An Inter-domain Routing Protocol N-BGP for Space Internetworking

Huiwen Chen(✉), Kanglian Zhao, Jiawei Sun, Wenfeng Li, and Yuan Fang

Nanjing University, Nanjing, China
chenhuiwen@smail.nju.edu.cn

Abstract. Boarder Gateway Protocol (BGP) is mainly used for inter-domain routing in terrestrial internetworking. However, when the traditional BGP is used for space internetworking, inter-domain link interruption might occur more frequently and the time of routing convergence will tend to be long, which would greatly reduce the stability of the network. A new variant of border gateway protocol, N-BGP is proposed in this paper for space internetworking. Firstly, the existing NTD-BGP method are adopted in N-BGP to deal with predictable link changes caused by orbital dynamics of satellites. For the unpredictable link break, BGP finite state machine is modified and a new link break detection mechanism is also introduced. Considering the predictability of satellite motion, the backup routing mechanism is also used to maintain the stability of the network, which realizes the high stability of inter-domain routing. The experimental results show that the improved routing protocol N-BGP is superior to the traditional BGP in reducing the detection time of link interruption and maintaining the network stability.

Keywords: Inter-domain routing protocol · Unexpected link interruption · Space environments

1 Introduction

Typical satellite networks include GEO, MEO, LEO and other satellite systems [1]. In space networks, each satellite system is generally regarded as an independent and complete autonomous system (AS) domain [2]. Within each AS autonomous domain, one or more satellites are selected as the boundary router of this domain to establish inter-domain links with the corresponding boundary routers of other domains to realize information transmission between different autonomous domains.

On the other hand, compared with the topology of space networks which change frequently because of the orbital dynamics of the satellites, the topologies of the terrestrial networks are relatively fixed and the distance between each pair of routers in the link is shorter, which results in shorter transmission delay. Therefore, the traditional BGP protocol and the network topology are tightly coupled in the terrestrial networks. When there is a change in the neighbor relationship, because the traditional BGP is sensitive to the change of link state, so it can detect the unexpected interruption of the link

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2021
Published by Springer Nature Switzerland AG 2021. All Rights Reserved
Q. Wu et al. (Eds.): WiSATS 2020, LNICST 357, pp. 283–296, 2021.
https://doi.org/10.1007/978-3-030-69069-4_24

quickly. Considering the characteristics of the space environment, the topology changes frequently because of the orbital dynamics of the satellites, resulting in the frequent updating of the neighborhood relations, which will cause the huge consumption of the limited onboard resources. Moreover, there are also unpredictable link interrupts, which are usually caused by the radiation interference of the communication channel or the temporary failure of a satellite. When unpredictable interrupts occur, the traditional BGP protocol often requires longer routing convergence time to detect link interruption. However, in space internetworking, the time for route updating can be long, which means the link might change again even if the route has not been updated. In the process from link interruption to link recovery, a large number of packets might be lost, which will not only increase the rate of packet loss, but also greatly reduce the stability of the network. The special situations as mentioned above in space internetworking will bring a series of challenges and burden to the satellites networks with limited bandwidth.

In order to solve the problems with the application of the traditional BGP protocol in the space environment [3], the existing research direction is mainly aimed at the frequent change of spatial topology, and a series of solutions are proposed. Wei Han [4] et al. proposed NCSR which applies network coding to multicast transmission of geographic satellite network BGP in response to environmental interference. Roman Chertov et al. [5] conducted a high-fidelity experimental study on intermittent space/ground links and its impact on BGP peer-to-peer sessions between ground and satellite routers. Fabrice Hobaya [6] et al. analyzed the different ways of deploying BGP in DVB-S2/RCS networks and the opportunities to leverage the reliable multicast transport layer. Eylem Ekici and Chao Chen [7] proposed the BGP-S protocol, which makes the automatic discovery of paths through satellite networks possible.

NTD-BGP [8] takes advantage of the predictability of the orbital dynamics of the satellites, establishes the neighbor relation based on router loopback address, reduces the number of changes in neighbor relations, decouples the mapping relation between network topology and inter-domain neighbor relations and route updates, realizes the fast update of route, and improves the stability of network. However, this kind of scheme only focuses on the predictable change in topology, but it cannot solve a series of problems caused by unpredictable link interruptions.

