Improvement of Border Gateway Protocol Against Failure on Autonomous Systems

Nasser solayman[1], Ayman EL-SAYED[2], and Mohammed Badawy[3]

**[1]Computer Science & Eng. Dept., Faculty of Electronic Eng.,
Menoufia University, Menouf 32952, Egypt**

**[2]Computer Science & Eng. Dept., Faculty of Electronic Eng.,
Menoufia University, Menouf 32952, Egypt**

**[3]Computer Science & Eng. Dept., Faculty of Electronic Eng.,
Menoufia University, Menouf 32952, Egypt**

Abstract

Border Gateway Protocol (BGP) is used for routing among autonomous systems, its main advantage among the other routing protocols is its stability and its ability to maintain and contain large number of updates in its routing table, and so this is very important as its main usage of it is routing in the internet. These autonomous systems create a large number of updates that cannot be maintained/handled by other routing protocol except BGP. BGP has a big problem which is convergence delay due to large number of updates that may reach to minutes in cases of topology failure or problems, also it need to high processing in the CPU memory which may lead to a freezing node in lot of cases. So it's so important to pay more work and attention to reduce these effects that lead to routing instability and nodes freeze. A lot of studied work on solving this problem create a dynamic model change in the BGP routing MRAI (minimum route advertisement interval) according to the network size. This MRAI is a main functional factor to decrease the convergence delay in much networks, but no one study the effect of many flapping node (neighbor) in a topology on the convergence delay and number of created messages which recreated more and more every time the flapping happened. In this paper, the effect of flapping node on different network sizes with various sized failure studied and proposed a solution with good performance in less processing time and convergence delay.

Keywords: *Border Gateway Protocol, Autonomous system.*

1. Introduction

BGP [1, 2, 3, 4, 5, 6] unlike the other routing protocols is an exterior gateway protocol used between autonomous systems and is a path vector routing protocol. After you enable BGP on your router you need to advertise your routes in the routing protocol to be handled in the routing table to be exchanged with others (injection/advertisement). [7] offers a flexible BGP injector (mBGPinjector) that advertise both online (real-time) and offline advertisements to BGP neighbors, mBGP can handle the dynamic changes in BGP configuration like BGP neighbor down and withdrawing the routes. Sure we need to control the routes in both direction (incoming and outgoing). If you need to control routes that will be advertised or received you have two options, the first one by not advertising it and this will control your routes only, the second option which is the best practice for both direction is to configure a policy to control and filter both incoming and outgoing traffic (routes). [8] Describes the routing policy on both directions input or output direction, applying it and making the filtration based on the preconfigured policy. [9] tires to make a prediction for the prefixes (networks) the will be advertised between BGP neighbors because as a reason for the BGP routing table growth due to large amount of updates (advertisements) there will be instability in routes selection and much time to get the best route, so they propose a solution for prefixes prediction through studying the relation between them and tracing many different networks traffic (prefixes) they get sets of prefixes (networks) with both good volume coverage and stability in time. [10] Also tries to make a stable BGP route selection by increasing the availability of routes and propose and they propose a new approach, Stable Route Selection (SRS), which uses a flexible route selection to enhance stability without losing availability and with control in amount of deviation. the internet is a collection of thousands different autonomous systems which are using the BGP for the inter-domain routing between them [11]. With this large growth in the number of AS there is must be a huge amount of advertisements due to topology changes (adding new network or removing it or route flapping) and sure a modification in the BGP core to handle the updates between them and also deal with this large amount of changes. Exchange of loop-free routing information is guaranteed. Every routing advertisement received must be go through several steps [12.13,14], first it will path through the ingress filter then compared to the routes existing in the routing table, after that it will be selected and added to the routing table of the node. Before advertisement to other nodes it must be filtered by egress filter and its policies must be applied on it (Figure 1. BGP operation).

To guarantee loop free path selection, BGP constructs a graph of autonomous systems based on the information exchanged between BGP neighbors. BGP views the whole internetwork as a graph, or tree, of autonomous systems. The collection of path information is expressed as a sequence of AS numbers called the AS Path. This sequence forms a route to reach a specific destination. Each router has the routing table which contains all the available routes to

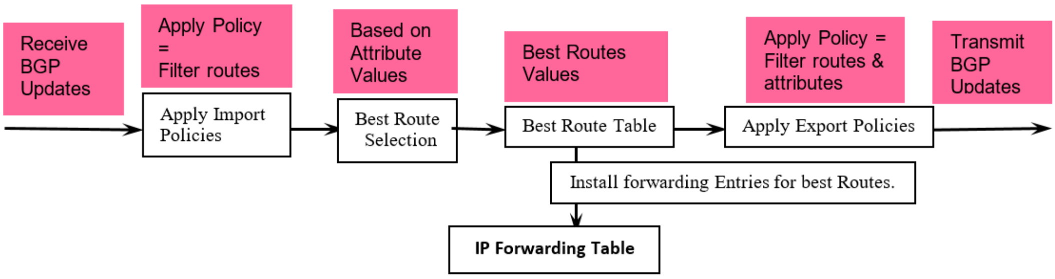


Fig. 1 BGP operations.

