2016 3rd International Conference on Engineering Technology and Application (ICETA 2016)
ISBN: 978-1-60595-383-0

The Simulation Research of Potential Loop in Redistribution of Multipoint Two-way Routing Protocol Based on the Butterfly Effect

Ruifang Zhang*
College of Mechanical and Control Engineering, Guilin University of Technology, Guilin, Guangxi, China

Chen Yang
Guilin Municipal Public Security Bureau, Guilin, Guangxi, China

ABSTRACT: This paper first conducted a simulation research on the redistribution theory of routing protocols, and proposed the inevitability of existence of latent ring circuit. Then the butterfly effect principle was analyzed, and putting forward the butterfly effect caused significant transformation in the complex system which was also suitable for multipoint two-way potential loop problems in the process of redistribution, leading to a collapse of the whole network. Finally, with the aid of Netlogo for simulation experiment in complex system, the simulation of butterfly effect was conducted under three situations where the potential loop produces, and the potential loop in the large-scale network, and particularly heavily node must be resolved under the network architecture. Otherwise it will cause the data stream storm because of the potential loop to result in the network paralysis.

Keywords: route protocol redistribution; potential loop; butterfly effect; Netlogo

1 INTRODUCTION

In large network environment, there are many different routing protocols. How can it ensure that the different routing protocols can learn from each other in some way in this environment, and ensure that the correctness of the routing entries is an effective way to guarantee the network functions at present and in the future? The redistribution between the routing protocols is a bridge to solve the communication between different routing protocols [1]. However, with the expansion of the scale of the network architecture, the use of multi-directional redistribution between different routing protocols also brings a lot of problems of routing, loop, etc., [2] which can easily be found and solved when they are deployed. The most difficult problem is the loop problem which probably occurs at any time and cannot be found. These loops become the hidden danger of the whole network communication system, which is called potential loop. This potential loop caused by the results can be explained by the butterfly effect. Once small packets cause the loop of routing entries, great waste will appear in the internal performance of the router, potential loop will spread to the whole communication system, which makes the efficiency of the whole communication system decrease rapidly and even result in network paralysis.

There are many scholars and researchers at home and abroad to do the academic research on the routing loop of the large structure. For example, in the literature [3] and [4], an analysis is made of the potential loop caused by the emergence of local network topology. And the literature [5] analyzes the advantages and disadvantages of the loop in a dynamic routing protocol. It can be seen that there is no research on the potential loop caused by the multidirectional redistribution of routing protocol in large scale environment so far. But the butterfly effect is real, and the tiny possibility of potential loop caused by route makes the paralysis of whole network become a reality. So solving the potential loop is helpful to improve the efficiency and robustness of the network system.

*Corresponding author: 631600961@qq.com

2 RESEARCH ON THE OCCURRENCE OF POTENTIAL LOOP

2.1 *The significance of redistribution*

In the network protocol, distance vector routing protocol is suitable for medium-sized network. It will not consider the whole topology, just get the overall routing information from the neighbors, and update its own routing table, which will generate a lot of non-optimal routing problem. When a node learned routing from its neighbors, next-hop routing is designated to the neighbor routers. However, because the bandwidth of the link, delay, node processing capabilities are not taken into account, the routing protocol is more suitable for medium-scale network, such as that in cities and counties. The representatives of this kind of routing protocol are EIGRP, RIP, etc.. [6]

Link-state routing protocol is mainly suitable for large and medium-sized network, which involves many values of the whole topology, such as node information, bandwidth, delay, etc., so it knows all situation of topology well. Each node can learn different link state information from its neighbors, and store in its own link state database. According to the Dijkstra algorithm, calculate the optimal path [7], and fill in the routing table. Moreover, this kind of routing protocol carries hierarchical refinement in different regions, different layers are denoted by different levels of LSA (link state advertisement), only a static route of all routers in NSSA (not so-stub area) points to the ASR (area border router). There is no necessary for each routing node in stub region to learn the whole routing information, which is also the concept of hierarchical structure, and the main purpose is to simplify the routing table, enhance the search efficiency, layer the different hierarchical routers, and on-demand procurement, which can save money, process the logic relationship between all layers, and make the most of the performance of the router. The representatives of this kind of routing protocol are OSPF and IS-IS [8].