The scheme presented in this paper utilizes the existing NTD-BGP method to cope with the predictable change of the topologies, while for the unpredictable link interruptions, a new mechanism is introduced to shorten the convergence time and improve the stability of the network for inter-domain routing in space environment.

2 The BGP Protocol

As an inter-domain routing protocol [9], BGP is responsible for the routing among different AS domains. The BGP routers in the same domain maintain the interior boarder gateway protocol (IBGP) neighbor relationship with each other, while the routers in different domains maintain the exterior boarder gateway (EBGP) neighbor relationship with each other. EBGP neighbor relationships require physical links between neighbor bodies, while only logical links are required between IBGP neighbor bodies. The BGP adopts a finite state machine, in which the router starts from the Idle state, exchanges a

series of messages, and finally reaches the Established state, successfully establishing the neighborhood body relationship, as shown in Fig. 1.

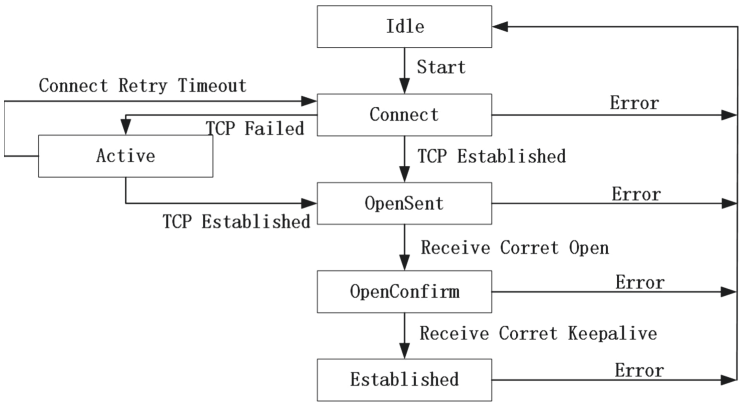


Fig. 1. BGP finite neighbor state machine

After the neighbor relationships are established, the router announces all the routing prefix information to all the neighbors to generate the forward information base (FIB). The state of the link is detected by sending keepalive messages periodically between neighbors (default 60 s), indicating the effectiveness of the link, and a value of hold time (default 180 s) is maintained between the neighbor bodies by default. When routers start exchanging open messages with each other, they will receive the value of send time from each other in the open message and determine the value of hold time and keepalive time after negotiation. The negotiation algorithm is shown in Algorithm 1.

Algorithm 1: time negotiation

1) If (send time from the other router < local hold time)
   local hold time = send time
2) If (local keepalive time < (send time from the other router / 3))
   local keepalive time = send time/3

When the router receives a larger hold time value than its own, no changes will be made. On the contrary, when it receives a smaller time, it will use the received time to replace its own hold time. When the router does not receive the keepalive message sent periodically by the neighbor body including hold time, a link interrupt will be inferred and both sides of the neighbor body will return to the Idle state from the Established state and send the undo route prefix to update the route. For the neighbors, if the hold time is too long, the routing update time will also be too long. If the link is interrupted unexpectedly, the packet loss rate of the link will be greatly increased and the stability of the network will be reduced. However, if the hold time is too small, the link will be updated frequently, resulting in the instability of inter-domain neighbor relations, which consumes the limited computing resources and bandwidth on the satellite networks.

Three keepalive messages without response indicates link interruption in the traditional BGP protocol. On the one hand, when the inter-domain link is interrupted unexpectedly, if the interruption time is short, the traditional BGP protocol cannot detect the link interruption in this period of time, then the router will not update the route and keep forwarding the data according to the original FIB resulting in packet loss. On the other hand, if the interruption time is long, the BGP will shut down the neighbor body. The router will turn to Idle state, declare the route to be canceled, and re-update the route. Before the route update is completed, the network will generate a large number of packet loss, which greatly reduces the stability of the network.

Take the topology in Fig. 2 as an example, inter-domain link between the border routers A and D breaks unpredictably, if link interruption time is short, the relationship between A and D will not change during the link break. So during this interruption, all the transmitting packets from router E to router F will be lost. If the link is interrupted for a long time and the link is still not recovered when the neighbor relation between A and D is closed, the border routers A and D will declare the route prefix on the whole network Sand the route will be convergent and updated again, which costs a lot of time and resources. This not only affects the stability of the network, but also wastes the limited onboard resources.