each destination, then the best routes will be selected after applying all the filters and policies on them and then deduce the best route to each destination in the topology [12, 13, 14] which is then advertised to its neighbors. BGP makes routing decisions based on network policies, BGP does not show the details of topologies within each AS. BGP sees only a tree of autonomous systems. TCP connections must also be negotiated between them before updates can be exchanged. Therefore, BGP inherits those reliable, connection-oriented properties from TCP. BGP database consists of a List of BGP neighbors, BGP table (forwarding database), List of all networks learned from each neighbor, can contain multiple paths to destination networks, Contains BGP attributes for each path and finally IP routing table (List of best paths to destination networks). Due to topology changes and route selection as a best route or a route ejection after withdrawals. There will be a recognized delay. These actions lead to long routing convergence time and the router’s CPU is highly utilized and may be freeze due to high BGP Routing Updates (messages), High convergence times which causing delay for reaching the destination will be a reason for loosing packets an increasing the time to reach the route for unavailable destination. Moreover, high router CPU utilization due to processing these large scale of messages will result in disruption to other tasks and misprocessing to them like SNMP and Keep alive messages, also in high CPU utilization can make the router freeze (crash) and cannot complete its usual processing tasks. A big sized failure and big BGP topology change will cause in flooding large number of updates and other needed messages (keep alive and BGP discovery ones) which will result in starting the BGP surviving process (try to find a new route for the withdrawal one) which by the way will result in flooding large number of messages that will increase the convergence delay and disabling large number of routers (freeze) due to processing these large number of updates [14, 15]. Also as the topology size increase as the effect of any change will be very big on all the router within this topology and will case instability within this AS and other Connected ASes. Nowadays the communication networks are the main method for communicating between any company branches or to allow connection to the internet through the service provider. Most of this company network connections must be covered in crises with a short convergence delay time which is very needed specially in the financial companies and bank as any data lose due to this convergence will lead to financial lose also, so it’s so important to understand the BGP (internet protocol) behavior and solve its issues as much as we can.[12] Propose a method for BGP routing advertisement by away of parallel processing for BGP routing advertisements with the pipeline and multithreading technologies which provide enhancement to the efficiency of routing advertisement processing.

BGP problem can be defined in two issues, the first one is the high convergence delay that the node taken to be adapted with the new changes or updates its routing table. The second issue is the high processing of the node's CPU (router) due to large numbers of updates (messages). The large number of update's message is caused by changing the topology. So we have to reduce or overcome the effect of the topology changes, which will result in reducing the large number of updates (messages) and so reducing the CPU processing overhead on the updates. In this paper, the proposed solution is presented to decrease the number of updates and the processing of CPU's routers.

The rest of the paper is organized as follows: Related work is described in section 2, in which the previous proposals are described. In Section 3, our proposal is depicted. Performance evaluation is given in Section 4. Finally, the paper is concluded in section 5.

2. Related Work

Many studies done before to study and solve the recovery issues and characteristics of the BGP as it’s the main routing protocol used today with Internet autonomous systems (ASes). As a result of these studies its was found that the convergence delay for a router to recover from a failed route and to find an alternative path for the failed one can be 3 minutes in 30% of the cases and can reach 15 minutes in other cases, which is very difficult to stand and not accepted with current environment [15, 16, 17, 18, 19]. Several studies have been made before o calculate the best and suitable convergence delay for the BGP but it lacked the simplicity and did not depend on the current complex multi ASes network with a multi links failure [15, 16, 17]. Previous studies [14, 17, 18] found that the minimum route advertisement interval is the main factor affecting the convergence delay of the BGP and any change in it will lead to a significant change in the BGP convergence delay [20, 21, 22]. The MRAI is the time between the router began sending an update to a destination through a neighbor and be able to send another update to the same destination through the same neighbor, each router has to wait at least this time before be able to send another update to the same neighbor. There is a maintained timer for this operation start and end with the two boundaries of sending update and try to send another one. Each router has one neighbor or more and so it must have a separate timer for each neighbor which control the updates between them.

Griffin and Premore [16] found that MRAI value depend on the size of the network and number of ASes exchanging updates with it, but they studied the effect of MRAI on a simple network not a complex one like we have nowadays. They found that by increasing the MRAI, the convergence delay of exchanging updates is increasing linearly. They found that the best default value suitable for many ASes is 30s. One of the best factors effecting convergence delay is the BGP updates generated due to topology changes which increase more and more and increasing while the network size increases. MRAI timer duration cannot be high or low as discussed before, as if MRAI is high the sending router will wait and cannot send updates till MRAI timer ends although the peer router is idle and not processing any more updates from the sending one, so the router will wait a time more than the time of the MRAI time and that's enough to make a large convergence delay within a network. And because we are speaking about a large numbers of routers within the AS and the connected ones. If the MRAI time is short so any update received will sent faster and will cause a fast change in the network (not needed and not practical) and we will reach with the CPU to process a large numbers of updates that not usable within our network and lead to processing overhead on the router and thus it will cause a convergence delay. So from all the above we can deduce that the MRAI depend on the size of the network and topology changes and we can't make the MRAI so high or so short.