Between the large-scale network and medium-sized network, or the medium-sized network and small-scale networks, interconnection between different scales will be involved, and different protocols cannot be identified, which means every protocol has its own language. This is just like an Englishman who can't speak Chinese meeting a Chinese who can't speak English, both of them cannot understand and deal with each other's information. Here we need a Chinese who can speak both English and Chinese as translator, to help them communicate, so does the routing protocol. In different routing protocols, a technology is needed to ensure the transformation between different protocols. That is the routing redistribution technology.

Routing redistribution makes routers running different network protocols identify and process the information from different network protocols. In fact, the border router is the most important, which is the so-called translator.

2.2 *Research on the emergence of potential loop*

In different routing protocols, the internal protocol number of IP header is used to distinguish the different adjacent protocols. The protocol number of RIP is UDP520, that of OSPF is 89 based on IP, and that of EIGRP is 88. First, the data message is received from the border router ASBR. If the protocol number of IP header is not consistent with the local protocol number, it will be converted to the relevant characteristics belonging to the local place, such as cost value in OSPF, bandwidth of EIGRP, delay, reliability, load, and MTU. It should be noted that, the assigned routing entries belong to different priority in different routing protocols, so a value is required to measure which is the administrative distance [9]. The administrative distance of RIP is 120, and that of OSPF is 110. In order to prevent the routing loop caused by administrative distance, the external administrative distance of EIGRP protocol is 170 and the internal one is 90. If there are two same paths for the objective message has the same two paths, that of higher administrative distance will be discarded, and the lower one will be used to transmit the routing protocol.

We verify the emergence of potential loop through experiments:

As shown in Figure 1, R1, R2,... R9 are nine routers which are located in different areas, and their loopback address is RX:X.X.X.X/32, for example, the loopback address of R1 is 1.1.1.1/32. The network segment among them is X X+1.0.0.0/24 network, for example, that between R1 and R2 is 12.0.0.0/24. The RX interface address is the network segment, of which the last 0 is changed to X. That is to say the address of interface S1/0 from R1 to R2 is 12.0.0.1/24 and so on.

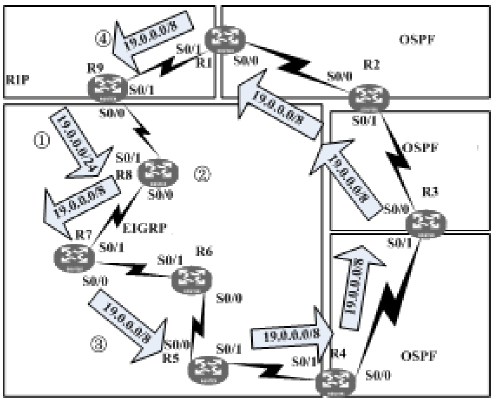

Figure 1. The network topology of potential loop caused by redistribution.

The simulation test is done through the Web-IOU. After whole network convergence, the R1 routing table entry is:

```
R1#show
*Mar 23 11:02:15.303: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2     1.0.0.0/8 [110/1] via 12.0.0.2, 00:01:28, Serial0/0
C        1.1.1.1/32 is directly connected, Loopback0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2     2.0.0.0/8 [110/1] via 12.0.0.2, 00:01:28, Serial0/0
O IA     2.2.2.2/32 [110/65] via 12.0.0.2, 00:28:29, Serial0/0
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2     3.0.0.0/8 [110/1] via 12.0.0.2, 00:01:28, Serial0/0
O IA     3.3.3.3/32 [110/129] via 12.0.0.2, 00:27:26, Serial0/0
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2     4.0.0.0/8 [110/1] via 12.0.0.2, 00:01:28, Serial0/0
O IA     4.4.4.4/32 [110/193] via 12.0.0.2, 00:05:25, Serial0/0
R     5.0.0.0/8 [120/2] via 19.0.0.9, 00:00:03, Serial0/1
R     6.0.0.0/8 [120/2] via 19.0.0.9, 00:00:03, Serial0/1
R     7.0.0.0/8 [120/2] via 19.0.0.9, 00:00:03, Serial0/1
R     8.0.0.0/8 [120/2] via 19.0.0.9, 00:00:03, Serial0/1
R     9.0.0.0/8 [120/1] via 19.0.0.9, 00:00:03, Serial0/1
      12.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
O E2     12.0.0.0/8 [110/1] via 12.0.0.2, 00:01:28, Serial0/0
C        12.0.0.0/24 is directly connected, Serial0/0
L        12.0.0.1/32 is directly connected, Serial0/0
      19.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
O E2     19.0.0.0/8 [110/1] via 12.0.0.2, 00:01:28, Serial0/0
C        19.0.0.0/24 is directly connected, Serial0/1
L        19.0.0.1/32 is directly connected, Serial0/1
      23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2     23.0.0.0/8 [110/1] via 12.0.0.2, 00:01:28, Serial0/0
O IA     23.0.0.0/24 [110/128] via 12.0.0.2, 00:27:58, Serial0/0
      34.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2     34.0.0.0/8 [110/1] via 12.0.0.2, 00:01:28, Serial0/0
O IA     34.0.0.0/24 [110/192] via 12.0.0.2, 00:26:19, Serial0/0
R     45.0.0.0/8 [120/2] via 19.0.0.9, 00:00:03, Serial0/1
R     56.0.0.0/8 [120/2] via 19.0.0.9, 00:00:03, Serial0/1
R     67.0.0.0/8 [120/2] via 19.0.0.9, 00:00:03, Serial0/1
R     78.0.0.0/8 [120/2] via 19.0.0.9, 00:00:03, Serial0/1
R     89.0.0.0/8 [120/1] via 19.0.0.9, 00:00:03, Serial0/1
```

