenhai Duan et al. [21] identify different BGP path exploration characteristics that follow events such as links failure or routes failure. The approach given has useful for distinguishing BGP route updates from route flapping at the time of BGP path exploration. The authors have developed a RFD+ algorithm that improves the stability of the internet routing. The main objective behind this approach is that, without affecting occasionally fail routes, it can correctly suppress persistent route flaps. Shivani deshpande et al. [23] proposed the BGP instability detection mechanism that can be executed by individual routers. The input data for detection of instability is BGP update messages received by routers from its neighbor. From this BGP update messages features (like AS path length, AS path edit distance) are extracted in every five minutes, this shows the change in topology. The GLR (Generalized Likelihood Ratio test), Segmentation boundary detection, Boundary position optimization algorithms are used to detect the changes. Today's internet routers are overcome by a number of BGP updates caused by events such as failure, session reset, and policy changes. Such events can delay routing convergence, which degrades the performance of networks in terms of jitter and delay sensitive application.

4.1. Dynamic Routing Decision

To analyze, predict and troubleshoot the behavior of network the ISPs have collects routing data. But this collected data is not complete and difficult to analyze manually. The Ashley Flavel et al. [41] combined the pieces of collected data to obtain a more complete view of network state. Also they have presented a technique for real time scenario, which dynamically determines the routing decision for all routers in the autonomous system.

The Qi Li, et al. [46] proposed a "stableBGP" that experimentally solve the BGP instability problem including path exploration and route oscillation. The "stableBGP" quickly stabilize the route selection problem by addressing the causes of route changes. The Zhang Jun, et al. [47] proposed a novel approach for quickly checking border gateway protocol route oscillation. The route update chain tag (RUCT) has been build to track the forwarding of update report and local routing library is used to record the change history of update report. The route oscillation can be found out by analyzing RUCT and local routing library. For checking oscillation time more efficiently, author's compares RUCT approach with relative preference (RP) approach and Token based approach. The experimental results show that RUCT needs

lesser time to check route oscillation than RP and Token based approach. In BGP guaranteed consistency is required between announce routing path and actual routing path. But in BGP no any mechanism that provides such guaranteed announcement. Some of the autonomous systems in interdomain routing could announce malicious information, which results in destroying stability of the internet.

The D. Papadimitriou, et al. [52] provides a stability metrics for stability of individual routes, stability computation for set of routing entries, most stable routes, and for best selected routes that described the stability properties of path vector protocol. Also they examine the effect of routing policies and instability on local routers. The duplicate announcements are the major BGP churn contributor analyzed by Ahmed Elmokshi, et al. [54] for BGP updates. Jian Jiang, et al. [49] proposed a verification of routing path mechanism to detect path inconsistency. In this technique sender and receiver autonomous systems generate routing evidence and communicate with each other to verify path, which is used to detect inconsistency in announced path. Instability in the network results in loss of packets, which in turn increases the latency and convergence time. Above section described the research work done by different researchers to reduce the convergence time by stabilizing the network.

5. Reducing Number of Updates

Wei Sun, et al. [24] propose the novel approach of differentiated processing in terms of BGP updates, which improve the routing convergence and reduces the routers load. Based on this approach the BGP updates are classified into two classes. Higher priority updates are processed sooner, while the lower priority updates are delayed to reduce router load and processing. The simulation result reduces the convergence time by 80% and having 30% fewer BGP updates. Mean Route Advertisement interval (MRAI) performs an important role in BGP convergence time. In the case of normal load, adaptive MRAI timers perform better for BGP updates. As soon as load is increased there may be a problem of flooding at routers and adaptive MRAI timer is not efficient. Adaptive MRAI timer fails to scale if the BGP Updates in the network are increasing. The convergence delay can be increase by increasing the failure in the internet. So for multiple failures, results in more convergence delay in the network. The Amit Sahoo et al. [39] presented a dynamic scheme that selects optimal MRAI value based on the size of the buffer messages at router, which reduces convergence delay for large network failure and keeping low value of delay for small failure. They also examined the batch processing scheme, which reduces the generation of invalid advertisement. These two techniques are designed to improve convergence delay in the network. Geoff Huston, et al. [25] proposed a Path Exploration Damping (PED) technique which reduces the volume of BGP update messages and decreases the average time required to restore reach-ability. They compare PED impact on convergence time with Mean route advertisement interval (MRAI), Route Flap Damping (RFD), and Withdrawal Rate Limiting (WRATE). From experimental results it was found that the total BGP announcement can decrease by up to 32%, and path exploration reduced by 77% compared with traditional MRAI approach. Rajvir Gill et al. [26] proposed the FLD-MRAI (Flexible Load Dispersing MRAI) algorithm that disperses the load in the network, which results in reducing the routers overhead. The authors focused on routing policies and their effects on number of updates, convergence time. The FLD-MRAI algorithm works in case of both high and normal loads. When degree of preference (DoP) chooses the shortest path, then FLD-MRAI believe this situation as normal load, and when DoP chooses the longest path then FLD-MRAI believe this situation as high load. The Mahesh Kumar and Shishir Kumar [13] proposed a technique that can keep the value of the mean route advertisement interval (MRAI) timer variable instead of keeping it constant [11]. The MRAI value depends upon the present network condition, due to this convergence time become relatively low and updating of network significantly faster. Andrey Sapegin, et al. [44] have analyzed a BGP updates from multiple observation points. They developed a method that classifies BGP updates into correlated or non-correlated updates. For forwarding and filtering of packets router requires lookup functionality. Nowadays there are serious challenges for update performance, memory efficiency and throughput. The Yanbiao Li et al. [45] presented a new parallel lookup model called split routing lookup model rather than looking for optimization techniques for traditional lookup model. In this model all the prefixes are split to produce redundancies, after that they are removed during information integration. The splitting of prefixes reduces routing updates also