A. Sahoo, et al. [21] and [22] studied the Impact of the route processing on the convergence delay and the factors that had a big effect on the BGP convergence delay and they found that minimum route advertisement interval (MRAI) and number of generated messages and the relation between the network size and the convergence delay. Also they looked at the characteristics of the network topology and its effect on the BGP convergence delay. Sure now we know that as the network size and topology increases as the number of the generated messages increase and so we need a much router CPU processing time and size for these large of updates, to be analyzed and filtered and so routed with the right way, all of this sure will increase the convergence delay in recovering from a fail status or sending updates in a changing network topology that have redundant links. For the MRAI the minimum route advertisement interval which control the time in between the router send an update for a specified destination to peers and try to send another updates to the same peers they modify this timer by making a dynamically changing scheme to this MRAI which always changes according to network size. By this solution they reduced the convergence delay by 3 times without this scheme which is a great success by this solution.

3. Our proposed

Our proposed solution in a brief can be said in these words (do not accept updates from flapping neighbor (Link)), it is how to handle updates from flapping neighbor which caused from a flapping link, as it's not important that we receive updates from flapping neighbor and then withdraw these updates and then receive it again and then withdraw it and then repeat it for a time of while the link is flapping, and make the CPU busy in processing these unused updates. There is no benefit from receiving updates for routes that we are not able to use it. From all the previous studies, we can deduce that, no clear method of how to reduce the effect of the topology changes in network, but all the tries done before were to handle these updates by dynamically change the MRAI according to network size [21]. They reduced the effect of these updates but they did not isolate it, especially that these updates have no need to be processed. In this work, the effect of topology changes is reduced by decreasing of in number of updates (messages) that causing a convergence delay and high CPU processing. Both the convergence delay and the CPU processing may lead to a freezing node (router), or reach to a degree we can neglect it [22, 23].

We will work on two different topologies and study the BGP behavior (delay and Number of updates) during different topology changes within 10 Minutes.

Before we apply our solution we want to focus on very important thing about BGP methodology and make it clear about how it operates:

- BGP Databases:
- Neighbors table: List of BGP neighbors
- BGP table (forwarding database)
    - ➢ List of all networks learned from each neighbor
    - ➢ Can contain multiple paths to destination networks.
    - ➢ Contains BGP attributes for each path
- IP routing table: List of best paths to destination networks.

When BGP neighbors first establish a connection, they exchange all candidate BGP routes. After this initial exchange, incremental updates are sent as network information changes, the information for network reachability can change, such as when a route becomes unreachable or a better path becomes available. BGP informs its neighbors of this by withdrawing the invalid routes and injecting the new routing information. Withdrawn routes are part of the update message.

BGP defines the following message types:

- Open: Includes hold time and BGP router ID
- Keep alive
- Update
    - ▪ Information for one path only (no multiple path)
    - ▪ Includes path attributes and networks
- Notification
    - ▪ When error is detected
    - ▪ BGP connection closed after message is sent

When establishing a BGP session, BGP goes through the following states:

- Idle: Router is searching routing table to see whether a route exists to reach the neighbor.
- Connect: Router found a route to the neighbor and has completed the three-way TCP handshake.
- Open sent: Open message sent, with the parameters for the BGP session.
- Open confirm: Router received agreement on the parameters for establishing session.
- Established: Peering is established; routing begins.

First, we will work on a network topology that consists of five Autonomous systems, and check our solution results on many updates (messages), each autonomous system represented with one router with different subnet. We will see the effect of the topology changes (flapping links) on our topology for different size failures. We will then apply our solution on it and see the results on enhancing our metrics (convergence delay, amount of update's messages).

Second we will work on a large network topology that consists of 32 Autonomous systems and apply our so it, our solution will show more effect on the performance of the network. The flow chart of our proposal is shown in Figure 2.

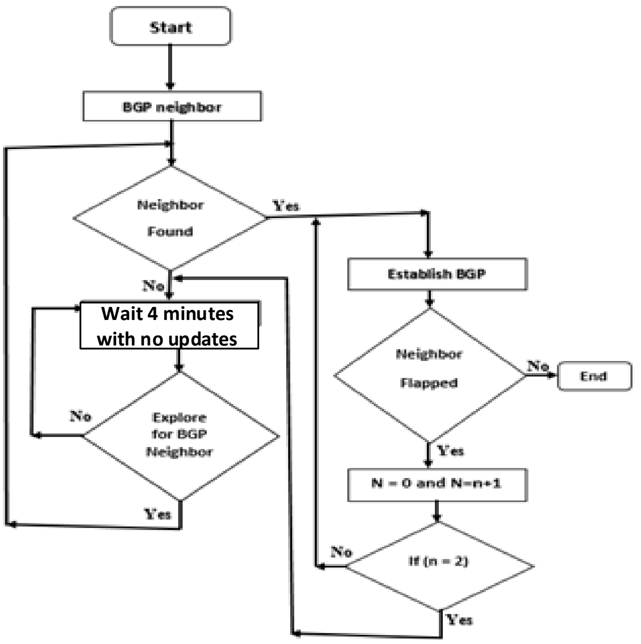


Fig. 2. Flow chart of our proposal.