Figure 2. R1 routing table.

After the completion of network convergence, the routing table of R1 is shown in Figure 2. As can be seen from the figure, there is a 19.0.0.0/8 bit routing entry above the 19.0.0.0/24 bit route, but the local interface address is 19.0.0.1/24. However, there are no 8 bits routing entries in the locality, and its origin of routing entry has a lot to do with 12.0.0.2, which is for the O E2 route, and the redistribution of routing entries. Let's track the path of the 19.0.0.0/8.

We regard any IP address as the destination address to track. Assuming that the IP address is 19.4.2.3/24, the tracking information is shown in Figure 3:

```
R1#traceroute 19.4.2.3

Type escape sequence to abort.
Tracing the route to 19.4.2.3

  1 12.0.0.2 12 msec 12 msec 12 msec
  2 23.0.0.3 20 msec 24 msec 56 msec
  3 34.0.0.4 44 msec 32 msec 28 msec
  4 45.0.0.5 44 msec 36 msec 44 msec
  5 56.0.0.6 44 msec 44 msec 36 msec
  6 67.0.0.7 44 msec 40 msec 44 msec
  7 78.0.0.8 48 msec 44 msec 44 msec
  8 89.0.0.9 32 msec 48 msec 44 msec
  9 19.0.0.1 52 msec 52 msec 48 msec
 10 12.0.0.2 56 msec 56 msec 52 msec
 11 23.0.0.3 56 msec 64 msec 68 msec
 12 34.0.0.4 68 msec 68 msec 64 msec
 13 45.0.0.5 88 msec 72 msec 84 msec
 14 56.0.0.6 84 msec 100 msec 84 msec
 15 67.0.0.7 88 msec 84 msec 80 msec
 16 78.0.0.8 80 msec 104 msec 92 msec
 17 89.0.0.9 84 msec 76 msec 84 msec
 18 19.0.0.1 88 msec 120 msec 88 msec
 19 12.0.0.2 76 msec 144 msec 92 msec
 20 23.0.0.3 92 msec 96 msec 100 msec
 21 34.0.0.4 112 msec 96 msec 112 msec
 22 45.0.0.5 124 msec 132 msec 168 msec
 23 56.0.0.6 124 msec 120 msec 128 msec
 24 67.0.0.7 128 msec 176 msec 152 msec
 25 78.0.0.8 120 msec 124 msec 128 msec
 26 89.0.0.9 116 msec 148 msec 128 msec
 27 19.0.0.1 132 msec 148 msec 148 msec
 28 12.0.0.2 144 msec 144 msec 144 msec
 29 23.0.0.3 156 msec 156 msec 144 msec
 30 34.0.0.4 144 msec 140 msec 156 msec
```

Figure 3. R1 potential loop.