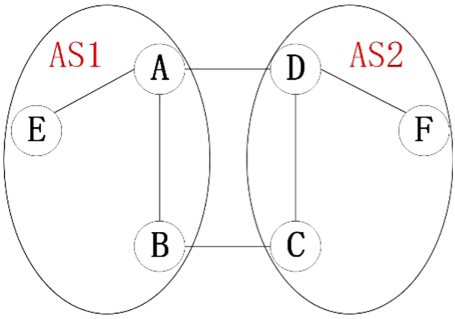


Fig. 2. Link detection mechanism of traditional BGP protocol

3 A New Variant of the BGP Protocol for Space Internetworking

Based on the traditional BGP, a new variant of the BGP protocol, N-BGP, is proposed in this section. Similar to the NTD-BGP protocol, N-BGP copes with the problem of routing updates caused by predictable topology changes. Moreover, in view of the unpredictable link break, N-BGP introduces a new inter-domain link break detection mechanism, which improves the BGP originally limited neighbor state machine itself and greatly shortens the time of detection of accident link breaks. Secondly, N-BGP calculates the corresponding backup routing for the link between each domain and stores in each router. When the new detection mechanism detects the unpredictable break link, the router turns to a new state, amending the routing itself to backup routing and guarantee the stability of the network.

3.1 The Detection Mechanism of the Unpredictable Link Interruptions

In N-BGP, the traditional BGP neighbor state machine is improved with the introduction of new detection mechanism. Hold time is set as 180 s by default while keepalive time is set as 60 s by default. On the border routers, test messages are sent every 10s regularly to detect the state information of inter-domain links. Once the neighbor does not receive the test messages, it judges that the link is down. The modified state machine is shown in Fig. 3.

When the detection mechanism detects a link interrupt, it modifies the router's own FIB to a backup FIB. When it detects the link recovery, it returns to the established state from the backup route state. When the backup route fails to meet the requirements, the traditional BGP route updating mechanism is reactivated. The new detection mechanism of the N-BGP greatly shortens the detection time of link interruption and reduces the consumption of onboard resource for calculation to some extent.

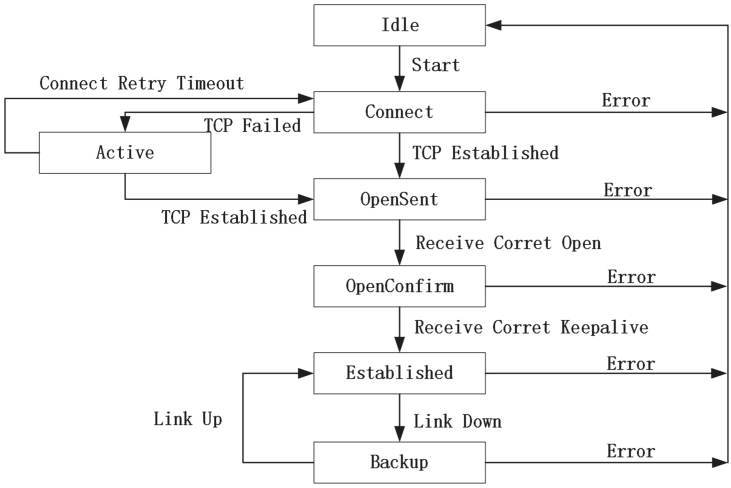


Fig. 3. Improved finite neighbor state machine

Unpredictable link interruptions can be divided into two categories:

1) If the link interruption is short, the link interruption and recovery are completed within the hold time in this situation. Then the neighbor relationship of neighbor body of each inter-domain link will not change. When an unexpected link interruption occurs, it turns to back up routes after receiving the probe message. After the link recovery, the original main route will be restored. As we can see in the following Fig. 4.

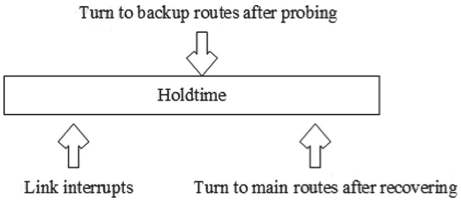


Fig. 4. Link interrupt detection mechanism with short interrupt time

2) If the link interruption time is long, the EBGP neighbor relationships will comes to an end and the routers will change to the Idle state. When the link reconnects, the route will be updated and the original main route will be restored in the routers. As we can see in the following Fig. 5.