4. Performance Evaluation

4.1 Simulation Setup

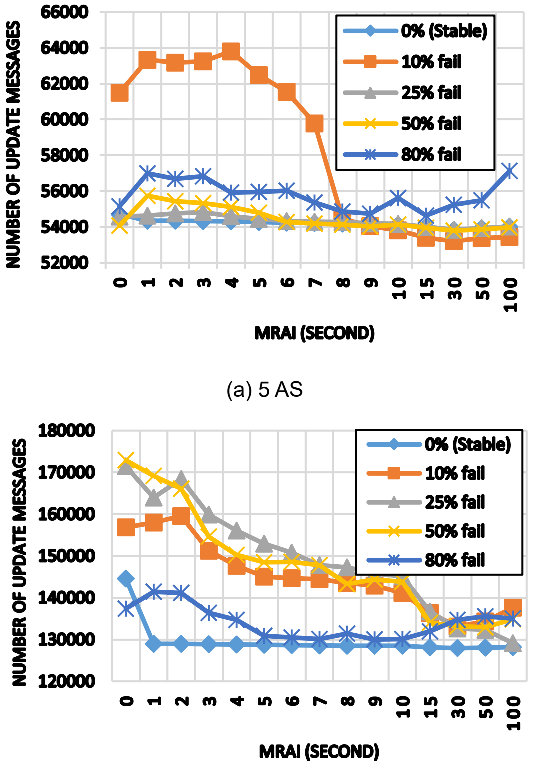
We will use the SSFNet [24], the best simulator can be used in BGP research which allow a flexible simulation with dig deeper details in BGP cor. We will use a topology that contain 5 autonomous systems and see the stable links behavior, then check the effect of topology changes (flapping links) on different sized failure topologies (10%fail, 25%fail, 50%fail, 80%fail) for different MRAI values and then apply our solution on it and see the results and also we will use another topology of 32 ASes and apply our solution on it with the same strategy and same steps.

4.2 Evaluation metrics

Number of updates (messages): large number of updates leads to high CPU utilization due to processing overhead on these large number of updates. Lower number of updates meaning better dealing with topology changes.
Convergence delay: Time taken by the routing protocol to recover from topology changes including flapping links and reroute over another link or withdraw this route and inform neighbors and updating all the routing table. Lower convergence delay meaning better dealing with topology changes.

4.3 Results

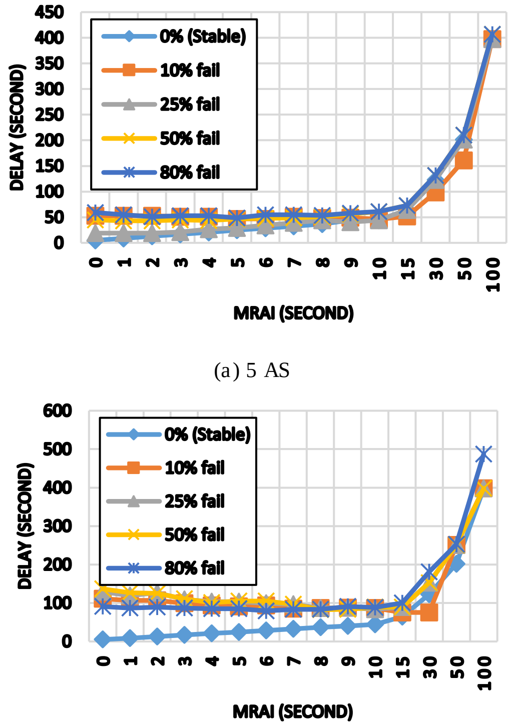
First of all, the impact of failure on the number of update messages and the delay is described in both Figure 3 and 4 respectively. Figure 3 depicts the number of update messages versus various MRAI values with both no failure and 10%, 25%, 50%, 80% failure and with different number of ASs. Figure 4 shows the delay versus the different MRAI values with the same parameters.



(a) 5 AS

(b) 32 AS

Fig. 3 Number of Updates Messages versus MRAI with 0 % (stable), 10%, 25%, 50%, and 80% failure.



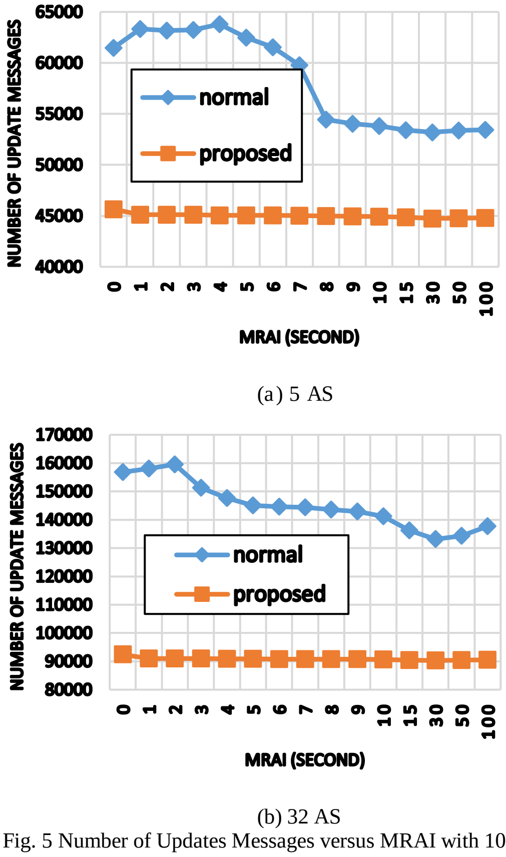
(a) 5 AS

(b) 32 AS

Fig. 4 Convergence delay versus MRAI with 0 % (stable), 10%, 25%, 50%, and 80% failure.