The analysis is shown in Figure 4, starting from ①, 19.0.0.0/24 bit routing entry is issued by R9 through the RIP protocol and is delivered to R8. According to the characteristics of RIP protocol, R8 automatically aggregates to A class routing entries of 19.0.0.0/8 bit (The aggregation can simplify the routing entry and improve the forwarding efficiency of the router). After aggregated in ②, R8 deliver the route aggregated by RIP to R7 through redistribution, and the same process ③ has been transferred to R9 ④. R9 received routing entries, and then compared with the local RIP database. If 19.0.0.0/24 bit routing entries instead of 19.0.0.0/8 bit routing entries are be found, the 19.0.0.0/8 routing entries will be automatically put into database, forming routing table. The local database is not LSDB, which is designed for route entries floating to improve the stability of route entry. In this way, a route forms a large and infinite loop.

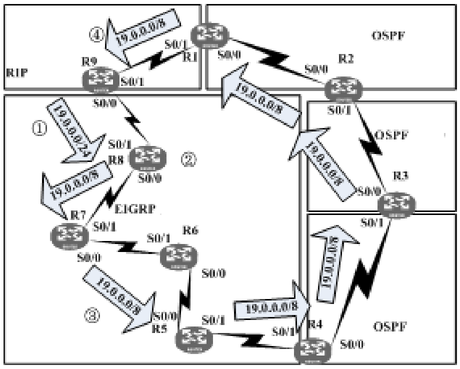

Figure 4. Analysis of potential loop.

```
R1#sho ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2     1.0.0.0/8 [110/1] via 12.0.0.2, 00:03:05, Serial0/0
C        1.1.1.1/32 is directly connected, Loopback0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2     2.0.0.0/8 [110/1] via 12.0.0.2, 00:03:04, Serial0/0
O IA     2.2.2.2/32 [110/65] via 12.0.0.2, 00:30:07, Serial0/0
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2     3.0.0.0/8 [110/1] via 12.0.0.2, 00:03:04, Serial0/0
O IA     3.3.3.3/32 [110/129] via 12.0.0.2, 00:30:07, Serial0/0
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2     4.0.0.0/8 [110/1] via 12.0.0.2, 00:03:04, Serial0/0
O IA     4.4.4.4/32 [110/193] via 12.0.0.2, 00:30:07, Serial0/0
R     5.0.0.0/8 [120/2] via 19.0.0.9, 00:00:13, Serial0/1
R     6.0.0.0/8 [120/2] via 19.0.0.9, 00:00:14, Serial0/1
R     7.0.0.0/8 [120/2] via 19.0.0.9, 00:00:14, Serial0/1
R     8.0.0.0/8 [120/2] via 19.0.0.9, 00:00:14, Serial0/1
R     9.0.0.0/8 [120/1] via 19.0.0.9, 00:00:14, Serial0/1
      12.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
O E2     12.0.0.0/8 [110/1] via 12.0.0.2, 00:03:06, Serial0/0
C        12.0.0.0/24 is directly connected, Serial0/0
L        12.0.0.1/32 is directly connected, Serial0/0
      19.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        19.0.0.0/24 is directly connected, Serial0/1
L        19.0.0.1/32 is directly connected, Serial0/1
      23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2     23.0.0.0/8 [110/1] via 12.0.0.2, 00:03:05, Serial0/0
O IA     23.0.0.0/24 [110/128] via 12.0.0.2, 00:30:08, Serial0/0
      34.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2     34.0.0.0/8 [110/1] via 12.0.0.2, 00:03:05, Serial0/0
O IA     34.0.0.0/24 [110/192] via 12.0.0.2, 00:30:08, Serial0/0
R     45.0.0.0/8 [120/2] via 19.0.0.9, 00:00:14, Serial0/1
R     56.0.0.0/8 [120/2] via 19.0.0.9, 00:00:14, Serial0/1
R     67.0.0.0/8 [120/2] via 19.0.0.9, 00:00:14, Serial0/1
R     78.0.0.0/8 [120/2] via 19.0.0.9, 00:00:14, Serial0/1
R     89.0.0.0/8 [120/1] via 19.0.0.9, 00:00:14, Serial0/1
```

Figure 5. R1 routing entries after filtering.

There are a variety of ways to solve the potential loop, such as policy routing, routing plus label, SDN, and so on. In this paper, we use the distribution list to match R8, and the ACL is used to filter the aggregated routing entries in the border router. The filtered routing entries are shown in Figure 5.