this model use for parallel processing for lookup address. The above section discussed about reducing the routing updates, due to this congestion in the network will reduced, which in turns improve the convergence time.

6.   Conclusion

This study sheds light on the effect of multiple simultaneous failures between inter-AS routing. We found that, at first the BGP convergence time increases rapidly with the degree of failure before leveling off and going down. This means that multiple failures can lead to considerable longer periods of instability as compared to single failures. In this paper, we surveyed current efforts to enhance the convergence speed of the BGP protocol and eliminate the duplicate advertisements in its operation to improve its stability. The needs for fast convergence and stability in path vector routing protocols continue to challenge the researchers as the routing domains grow larger and more complex.

References

[1]   C Labovitz, R Wattenhofer, S Venkatachary, A Ahuja. *The impact of Internet policy and topology on delayed routing convergence.* In Proc. INFOCOM. 2001: 537-546.
[2]   C Labovitz, A Ahuja, A Bose, F Jahanianitz. *Delayed Internet routing convergence.* In Proc. SIGCOMM. 2000:175-187.
[3]   Yehuda Afek, Anat Bremler-Barr, Shemer Schwarz. Improved BGP Convergence via Ghost Flushing. *IEEE Journal on Selected Areas in Communications.* 2004; 22(10): 1933-1948.
[4]   Timothy G Griffin, Brian J Premore. *An experimental analysis of BGP convergence time.* In Proc. ICNP. 2001: 53-61.
[5]   D Pei, X Zhao, L Wang, D Massey, A Mankin, SF Wu, L Zhang. *Improving BGP convergence through consistency assertions.* In Proc. IEEE INFOCOM. 2002: 902-911.
[6]   Pei D, Zhang B, et al. An analysis of path-vector routing protocol convergence algorithms. Computer Networks. 2005.
[7]   www.ieee802.org/1/files/public/docs2007/au-jain-fecn-20070124.pdf
[8]   Mohammad Yanuar Hariyawan. Comparison Analysis of Recovery Mechanism at MPLS Network. International Journal of Electrical and Computer Engineering (IJECE). 2011; 1(2): 151-160.
[9]   Dan Pei, Beichuan Zhang, Daniel Massey, Lixia Zhang. An analysis of convergence delay in path vector routing protocols. *Computer Networks.* 2005; 398-421.
[10] Lixin Gao, Jennifer Rexford. Stable Internet Routing Without Global Co-ordination. *IEEE/ACM Transaction on Networking.* 2011; 9(6): 681-692.
[11] R Perlman. Interconnections. 2nd ed. Reading, MA: Addison-Wesley. 1999.
[12] Sahoo A, Kant K, Mohapatra P. *Improving BGP convergence delay for large-scale failures.* In Proceedings of the international conference on dependable systems and networks. 2006: 323-332.
[13] Mahesh Kumar, Shishir Kumar. Analyzing and Improving Network Availability in Inter-domain Routing. Springer Science+Business Media New York 2013. 2013.
[14] TG Griffin, GT Wilfong. *A safe path vector protocol.* In Proc. INFOCOM. 2000.
[15] CT Ee, V Ramachandran, BG Chun, K Lakshminarayanan, S Shenker. *Resolving inter-domain policy disputes.* In Proc. SIG-COMM. 2007.
[16] TG Griffin, JL Sobrinho. *Metarouting.* In Proc. SIGCOMM. 2005.
[17] Luca Cittadini, Massimo Rimondini, Stefano Vissicchio, Matteo Corea, Giuseppe Di Battista. From Theory to Practice: Efficiently Checking BGP Configurations for Guaranteed Convergence. *IEEE Transactions on Network and Service Management.* 2011; 8(4).
[18] Nick Feamster, Hari Balakrishnan. *Detect BGP Configuration Faults with Static Analysis.* Proceeding NSDI'05 Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation. 2005; 2: 43-56.
[19] Renata Teixeira, Aman Shaikh, Tim Griffin, Jennifer Rexford. Damping BGP route flaps. *Journal IEEE/ACM Transactions on Networking.* 2008; 16(6): 1295-1307.
[20] Zhuoqing Morley Mao, Ramesh Govindan, George Varghese, Randy H Katz. *Route Flap Damping Exacerbates Internet Routing Convergence.* Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications. 2002: 221-233.
[21] Zhenhai Duan, Chandrashekar J, Krasky J, Kuai Xu. Damping BGP Route Flaps. *Journal of IEEE Communication and Networks.* 2007; 9(4): 490-498.
[22] Yang Richard Yang, Haiyong Xie, Hao Wang, Avi Silberschatz, Arvind Krishnamurthy, Yanbin Liu, Li Erran Li. On Route Selection for Inter-domain Traffic Engineering. *IEEE Network.* 2005: 20-27.
[23] Shivani Deshpande, Marina Thottan, TinKamHo, Biplab Sikdar. An Online Mechanism for BGP Instability Detection and Analysis. *IEEE Transactions on Computers.* 2009; 58(11): 1470-1484.