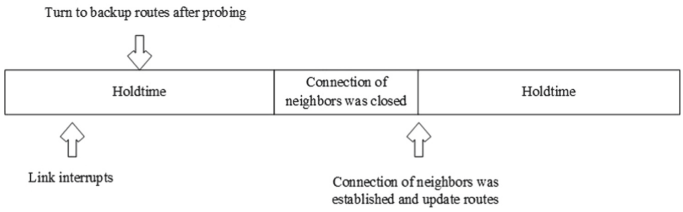


Fig. 5. Link interruption detection mechanism with long interruption time

3.2 Calculation of the Backup Path

Take the above topology in Fig. 2 as an example, there are two AS domains in the topology, and two border routers are set in each domain to connect with the other domain. The number of the inter-domain links between the domains are two. When an inter-domain link is interrupted unexpectedly, the border router replaces the main route with the stored backup route. The calculation of backup route is mainly aimed at the next hop, and the next hop is modified as the backup route. The backup routing mechanism of the N-BGP consists of the following three steps:

Firstly, a table of inter-domain topological relation is introduced, which records the border routers in AS1 and AS2 in real time, as well as the relations between them. The stored table of inter-domain topological relation is shown in Table 1, which has border router A and B in AS1, border router D and C in AS2. And there is an inter-domain link between router A and router D, and an inter-domain link between router B and C.

Secondly, the inter-domain topology relation table, IGP routing table, and BGP routing table stored in router A is summarized as mentioned above. There are three destinations in AS2 to router A in AS1. Each destination is described as a prefix. To arrive each destination, router D will be its next hop, which is the same as described in the following Table 2. In AS1, there are two destinations except router A. And to reach router E or B, next hop is also shown as in the following Table 3.

Table 1. Table of inter-domain topological relation.

AS1	AS2
A	D
B	C

Table 2. BGP routing table.

Destination	Next hop
Prefix1	D
Prefix2	D
Prefix3	D

Table 3. IGP routing table.

Destination	Next hop
E	E
B	B

Third, backup FIB is summarized as mentioned above (Table 4).

Table 4. Backup FIB.

Destination	Next hop
Prefix1	B
Prefix2	B
Prefix3	B

The principle of the calculation of the backup route is:

1) For any routing table item (destination, next hop), if and only if the next hop is the EBGP neighbor node of the router, the corresponding backup route (destination', next hop) is generated.
2) For any backup route (destination', next hop), destination' router and destination router are in the same AS.

Taking the topology shown in Fig. 2 as an example, there is an inter-domain link between router A and router D, and there is also an inter-domain link between router

B and router C, and EBGP neighbor relationship is established respectively. Router A, router B and router E belong to the same domain AS1 and are the IBGP neighbors to each other. For router A, any destination prefix in domain AS2 can be reached by router D for the next hop, but also can be reached by another border router C in the same domain through router B. So as for router A, it uses path A to D to arrive AS2 as main route while it also uses path A-B-C-D as backup route.

When the link between router A and router D is interrupted unexpectedly, the route on router A and router D is switched to the backup route, which can guarantee the stability of the network during interruption and reduce the packet loss rate. For other routers in the domain, the routing table is kept unchanged and router A or router D is still taken as the next hop to the destination in the other domain. When the link is restored, the backup route is cancelled and switched back to the original route.

3.3 Main Modules of N-BGP Protocol

Main modules of N-BGP protocol are shown in Fig. 6.

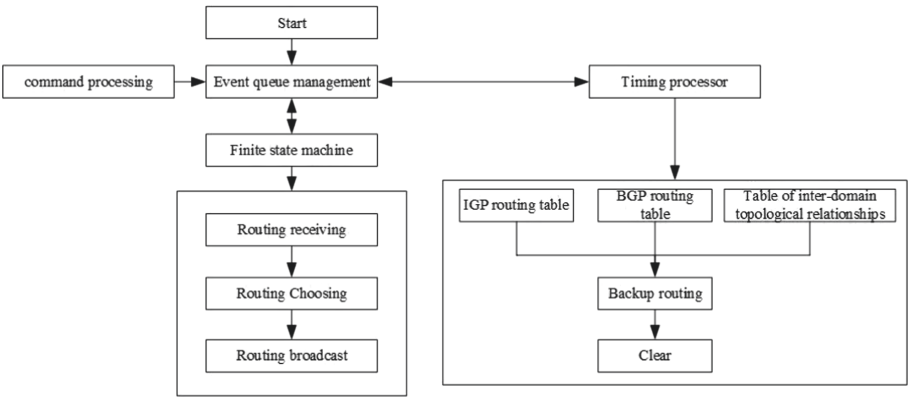


Fig. 6. Main modules of the BGP protocol.