We recognize that for different size failure the number of messages increased, especially at 10% failure, for different sized failure we must know that we lost the flapping ASes, so the number of update messages is decreased, plus we have to know that there is up normal behavior resulted from these flapping links that we cannot imagine or count. For the convergence delay we determine that it's always higher than the stable situation and the most important point is at MRAI=0. At this time, the convergence delay would reach the zero but it didn't because of the behavior of the flapping links.

In order to evaluate our proposed, different failures size (10%, 25%, 50%, and 80% failure) and various number of Ass (5 ASs and 32 ASs) are applied in both normal case and our proposed case. Figure 5, 7, 9, and 11 depict number of update messages versus MRAI with 10%, 25%, 50%, and 80% failure respectively. Figure 6, 8, 10, and 12 show the behavior of convergence delay versus MRAI for normal and our proposed cases for 10%, 25%, 50%, and 80% failure respectively.



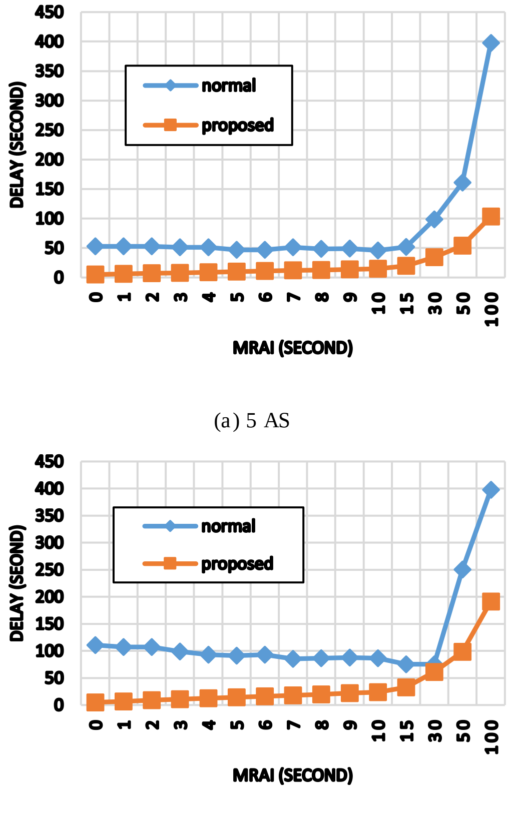
(a) 5 AS

(b) 32 AS

Fig. 5 Number of Updates Messages versus MRAI with 10% failure.

In 10%, 25%, and 50% failure, it noted that the little flapping links (neighbors) causes a high number of updated messages. As these updates messages resulted from these flapping links will be updated through large number of ASes which still up and flooding its routing table updates. In 80% failure, it noted that there are large number of lost ASes that become down. So the number of updated messages will be lower than any other sized failure. The flapping links causes a high number of updated messages that resulted from these flapping links. The flapping links will be updated through large number of ASes which still up and then flooding its routing table updates. The convergence delay is high as the router must wait a time of MRAI to resend the next update and also time generated from huge number of updates due to flapping links causing CPU high processing delay and may be freeze.

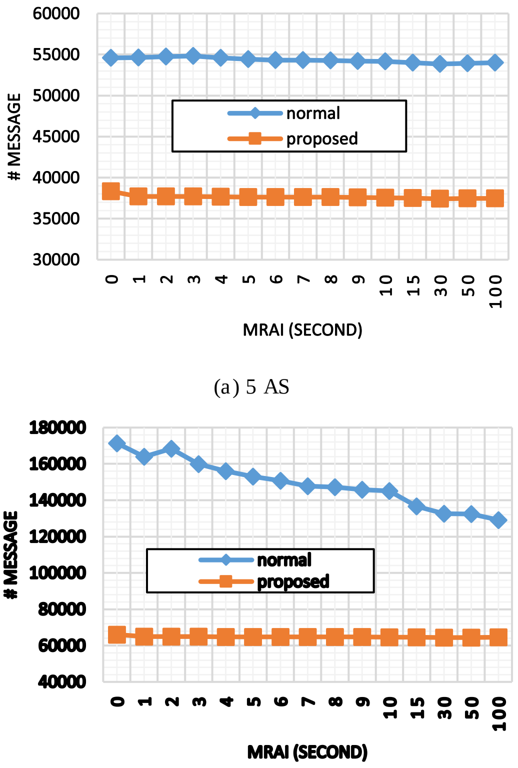
Our proposal results that there is a high modification on both number of updates and convergence delay in different failures. Also all the convergence delays for different failures starts from zero and under the stable topology line.