[24] Wei Sun, Zhuoqing Morley Mao, Kang G Shin. *Differentiated BGP Update Processing for Improved Routing Convergence.* IEEE Conference Publication, ICNP Network Protocol. 2006.

[25] Geoff Huston, Mattia Rossi, Grenville Armitage. A Technique for Reducing BGP Update Announcements through Path Exploration Damping. *IEEE Journal on Selected Areas in Communications.* 2010; 28(8): 1271-1286.

[26] Rajvir Gill, Ravinder Paul, Ljiljana Trajkovic. *Effect of MRAI Timers and Routing Policies on BGP Convergence Times.* In proc. IPCCC, IEEE 31st International Conference. 2012.

[27] Wang Feng, Qiu Jian, Gao Lixin, Wang Jia. On understanding transient interdomain routing failures. *IEEE/ACM Trans Network.* 2009; 17(3): 740-751.

[28] Wang Feng, Gao Lixin. *Path diversity aware interdomain routing.* In: IEEE INFOCOM 2009. 2009: 307-315.

[29] Chaitanya K Krishna, Kishore Ch Ravi. An approach to shortest path technique for BGP using OSPF. *International Journal Computer Science and Information Technology.* 2010; 1(5): 389-391.

[30] Wang Yi, Schapira Michael, Rexford Jennifer. *Neighbor-specific BGP: more flexible routing policies while improving global stability.* In: METRICS measurement and modeling of computer systems. 2009: 217-228.

[31] Mahesh Kumar, Shishir Kumar. An approach to stabilize interdomain routing protocol after failure. *Computers and Electrical Engineering.* 2013; 39: 237-245.

[32] Miao Xue, Gang Fu, Ruitao Ma, Longshe Huo. Source-Directed Path Diversity in the Interdomain Routing. *Journal of Networks.* 2014; 9(12).

[33] Jyh-haw Yeh, Wei Zhang, Wen-chen Hu, Chung-wei Lee. Design and simulation of a supplemental protocol for BGP. *Science Direct, Elsevier, Computer Networks.* 2005; 49: 172-200.

[34] Vivian Elliott, Kenneth J Christensen. Characterizing and reducing route oscillations in the Internet. *Elsevier Science, Computer Communications.* 2003; 26: 143-153.

[35] Li Xiao, Guanghui He, Klara Nahrstedt. BGP session lifetime modeling in congested networks. *Science Direct, Elsevier, Computer Network.* 2006; 50: 3315-3333.

[36] B Quoitina, S Tandela, S Uhligb, O Bonaventure. Interdomain traffic engineering with redistribution communities. *Computer Communications.* 2004; 27: 355-363.