Potential loop is able to become the hidden danger in the redistribution process of network. If a small route is not carefully observed, it will cause the whole network crash according to the butterfly effect.

3 BUTTERFLY EFFECT THEORY

According to the research in 2.2 section, the potential loop can be seen everywhere, which is not paid much attention for many people. However, the tiny detail can lead to an enormous change in the whole network.

The butterfly effect is a concept of chaos theory, and it is a typical representative of explaining the chaotic characteristics of the complex system. Due to the nonlinear interaction of the complex system, a small change of the input will result in an enormous change after the changes in the complex system. The most vivid metaphor is that a butterfly flapping its wings in the Amazon rainforest of South Africa can generate a violent storm in Texas two weeks later. The fundamental reason is the complexity of weather system (the flap of a butterfly's wings changes air system around and generates weak airflow, which causes corresponding changes of the surrounding air or other systems. It is chain reaction, which leads to great changes in other systems eventually [11].

The butterfly effect was first proposed by the American meteorologist Lorenz, in Massachusetts Institute of Technology. In order to predict the weather, he used the model simulated by computer to solve the 13 equations of the earth's atmosphere. In an experiment, in order to get a better understanding of the results, an intermediate value was increased from 0.506 to 0.506127. However, such a small change led to two distinct results, and the similarity of the two curves completely disappeared. Hence, she proposed the same initial extreme complex nonlinear instability theory, which totally changes the understanding of mathematics. Why it is so big for the difference between initial values with such high similarity processed by a complex? This discovery gave people a new idea of analyzing complex systems [12].

Butterfly effect shows that the results of the development of things have a great dependence on the initial value. The smallest changes of the initial value will cause huge consequences such as the past stock market crash in United States, the financial crisis in Asian, and the El Nino phenomenon in Pacific Ocean. Butterfly effect implies that the tiny details should be paid more attention when seeking for the nature of things and the overall situation. That is to say, the details determine success or failure.

The large-scale network is a complex system. The problems whether there is the butterfly effect in it, and how large is the influence of the butterfly effect on the complex system have been proposed, however, because of the convergence of the network and avoiding loop, there are few people to study this kind of problem. It is a novel discovery that the butterfly effect actually exists in potential loop. Using computer to simulate the butterfly effect of potential loop will make a big difference to the topology, state, stability of the whole network.

4 SIMULATION MODEL DESIGN OF POTENTIAL LOOP

Netlogo is adopted in the simulation environment, which can clearly describe the relationship of various components in the complex system [13]. Inspect the relationship between subject and the complex system or that between subjects by adjusting the different behavior of the subject.

4.1 *Subject behavior design*

The behavior of each subject in large network system affects every aspect of the network system. In order to confirm the impact of the potential loop, the main body is divided into the following parts:

(1) Number-of-nodes: The range is from 10 to 1000.

(2) Average-node-degree: It means in what way the nodes are connected to each other and the range is from 1 to number-of-nodes.

(3) Initial-loop: It means the numbers of nodes which appear in the potential loop at the start of the description. The range is from 1 to number-of-nodes.

(4) Packet-transmittability: It identifies the successful probability of data traffic which is sent to the opposite end. Under normal circumstances, the forwarding speed of the data message of the current device is limited, which is 80%-95% basically. The range is from 1% to 100%.

(5) Packet_frequency: It shows the number of every data packet which is sent by each node every time.

(6) Reboot: It is probability of restart of the device which is affected by the potential loop. The range is from 1% to 100%.

(7) Distribute-list: It represents the distribution list is adopted to solve the potential loop. The range is from 1% to 100%.

The network state diagram of the output result:

Normal: dark gray, normal.

Loop: gray-white point, in the potential loop.

The vertical axis: the percentage of nodes.

The horizontal axis: the sending times of the ticks nodes after receiving data packet.

4.2 *The simulation of potential loop*

Case 1: the number of physical nodes is 150, and the average node is that there are 4 nodes connecting with each other around the nodes. The potential loop just appears in one point (gray-white part in Figure 6). The transmittability is 80%, and each node can send 4 data traffic. Simulation results are shown in Figure 6 and 7.