1) The start module mainly completes the initialization.
2) The event queue management module mainly manages the time queue, which is the trigger condition of the state transfer of N-BGP finite state machine and promotes the operation of the module of finite state machine.
3) The command processing module is responsible for processing various commands and calls related functions for processing.
4) The timing processing module handles the event timeout and other behaviors through the timer queue, detects the link state through the timing processing module, and then turns to the backup routing mechanism.
5) The calculation module of backup route is shown in the box, indicating that the backup route is calculated by IGP routing table, BGP routing table and inter-domain topological relation table. In addition, in the space internetworking, when the satellite

motion produces a change in topology, the backup route stored in the original storage is cleared by the clearance mechanism to reduce the overhead of the satellite.

6) The module of finite state machine is responsible for the management of finite neighbor state machine. In the original BGP protocol, there are 13 events that can trigger the state change. When the neighbor relationship is established, a series of processing processes from receiving to sending are completed through the routing receiving, routing selection and routing broadcast modules in the box.

Compared with the traditional BGP protocol, the new protocol N-BGP not only can deal with a series of problems such as longer time of routing convergence caused by frequent changes of the routing update frequently. In view of the unpredictable link break, it introduces a new detecting mechanism, which changes the traditional BGP neighbor finite state machine. The new detection mechanism can be more effective and rapidly detect link interruption, greatly reducing the routing convergence time. On the other hand, the table of inter-domain topological relation is introduced, and the backup route is calculated by the table of inter-domain topological relation, IGP routing table and BGP routing table. When the backup route fails to work, the traditional BGP mechanism is reverted to and the route is re-converged and updated to ensure the effectiveness.

4 Simulation Results

4.1 Experimental Scenarios

In this part, the performance of the proposed N-BGP will be verified in the case of unpredictable link interrupts, especially with the comparison with the traditional BGP. A topology of eight simplified nodes in a certain time slice is assumed, as shown in Fig. 7.

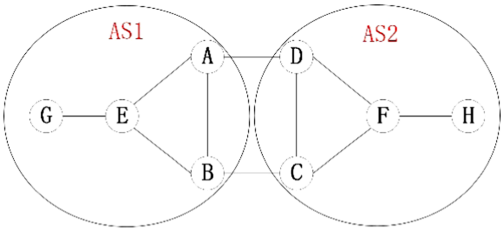


Fig. 7. Test topology.

In this topology, there are two AS domains, each containing four router nodes and two boundary routers. There are altogether four boundary routers in the whole topology, two of which are EBGP neighbor bodies of each other, and there are two interdomain links between the two domains. In order to simulate space environment and verify the validity of the improved inter-domain routing protocol, it uses Docker [12] and the software router Quagga [11] as routers. At the same time, the routers are connected by OVS [13] and it uses OVS flow table to simulate link interruption and recovery,

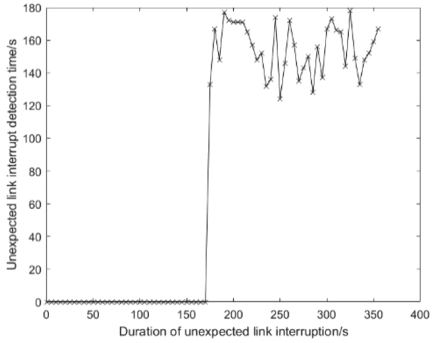
which effectively increases the fidelity of the emulation. Considering the impact of link interruption time on performance, different lengths of the link interruption time are selected here as independent variables to test the performance.