[37] Osamu Akashia, Kensuke Fukud, Toshio Hirotsu, Toshiharu Sugawara. Policy-based BGP-control architecture for inter-AS routing adjustment. *Computer Communications.* 2008; 31: 2996-3002.

[38] Taoyu Lia, Yuncheng Zhu, KeXu, Maoke Chen. Performance model and evaluation on geographic-based routing. *Computer Communications.* 2009; 32: 343-348.

[39] Amit Sahoo, Krishna Kant, Prasant Mohapatra. BGP convergence delay after multiple simultaneous router failures: Characterization and solutions. *Computer Communications.* 2009; 32: 1207-1218.

[40] http://en.wikipedia.org/wiki/Route_flapping.

[41] Ashley Flavel, Jeremy McMahon, Aman Shaikh, Matthew Roughan, Nigel Bean. BGP route prediction within ISPs. *Computer Communications.* 2010; 33: 1180-1190.

[42] Huaming Guo, Wei Su, Hongke Zhang, Sy-Yen Kuo. On the convergence condition and convergence time of BGP. *Computer Communications.* 2011; 34: 192-199.

[43] Martin O. Nicholes, Chen-Nee Chuah, S Felix Wu, Biswanath Mukherjee. Inter-domain collaborative routing (IDCR): Server selection for optimal client performance. *Computer Communications.* 2011; 34: 1798-1809.

[44] Andrey Sapegin, Steve Uhlig. On the extent of correlation in BGP updates in the Internet and what it tells us about locality of BGP routing events. *Computer Communications.* 2013; 36: 1592-1605.

[45] Yanbiao Li, Dafang Zhang, Kun Huang, Dacheng He, Weiping Long. A memory-efficient parallel routing lookup model with fast updates. *Computer Communications.* 2014; 38: 60-71.

[46] Qi Li, Mingwei Xua, Jianping Wu, Patrick PC Lee, Dah Ming Chiu. Toward a practical approach for BGP stability with root cause check. *Journal of Parallel Distributed Computing.* 2011; 71: 1098-1110.

[47] ZHANG Jun, HU Ziying, ZHANG Tao. Update Chain-based Approach for Checking Route Oscillation of BGP. *Chinese Journal of Aeronautics.* 2011; 24: 202-209.

[48] LI Chun-xiu, LI Xin, LI Ke, ZHANG Hong, SHI Yu-long, CHEN Shan-zhi. Toward software defined AS-level fast rerouting. *The Journal of China Universities of Posts and Telecommunications.* 2014; 21(6): 100-108.

[49] Jian Jiang, Wei Li, Junzhou Luo, Jing Tan. A network accountability based verification mechanism for detecting inter-domain routing path inconsistency. *Journal of Network and Computer Applications.* 2013; 36: 1671-1683.

[50] Alejandro Ruiz-Rivera, Kwan-Wu Chin, Sieteng Soh. A novel framework to mitigate the negative impacts of green techniques on BGP. *Journal of Network and Computer Applications.* 2015; 48: 22-34.

[51] Dan Pei, Matt Azuma, Dan Massey, Lixia Zhang. BGP-RCN: improving BGP convergence through root cause notification. *Computer Networks.* 2006; 48: 175-194.

[52] D Papadimitriou, A Cabellos. Analysis of Path-vector Routing Stability. Provided by Technical University of Catalania. 2012.

[53] Stefano Vissicchio, Laurent Vanbever, Cristel Pelsser, Luca Cittadini, Pierre Francois, Olivier Bonaventure. Improving Network Agility With Seamless BGP Reconfigurations. *IEEE/ACM TRANSACTIONS ON NETWORKING*. 2013; 21(3): 990-1002.

[54] Ahmed Elmokashfi, Amund Kvalbein, Constantine Dovrolis. BGP Churn Evolution: A Perspective from the Core. *IEEE/ACM TRANSACTIONS ON NETWORKING.* 2013; 20(2): 571-583.

[55] Chengchen Hu, Kai Chen, Yan Chen, Bin Liu, Athanasios V Vasilakos. A Measurement Study onPotential Inter-Domain Routing Diversity. *IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT.* 2012; 9(3): 268-278.

[56] Y Rekhter, T Li, S Hares. RFC 4271 A Border Gateway Protocol 4 (BGP-4). *IETF.* 2006.

[57] Aleksandar Cvjeti´, Aleksandra Smiljani´. Improving BGP Protocol to Advertise Multiple Routes for the Same Destination Prefix. *IEEE COMMUNICATIONS LETTERS.* 2014; 18(1).