(a) 5 AS

(b) 32 AS

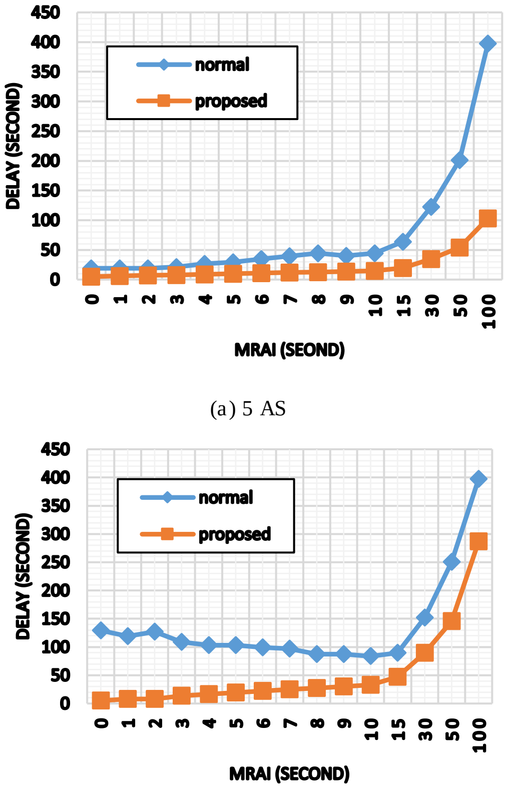
Fig. 6 Convergence delay versus MRAI with 10% failure.



(a) 5 AS

(b) 32 AS

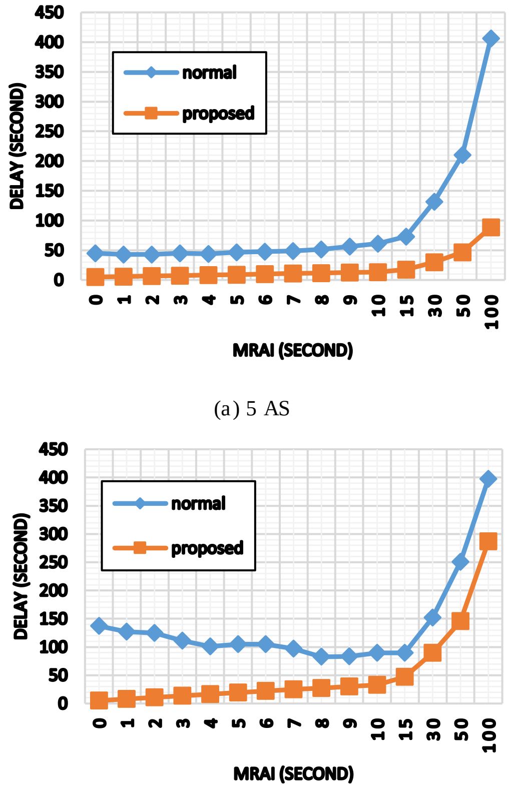
Fig.7 Number of Updates Messages versus MRAI with 25% failure.



(a) 5 AS

(b) 32 AS

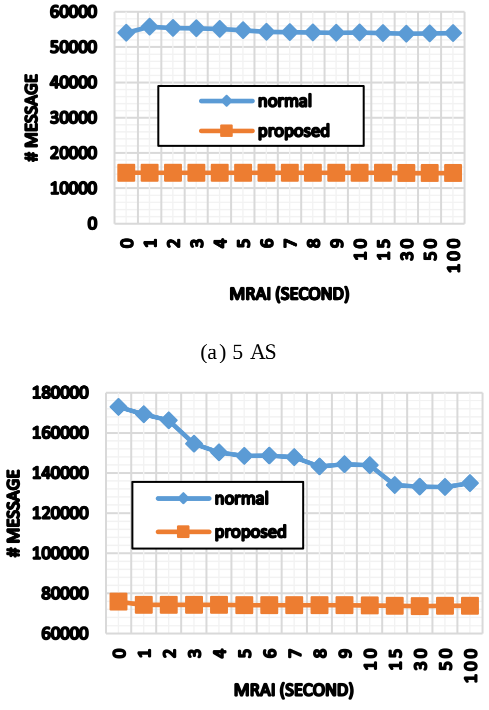
Fig. 8 Convergence delay versus MRAI with 25% failure.



(a) 5 AS

(b) 32 AS

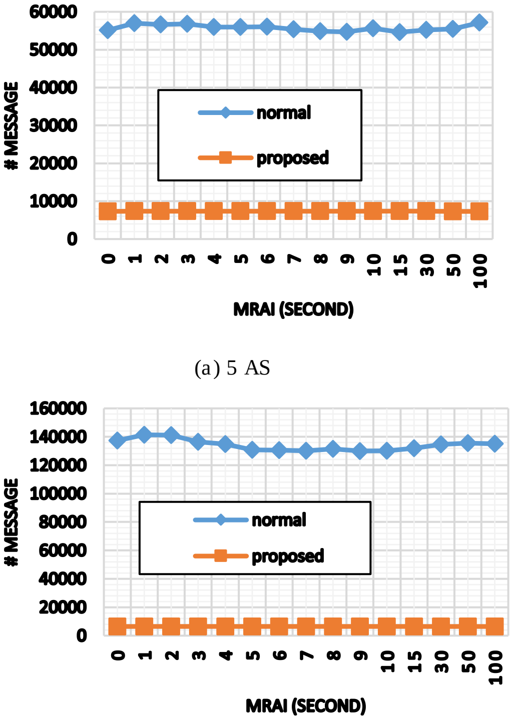
Fig. 10 Convergence delay versus MRAI with 50% failure.