4.2 Performance Analysis

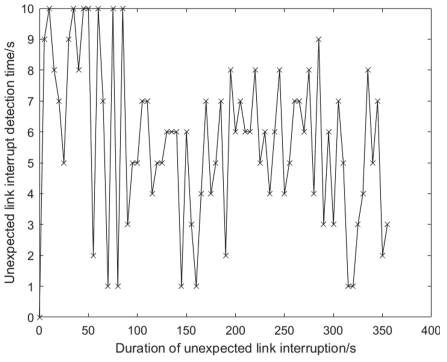
Three metrics are selected to evaluate the performance of the proposed N-BGP and the traditional BGP protocol, which are the detection time of the unexpected link interruption, the routing convergence time and the network stability.

Among them, the detection time of the unexpected link interruption indicates the time required to detect the unpredictable link interruption.

Routing convergence time T, on the other hand, contains two parts. One is convergence time after link interruption is detected. The other is the convergence time after routing recovery. In the test of routing convergence time, the time of routing convergence is mainly tested under different link interrupt times randomly.



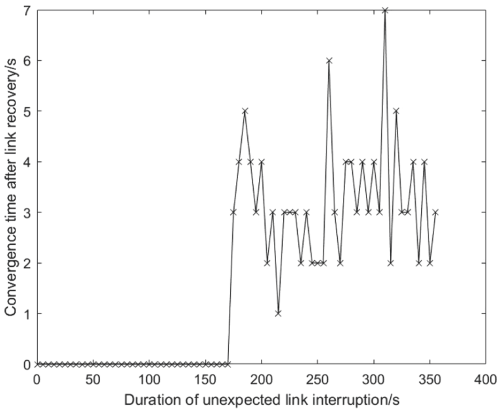
(a) Detection time in traditional BGP protocol



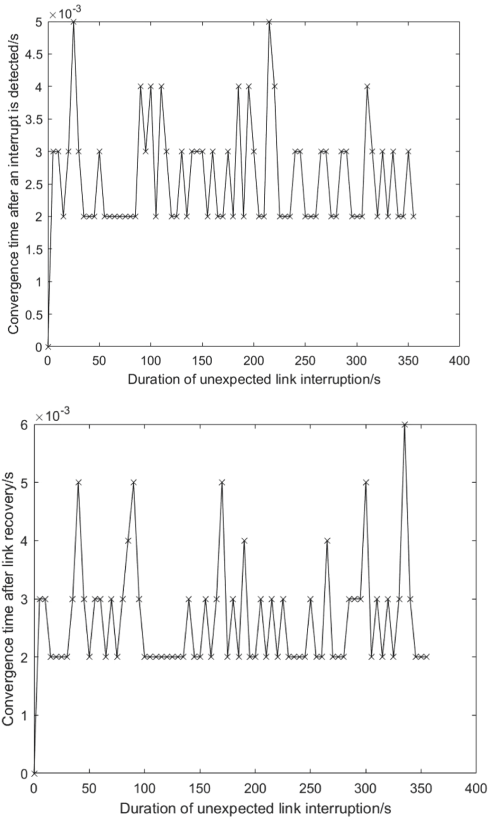
(b) Detection time in N-BGP

Fig. 8. The detection time of the unexpected link interruption.

In Fig. 8, the link interruption time is selected from 5s to 360s, and each 5s is a step length. When the unpredictable link interruption duration is less than 180s, it can



(a) Convergence time of traditional BGP protocol



(b) Convergence time of improved protocol

Fig. 9. Routing convergence time.

be found that link interruptions cannot be found by the traditional BGP protocol. When the unpredictable link interruption is more than 180s, the traditional BGP protocol can detect the interruption, but the detection time fluctuates randomly within the scope of 120s to 180s, which means that we need a long time to detect the accidental interruption. In contrast, it can be found that the link interruption can be detected by the improved protocol relatively quickly after about 10s. The detection time of link interrupt fluctuates in the range of 0-10s, and the detection speed is much faster.

When an unpredictable link interruption occurs, the route convergence time is mainly composed of two parts: the route convergence time from the detection of link interruption to the end of route convergence, and the route convergence time from the link recovery to the end of route convergence. For the BGP protocol, the detection time is relatively long and the route convergence time from the detection to the end of routing convergence is negligible compared with the detection time. The test results for the routing convergence time are shown in Fig. 9.