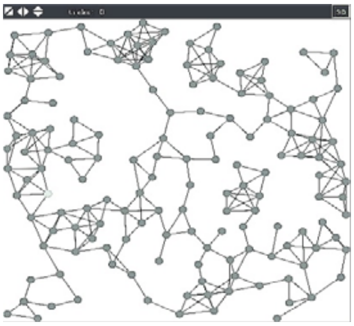

Figure 6. The initial state of simulation of 150 nodes.

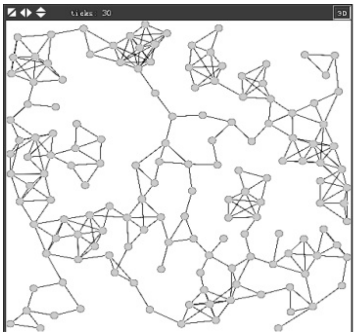

Figure 7. The state of 150 nodes after execution.

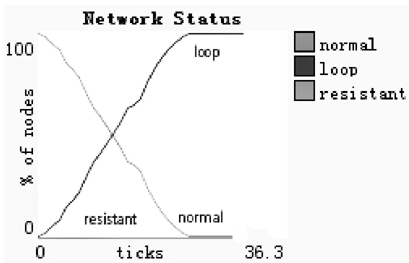

Figure 8. The network state of potential loop of 150 nodes

As can be seen from Figure 8, the normal state appears in the ticks at 36.3. If it is reached, the full network will be in invalid routing selection. It is just a potential loop that caused the whole network paralysis under 150 nodes under. Next we restart the device to observe whether it will be eased.

Assuming that the entire network is completely paralyzed, restart the 15% of the device, and the simulation results is shown in Figure 9 and 10:

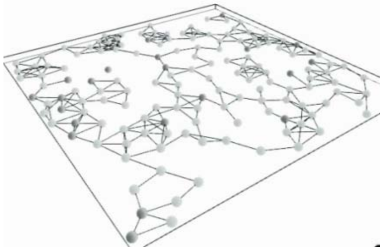

Figure 9. Continue to spread under the situation that the device with 150 nodes is restarted - process 1.

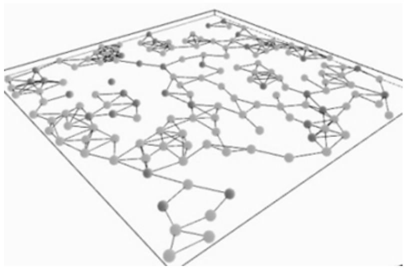

Figure 10. The potential loop continues to propagate after the restart of the device - process 2.

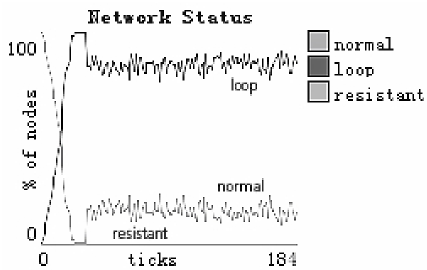

Figure 11. The network state of the restart of 15% of devices with 150 nodes.

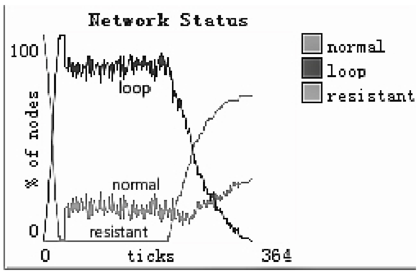

Figure 12. The network state of distribution list of the device with 150 nodes which is increased 10%.

As can be seen from Figure 11 and 12, after the restart of 15% of the device, the network is still proceeds in the addressing of potential loop and delivery of data packet. The percentage of normal nodes is only 10%-20%, and that of potential loop node is 80%-90%.

Table 1. The possible route of the butterfly effect caused by the state of the potential loop under different circumstances.

	Nodes	Initial potential loop	Packet forwarding rate %	Packet forwarding times	Restart device %	Distribution list %	Full network loopticks	Repair ticks
1	150	1	80	4	15	10	36.3	364
2	260	1	80	4	15	10	58.8	571
3	290	1	80	4	15	10	184	715

For this situation, the potential loop can be eliminated by strategies only. Add strategy to the various nodes, use the distribution list to remove the potential loop, and the state is as follows:

Gray part shows the state after the distribution list is added and the potential loop will be removed. It can be seen that only 10% of the distribution list can solve the potential loop of the whole network topology.

According to different situations, the simulation results of the state after increasing nodes are shown in Figure 13 and 14.