(a) 5 AS

(b) 32 AS

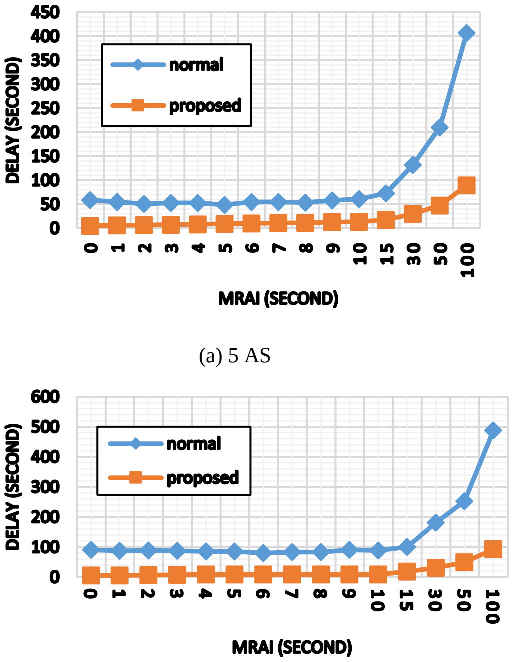
Fig. 9 Number of Updates Messages versus MRAI with 50% failure.



(a) 5 AS

(b) 32 AS

Fig. 11 Number of Updates Messages versus MRAI with 80% failure.



(a) 5 AS

(b) 32 AS

Fig. 12 Convergence delay versus MRAI with 80% failure.

4.4 Discussion

For each neighbor within the topology try to send updates to its neighbor which will be advertised to all the other neighbors, a session must be established between each neighbor and another, this session establishment is done by open a TCP connection (specially port 179) and this acquire lot of messages (not BGP updates) to be sent like ACK messages, keep alive messages, session parameters, notification messages and this session established when start a new MRAI timer.

So if the MRAI is small a lot of session establishment messages is sent many times which will consumes CPU processing, but on the other side there is no convergence delay (may be reaches zero) in stable network topology as the router doesn't have to wait long MRAI to send the update (topology changes) to its neighbor.

For MRAI is long so you have less Session establishment messages and also less BGP updates for a flapping topology, and a high convergence delay as you have to wait this long period of MRAI to send your next update and this is clear for stable and different sized failure.

For different sized failure network, we determine that although the MRAI is zero, the convergence delay is not zero like the stable network, but it's always has a value resulted from topology change.

Different sized failure topology has a no formal distribution of updates due to un-normal network activity resulted from flapping links, also we can recognize as we have more size fail topology you have less generated messages because we lose the flapping ASes within this topology, we can recognize a highly updates is generated in 10 % fail as little node are flapping and a more ASes is sending updated.

Convergence delay is increasing linearly and start to go exponential after MRAI=30 which is remarkable also has a low number of generated updated, so in real life we put MRAI=30 for better convergence delay and updated messages during all supposed topology changes.

After applying our proposal on different sized failure network topology we can determine that we reached the behavior of 0 % fail for the two factors (updates, convergence delay) and also the convergence delay is equal to zero at MRAI=0, also in the big sized failure topology we found a lower updates generated as we have isolated the unnecessary updated resulted from the flapping neighbors.

5 Conclusion

The behavior of the flapping neighbor (link) will lead to large amount of update messages. that will lead to instability in our network and will lead to CPU high utilization due to processing these large number of updates messages, there is no need to receive updates from a flapping neighbor as it will be with no benefit and lead to unnecessary CPU utilization. so, by disabling this flapping neighbor, we save the CPU processing and the unneeded updates (messages), and then we have a less processing time and convergence delay.

References

[1] Stewart, J.W.: BGP4: Inter-Domain Routing in the Internet. Addison-Wesley (1998).

[2] A. Lutu, M. Bagnulo, C. Pelsser, O. Maennel and J. Cid-Sueiro, "The BGP Visibility Toolkit: Detecting Anomalous Internet Routing Behavior," in IEEE/ACM Transactions on Networking, vol. 24, no. 2, pp. 1237-1250, April 2016.

[3] S. Papadopoulos, K. Moustakas, A. Drosou and D. Tzovaras, "Border gateway protocol graph: detecting and visualising internet routing anomalies," in IET Information Security, vol. 10, no. 3, pp. 125-133, 5 2016.

[4] S. Frey et al., "It Bends but Would It Break? Topological Analysis of BGP Infrastructures in Europe," 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, 2016, pp. 423-438.

[5] M. Ćosović, S. Obradović and L. Trajković, "Performance evaluation of BGP anomaly classifiers," Digital Information, Networking, and Wireless Communications (DINWC), 2015 Third International Conference on, Moscow, 2015, pp. 115-120.

[6] M. Chen, M. Xu, X. Song and Y. Yang, "Towards identifying Large-scale BGP Events," Local Computer Networks (LCN), 2015 IEEE 40th Conference on, Clearwater Beach, FL, 2015, pp. 165-168.

[7] J. Pan and Y. Liu, "A Flexible and Lightweight BGP Route Injector to Multiple Peers," Network Computing and Applications (NCA), 2015 IEEE 14th International Symposium on, Cambridge, MA, 2015, pp. 147-150.

[8] M. Caesar and J. Rexford, "BGP routing policies in ISP networks," in IEEE Network, vol. 19, no. 6, pp. 5-11, Nov.-Dec. 2005.

[9] W. Shao, L. Iannone, J. L. Rougier, F. Devienne and M. Viste, "Scalable BGP prefix selection for effective inter-domain traffic engineering," NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, Turkey, 2016, pp. 315-323.