The duration of unexpected interruption is selected ranging from 5 to 360s, and the step length is 5s. Considering that the convergence time after link interruption in BGP can be ignored compared with the detection time, the routing convergence time after link recovery is shown in Fig. 9(a). It can be found that when the protocol detects link interruption, the convergence time fluctuates within 1–7 s and the convergence speed is slow. When N-BGP is adopted, the convergence time fluctuates within the range of 0–10 ms. This is because of the existence of the backup routes, which greatly reduces the convergence time. By testing the packet loss rate within the link interrupt time, the network stability of the two protocols can be compared as in Fig. 10.

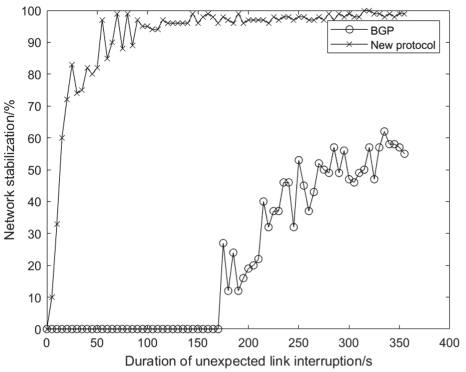


Fig. 10. Network stabilization.

It can be found that the network stability of the BGP protocol is poor, which is less than 50%, and increases gradually with the increases of link interruption duration. However, the N-BGP protocol has better network stability, which increases rapidly with the increases of link interruption duration and maintains about 100% in a long range.

5 Conclusions

In this paper, N-BGP is proposed to solve a series of performance problems caused by frequent topology changes and unpredictable inter-domain link interruptions. N-BGP adopts the scheme of the NTD-BGP protocol and introduces a new detection mechanism to detect the inter-domain link interrupts at a faster speed. In addition, considering the predictability of orbital dynamics of the satellites, a backup routing mechanism is introduced to guarantee the corresponding backup route on the boundary router. When the link interruption is detected quickly, the backup route is switched to ensure the stability of the network. Finally, the new improved protocol was designed and implemented in Quagga. The results of emulation show that the proposed N-GBP protocol greatly improves the network stability by shortening time for link interruption detection and backup routes. However, N-BGP requires a certain amount of space to store routing information on the router, which increases the cost of routing. The future research will be focused on how to reduce the routing cost as well as shorten the routing convergence time and improve the routing stability.

References

1. Roddy, D.: Satellite Communications (2003)
2. Chandra, R., Traina, P., Li, T.: BGP communities attribute. RFC 1997, August 1996
3. Narvaez, P., Clerget, A., Dabbous, W.: Internet routing over LEO satellite constellations. In: Third ACM/IEEE International Workshop on Satellite-Based Information Services (WOSBIS 1998) (1998)
4. Han, W., Wang, B., Feng, Z., et al.: NCSR: multicast transport of BGP for geostationary Satellite network based on network coding. In: 2015 IEEE Aerospace Conference, pp. 1–10. IEEE (2015)
5. Chertov, R., Almeroth, K.: Using BGP in a satellite-based challenged network environment. In: 2010 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), pp. 1–9. IEEE (2010)
6. Hobaya, F., Chaput, E., Baudoin, C., et al.: Reliable multicast transport of BGP for geostationary satellite networks. In: 2012 IEEE International Conference on Communications (ICC), pp. 3239–3244. IEEE (2012)
7. Ekici, E., Chen, C.: BGP-S: a protocol for terrestrial and satellite network integration in network layer. Wireless Netw. **10**(5), 595–605 (2004)
8. Yang, Z., Wu, Q., Li, H., et al.: NTD-BGP: an inter-domain routing protocol for integrated terrestrial-satellite networks. J. Tsinghua Univ. (Sci. Technol.) **59**(7), 512–522 (2019)
9. Hares, S., Rekhter, Y., Li, T.: A Border Gateway Protocol 4 (BGP-4) (2006)
10. Papa, A., De Cola, T., Vizarreta, P., et al.: Dynamic SDN controller placement in a LEO constellation satellite network. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp. 206–212. IEEE (2018)

11. Quagga Routing Suite. https://www.quagga.net/
12. Boettiger, C.: An introduction to Docker for reproducible research, with examples from the R environment. ACM Sigops Oper. Syst. Rev. **49**(1), 71–79 (2014)
13. Open vSwitch. https://www.openvswitch.org/
14. Ramanath, A.: A Study of the interaction of BGP/OSPF in Zebra/ZebOS/Quagga (2004)