Case 2: The nodes are increased to 260, the potential loop node is 1, the packet forwarding probability is 80%, and the packet forwarding rate is 4.

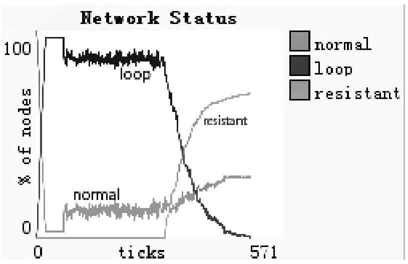

Figure 13. The network state of 260 physical nodes.

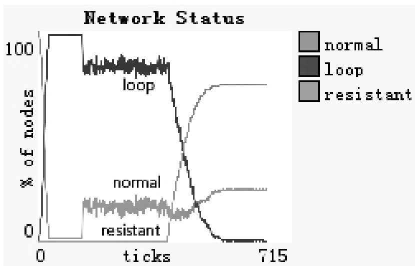

Figure 14. The network state of 260 physical nodes.

4.3 *The analysis of simulation result*

In order to understand the degree of influence and the recovery condition of the potential loop in different environments, the network state in different environments is concluded in Table 1.

As can be seen from Table 1, in the case of the increase of the number of nodes, the core ticks of the whole network is also different, and the number of times of ticks repair also grows. From the simulation results we can see that, regardless of the size of the topology, the invalid addressing of the potential loop will run out of the device resource sooner or later. The butterfly effect theory is suitable to explain the phenomenon: it is the small possible route that leads to significant problems in complex systems.

5 CONCLUSION

The paper studies the potential loop caused by multipoint two-way redistribution in large routing protocols, and using simulation method to prove its existence, and shield the possible route by rejecting the aggregate route entry to add detail routing. By studying the butterfly effect, it is found that this theory is suitable to explain the huge consequences caused by the potential loop. In the end, the process of butterfly effect of the potential loop is simulated in three situations, and the result shows any tiny possible routing will cause serious problem such as the whole network paralysis under any condition. Therefore, in the design of the architecture of large-scale network, the butterfly effect of the potential loop should be paid more attention, which can ensure the security and reliability of the whole network.

REFERENCES

[1] Hawk D.E. 2014. Method for computing IO redistribution routing: U.S. Patent 8,627,256 [P]. 2014-1-7.

[2] Boers A., Rosen E.C., Wijnands J.I. 2014. System and method for detecting loops for routing in a network environment: U.S. Patent 8, 644, 186[P]. 2014-2-4.

[3] Fu C.B., Tian A.H., Xiao H.M. 2013. Virtualization simulation based on routing protocol. *Applied Mechanics and Materials*, 401: 2025-2028.

[4] Yu Jian. 2013. Countermeasures against potential loop laults in network transformation of Guangxi TV station. *Advanced Television Engineering*, 11: 208.

[5] Zhang Junfeng, Zhong Cheng. 2011. Analysis and solution method for potential loop problem in local area network for Guangxi television station. *Journal of Guangxi Academy of Sciences*, 27(1): 73-77.

[6] [6] D'Angelo G., D'Emidio M., Frigioni D. 2014. A loop-free shortest-path routing algorithm for dynamic networks. *Theoretical Computer Science*, 516: 1-19.

[7] Wang Fangxiu, Zhou Kang. 2013. Improvement and simulation of Dijkstra algorithm based on backtracking algorithm. *Computer Simulation*, 30(11): 352-355.

[8] Antsura J., Milojevic I., Previdi S., et al. 2013. Segment routing with IS-IS routing protocol.

[9] Zhang Tao. 2013. Configuration and adjustment of management distance in route redistribution. *Science & Technology Vision*. (22): 38-38.

[10] Zhao Lidan, Zheng Xiaoling, Shao Li, et al. 2012. Study of computer simulation of butterfly effectiveness in traf-

fic jams. *Journal of Hefei University of Technology*, 35(2): 221-224.
[11] Di X, Xiong K, Zhang Y, et al. 2014. Joint fountain codes and network coding for wireless butterfly networks. *Electronics & Electrical Engineering*, 20(2).
[12] Yuzhou Y., Dan Z., Huifeng X., et al. 2014. The modeling and simulation of universities' research project management based on NetLogo. *Future Computer and Information Technology*, 86: 353.