[10] P. B. Godfrey, M. Caesar, I. Haken, Y. Singer, S. Shenker and I. Stoica, "Stabilizing Route Selection in BGP," in IEEE/ACM Transactions on Networking, vol. 23, no. 1, pp. 282-299, Feb. 2015.

[11] Huston, G.: Analyzing the Internet's BGP Routing Table. Cisco Internet Protocol Journal (2001).

https://doi.org/10.20943/01201703.1421

[12] Lina Ding, Xingwei Wang, Fuliang Li and Min Huang, "A parallel processing method for Border Gateway Protocol UPDATE messages," Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on, Zhangjiajie, 2015, pp. 2044-2048.

[13] Halabi, S., McPherson, D.: Internet Routing Architectures. Second edn. Cisco Press (2001)

[14] A. Sahoo, K. Kant, and P. Mohapatra, “Characterization of Istanbul, Turkey, Jun. 11–15, 2006.

[15] C. Labovitz, A. Ahuja, et al., “The Impact of Internet Policy and Topology on Delayed Routing Convergence,” in Proc. IEEE INFOCOM 2001, vol. 1, Anchorage, Alaska, Apr. 22—26, 2001, pp. 537–546.

[16] T.G. Griffin and B.J. Premore, “An experimental analysis of BGP convergence time,” in Proc. ICNP 2001, Riverside, California, Nov. 11–14, 2001, pp. 53–61.

[17] Dan Pei, B. Zhang, et al., “An analysis of convergence delay in path vector routing protocols,” Computer Networks, vol. 30, no. 3, Feb. 2006, pp. 398–421.

[18] D. Obradovic, “Real-time Model and Convergence Time of BGP,” in Proc. IEEE INFOCOM 2002, vol. 2, New York, Jun. 23–27, 2002, pp. 893–901.

[19] G. Siganos and M. Faloutsos, “Analyzing BGP Policies: Methodology and Tool,” in Proc. IEEE INFOCOM 2004, vol. 3, Hong Kong, Mar. 7–11, 2004, pp. 1640-1651.

[20] Labovitz, C., Ahuja, et al., “Delayed internet routing convergence,” in Proc. ACM SIGCOMM 2000, Stockholm, Sweden, Aug. 28–Sep. 1, 2000, pp. 175–187.

[21] Sahoo, A.; Kant, K.; Mohapatra, P., "Improving BGP Convergence Delay for Large-Scale Failures," International Conference on Dependable Systems and Networks (DSN), pp.323-332, 25-28 June 2006.

[22] S. Deshpande and B. Sikdar, “On the Impact of Route Processing and MRAI Timers on BGP Convergence Times,” in Proc. GLOBECOM 2004, Vol. 2, pp 1147- 1151.

[23] H. Tangmunarunkit, J. Doyle, et al, “Does Size Determine Degree in AS Topology?” ACM SIGCOMM Computer Communication Review, vol. 31, issue 5, pp. 7–10, Oct. 2001. “SSFNet: Scalable Simulation Framework”. URL: http://www.ssfnet.org/

Nasser Solayman, B.Sc. of computer & systems, Faculty of Engineering, Zagazig University July 2007.Network Support Engineer (information and decision support center) Current (From 11/11/2012– Till Now). Network Engineer, “Barclays Bank (15/03/2010 – 01/11/2012). paper published on Menoufia University Faculty of Engineering First International Conference (Ninth Conference of Sustainable Environmental Development) 24-28 March 2017 with title (Improving Performance of Border Gateway protocol for Large-Scale Autonomous Systems)

Ayman El-Sayed, received the BSc degree in computer science and engineering in 1994, the master’s degree in computer networks in 2000 from the University of Menofia, Egypt, and the PhD degree in computer network in 2004 from “Institute National De Polytechnique De Grenoble” INPG, France. He is an associate professor in the Computer Science and Engineering Department, Faculty of Electronic Engineering, Menofia University, Egypt. He is specialized in soft computing, algorithms, and data structure. In addition, his interests include multicast routing protocols, application-level multicast techniques, multicast on both mobile network and mobile IP, and image processing techniques. In addition, there are other interesting topics such as bioinformatics, Biocomputing, and bio computer. He is an approved supervisor for MSc and PhD programs in various University. He has completed various project in government and private organization. He has published more than 75 research papers in international Journals and two books about OSPF protocol and multicast protocols. Currently, he is serving as an editorial board member in various international Journals and conferences. He is a senior member of the IEEE.

Mohammed Badawy, received his B.Sc. and M.S. in computer science and engineering at Menoufia University (Egypt) and received his Ph.D. in computer science and engineering at Czech Technical University in Prague (Czech Republic). He worked as assistant professor in the department of Computer Science and Engineering at Menoufia University (Egypt) from 2002 to 2005. He worked as assistant professor in the department of Information Technology at Taif University (Saudi Arabia) from 2005 to 2010 (3 years of them as chairman of the department). Currently, he worked as a consultant in the deanship of Information Technology at Islamic University (Saudi Arabia) from 2010. His research interests include databases, data stream systems, and software development. He is a member of Association of Computer Science and Information Technology (IACSIT) and a reviewer of the International Journal of Engineering and Technology (IJET). He has published about 15 papers in various scientific journals and refereed conferences.